Multipartite secure state distribution

W. Dür,[1,2] J. Calsamiglia,[1] and H.-J. Briegel[1,2]
[1]*Institut für Theoretische Physik, Universität Innsbruck, Technikerstraße 25, A-6020 Innsbruck, Austria*
[2]*Institut für Quantenoptik und Quanteninformation der Österreichischen, Akademie der Wissenschaften, Innsbruck, Austria*
(Received 13 December 2004; revised manuscript received 11 February 2005; published 26 April 2005)

We introduce the distribution of a secret multipartite entangled state in a real-world scenario as a quantum primitive. We show that in the presence of noisy quantum channels (and noisy control operations), any state chosen from the set of two-colorable graph states (Calderbank-Shor-Steane codewords) can be created with high fidelity while it remains unknown to all parties. This is accomplished by either blind multipartite entanglement purification, which we introduce in this paper, or by multipartite entanglement purification of enlarged states, which offers advantages over an alternative scheme based on standard channel purification and teleportation. The parties are thus provided with a secret resource of their choice for distributed secure applications.

DOI: 10.1103/PhysRevA.71.042336 PACS number(s): 03.67.Hk, 03.67.Mn, 03.67.Pp

I. INTRODUCTION

In classical information theory, a number of basic primitives are known—among them bit commitment, coin tossing, fingerprinting, Byzantine agreement and key distribution—which serve as building blocks for practically relevant applications. Several of these classical primitives have also been investigated in a quantum setup. It was shown that quantum features allow one to perform certain tasks apparently impossible in a classical setup, the most prominent example being (quantum) key distribution, which allows for unconditional secure communication. The quantum nature of states offers, however, not only additional possibilities to realize classical primitives, but also allows us to consider new primitives that are intrinsically quantum and hence do not have a counterpart in classical information theory or classical physics. An important aspect of such quantum primitives—which has been mostly neglected in previous discussions—is the stability of these concepts under imperfections, i.e., the realization of the task in a real-world scenario. A task that might seem trivial in an idealized scenario may become highly nontrivial or even impossible under realistic conditions, i.e., when taking inevitable noise in quantum channels and local control operations into account. We emphasize that noise is not just a practical issue, but is a fundamental limitation one has to cope with in quantum systems.

In this paper, we will discuss a robust quantum primitive, which may be used as a basic building block for both quantum and classical security applications in situations where local and channel noise are present. Specifically, we will consider the secret creation of a spatially distributed multipartite entangled state with high fidelity. We will consider the set of all two-colorable graph states as possible target states. Two-colorable graph states include many qualitatively different types of multipartite entangled states, each of which can serve as a different resource to perform certain security tasks. In particular, they include any collection of bipartite singlet states shared between some of the parties, any type of multipartite GHZ states, so-called cluster states [1,2] (a universal resource for measurement-based quantum computation), as well as algorithmic specific resources which allow one to implement a certain algorithm (or nonlocal unitary operation) by means of measurements. As has been shown recently, two-colorable graph states are equivalent to codewords of Calderbank-Shor-Steane (CSS) codes [3]. It may be of interest to the end users that the state remains secret to any third party, i.e., nobody else knows which specific resource they share (and hence which tasks they are able to perform). The information about the state can even remain unknown to the parties themselves, being only disclosed to a single end user (e.g., a trusted party or dealer). This is relevant in the implementation of distributed secure quantum applications over noisy communication channels, which count with an additional "adversary," the eavesdropper (that should be considered as the noise source in the channel), and that might collaborate with the untrustful parties. There are standard purification protocols [3–9] used to reduce noise levels and factor out any possible eavesdropper even in the presence of noise [10]. However, these protocols cannot straightforwardly be accommodated to account for possible untrustful parties—which actively participate in the purification protocol—and for their possible complicity with the eavesdropper.

In this paper, we present ways to achieve the secure distribution of the aforementioned graph states under realistic conditions, i.e., noisy quantum channels and imperfect local control operations. After fixing notation and describing the scenario for secret state distribution in Sec. II, we present three possible solutions to the problem in Sec. III. The first approach, described in Sec. III A, is based on channel purification and teleportation, while the second and third approach deal with direct multipartite entanglement purification. The second approach, described in Sec. III B, uses blind multipartite entanglement purification, which we introduce in this paper. In the third approach (see Sec. III C), the security is guaranteed by purifying an enlarged entangled state. We summarize and conclude in Sec. IV.

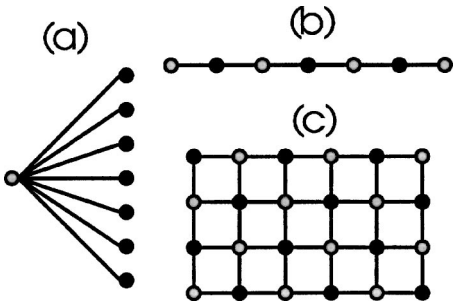

FIG. 1. Examples of two-colorable graphs which correspond to (a) GHZ state; (b) linear cluster state; (c) two-dimensional cluster state. Vertices with the same color are not connected by edges.

II. DEFINITIONS AND DESCRIPTION OF THE SCENARIO

A. Two-colorable graph states

We start by defining two-colorable graph states. A graph G, given by a set of N vertices $\{1,2,\ldots,N\}$ connected in a specific way by edges E, is called two-colorable if there exists two groups of vertices, A,B, such that there are no edges inside either of the groups, i.e., $\{k,l\}\notin E$ if $k, l\in A$ or $k, l\in B$ (see Fig. 1). To every such graph there corresponds a basis of N-qubit states $\{|\boldsymbol{\mu}\rangle_G\}$, where each of the basis states $|\boldsymbol{\mu}\rangle_G$ is the common eigenstate of N commuting correlation operators K_j^G with eigenvalues $(-1)^{\mu_j}$, $\boldsymbol{\mu}=\mu_1\mu_2\cdots\mu_N$. That is, they fulfill the set of eigenvalue equations $K_j^G|\boldsymbol{\mu}\rangle_G=(-1)^{\mu_j}|\boldsymbol{\mu}\rangle_G$, $j=1,\ldots,N$. The correlation operators are uniquely determined by the graph G and are given by

$$K_j^G=\sigma_\alpha^{(j)}\prod_{\{k,j\}\in E}\sigma_\alpha^{(k)}, \tag{1}$$

where $\alpha=x$ $[\alpha=z]$ if $j\in A$ $[j\in B]$, respectively, and $\sigma_\alpha^{(k)}$ denotes the application of the corresponding Pauli operator by party k. Note that the so-defined graph states are identical to the usual graph states, as introduced in [2] and, e.g., used in Refs. [8,9], up to local Hadamard operations performed on all particles in B. As has been shown recently [3], they are in fact equivalent to codewords of the CSS codes. We also remark that the correlation operators $\{K_j\}$ are the generators of a group which is often called the stabilizer of the state $|\mathbf{0}\rangle_G$, and the corresponding description in terms of the stabilizers is also referred to as the stabilizer formalism.

We will also consider mixed states ρ, which for a given graph G can be written in the corresponding graph state basis $\{|\boldsymbol{\mu}\rangle_G\}$, $\rho=\Sigma_{\boldsymbol{\mu},\boldsymbol{\nu}}\lambda_{\boldsymbol{\mu}\boldsymbol{\nu}}|\boldsymbol{\mu}\rangle\langle\boldsymbol{\nu}|$. We will often be interested in fidelity of the mixed state, i.e., the overlap with some desired pure state, say $|\mathbf{0}\rangle_G$, $F=\langle\mathbf{0}|\rho|\mathbf{0}\rangle$.

B. Description of scenario

We consider a central party C (the company), which is connected via noisy quantum channels to N spatially separated local agents A_j, $j\in\{1,2,\ldots,N\}$. The company offers the service to spatially separated customers to deliver upon request any multipartite entangled state chosen from the set of two-colorable graph states, specified by the graph G and the (basis) index $\boldsymbol{\mu}$, with chosen fidelity $F=1-\epsilon$. The state is delivered by the local agents A_j to the end users E_j. The company guarantees as a special security service that the local agents, a potential eavesdropper, or any other party different from the one who placed the order, cannot learn any information about the chosen state.

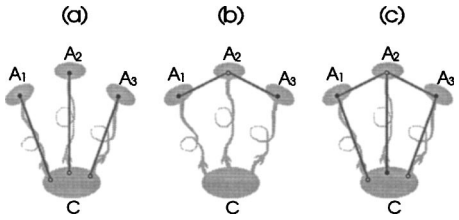

FIG. 2. Setup for secure distribution of multipartite entangled states based on (a) channel purification (i); (b) direct purification of multipartite entangled states (ii); (c) purification of enlarged entangled states (iii).

III. SECRET STATE DISTRIBUTION: POSSIBLE SOLUTIONS

We remark that in the case of noiseless quantum channels between C and the local agents, the described task can be trivially achieved by creating locally at C a single copy of the requested state and distributing it to the local agents. The single copy does not allow the local agents and a potential eavesdropper to learn information about the graph G, even if they decide to cooperate and perform measurements. This follows from the fact that the basis index $\boldsymbol{\mu}$ is unknown and random from the point of view of the local agents, which implies that for any chosen graph G the ensemble of states $\{|\boldsymbol{\mu}\rangle_G\}$ forms the identity and ensembles corresponding to different graphs G are hence indistinguishable. However, if (as in a realistic scenario) the quantum channels connecting the central station C with the local agents A_j are noisy, the task becomes nontrivial. In this case, the state obtained by the local agents ρ_A will be mixed and the fidelity will be below the desired one.

Realistic applications must be designed to cope with two sources of errors, namely noisy channels and noisy local operations. It is well known that problems arising from the noisy channels can be overcome using *entanglement purification*. In a multipartite scenario, we will thus opt for one of the following approaches depending on the particular conditions (see Fig. 2).

(i) Channel purification (see Sec. III A): The channel itself may be purified. This can be accomplished by sending parts of maximally entangled singlet states through each individual channel from C to A_j and creating from the resulting multiple copies of the noisy bipartite entangled states a few copies with high fidelity by a sequence of local operations and classical communication (LOCC), e.g., using one of the entanglement purification protocols of Refs. [4,5]. These high-fidelity entangled states can then be used for teleportation [11] and serve as a purified channel, thereby allowing for the distribution of arbitrary multipartite entangled states.

(ii) Direct multiparty entanglement purification (see Sec. III B): The resulting multipartite mixed states ρ_A can be pu-

rified. That is, several copies of the multipartite mixed states $\rho_{\boldsymbol{A}}$ are produced by distributing the locally created graph state through noisy channels to the local agents A_j. A suitable sequence of LOCC, e.g., the purification protocol for two-colorable graph states introduced in Ref. [8], allows us to create few copies with (arbitrary) high fidelity.

(iii) Purification of enlarged states (see Sec. III C): One can purify an enlarged entangled state, i.e., a (graph) state that is entangled with additional particles that are kept at the central station, while the remaining particles are sent through the noisy channels. The resulting mixed state $\rho_{\boldsymbol{AC}}$ is purified by means of direct multipartite entanglement purification as in (ii), and the desired state shared among the parties A_j can be created from the purified state (ideally given by $|\Psi_{\boldsymbol{AC}}\rangle$) by means of local measurements in C.

On top of the noise from channels, there is also noise in the local control operations. In this case, it turns out that entanglement purification is still possible, although the minimal required fidelity $F_{\min}$ (i.e., the maximal acceptable channel noise) as well as the maximal reachable fidelity $F_{\max}$ of the purified states is limited by the amount of noise in the local control operations [8,9,12] and in fact strongly depends on the entanglement purification protocol that is used. It was shown in Ref. [9] that direct multipartite entanglement purification offers advantages over protocols based on bipartite purification. In particular, for graph states of small degree and a generic noise model for local operations, the reachable fidelity for multipartite states created by bipartite entanglement purification (i.e., channel purification) and teleportation turns out to be *smaller* than the fidelity of the states created by direct multipartite entanglement purification, i.e., $F_{\max}^{(ii)} > F_{\max}^{(iii)} > F_{\max}^{(i)}$. This is true for all values of the local noise (see Fig. 7 in [9]). The upper fixed points $F_{\max}$ only depend on noise in local control operations and on the entanglement purification protocol. On the other hand, the minimal required fidelity $F_{\min}$ (which again depends on the purification protocol and noise in local control operations) puts limits on the maximal acceptable channel noise. The minimal required fidelity $F_{\min}$ fulfills for uncorrelated channels $F_{\min}^{(\mathrm{i})} < F_{\min}^{(\mathrm{iii})} < F_{\min}^{(\mathrm{ii})}$, while in the case of correlated channels the situation can also be the other way around. In general, each of the three schemes (i)–(iii) has its own advantages. There are parameter regimes (noise level of local operations, channel noise) for which a certain scheme allows one to create an entangled state with sufficiently high fidelity, while the other two schemes fail. In particular, it can happen that a multipartite state cannot be produced with required fidelity $F=1-\epsilon$ as requested by customers when using method (i), while a protocol based on direct multipartite entanglement purification (ii) or (iii) enables one to reach the required fidelity. These facts are our main motivation to provide alternative methods to (i) to accomplish the secret creation of a multipartite entangled state, that are based on direct multiparty entanglement purification.

A. Channel purification

For perfect local control operations, approach (i) immediately leads to a protocol to create arbitrary multipartite entangled states with high fidelity in such a way that local agents and possible eavesdroppers do not learn any information about the created state. The purification of the channel does not contain any information about the state, and the presence of eavesdroppers can be excluded by checking the resulting singlet states (e.g., by testing a violation of Bell's inequality or, simpler, by measuring the expectation values of the correlation operators $\langle K_j\rangle$, $j=1,\ldots,N$) [13]. After successful teleportation, the local agents only possess a single copy of an unknown state in a random basis. Again, as in the case of noiseless channels, the ensembles corresponding to different graphs G are indistinguishable. The teleportation process may even be postponed until the local agents deliver (several copies of) the purified singlets to the end users (who may then check the validity of the singlets together with C by testing a random subset) before teleporting the requested multipartite state. This circumvents any possible attempts of the local agents or eavesdroppers to learn information about the state or to corrupt the delivered state at a later stage. Security requirements are fulfilled even in the presence of imperfect control operations, as no information regarding the finally distributed state can be learned.

B. Direct multipartite entanglement purification

We now turn to the second scenario (ii), the direct purification of noisy multipartite entangled states, namely two-colorable graph states. For simplicity of the analysis, we consider in the following noiseless local operations. This restriction is, however, not crucial and will in fact be dropped later on. We start by summarizing the main steps involved in any multipartite purification protocol [8,9]: (a) Depolarization of the mixed state ρ to standard form ρ_G diagonal in the basis of entangled states to be purified; (b) local operations on two (or more) copies of the state ρ_G in such a way that information about the first state(s) is transferred to the last one; (c) measurement of the last state to retrieve this information, public announcement of the measurement outcomes, and keeping or discarding the remaining states depending on the measurement outcomes.

It is easy to see that information about the state $|\boldsymbol{\mu}\rangle_G$ to be purified, both about the graph G and the used basis $\boldsymbol{\mu}$, can be learned in various ways by all local agents involved in such a protocol. In the depolarization process (a), elements of the stabilizer of $|\boldsymbol{\mu}\rangle_G$ (all possible products of correlation operators K_j^G) are applied [3,8,9], which reveal information about the graph G. The local operations and measurements performed in the second step provide knowledge about the structure of the graph. For example, in the recurrence protocol of Ref. [8], the two-coloring of the graph is revealed. The information about the measurement outcomes together with the fact that a particular outcome is interpreted as a successful step also allows the parties to obtain information about the graph. The statistics of measurement outcomes in several steps of the protocol can be used to learn both G and $\boldsymbol{\mu}$, as for all possible graphs the expectation values of K_j^G can be calculated and the corresponding histograms can be analyzed. Finally, since in principle a large number of copies of the state are available, (some of) the local agents can decide

to perform state tomography on a subensemble, thereby learning all information about the state they should purify. That is, when using any (known) direct multiparticle entanglement purification protocol, the secrecy of the state to be purified is not guaranteed.

1. Blind purification

In the following, we will present a modified multipartite entanglement purification protocol where it is impossible for all involved local agents to learn any information about the state being purified, even if *all* of them decide to collaborate and even if they conspire with a possible eavesdropper who is in full control of all quantum channels between C and A_j. The central station C coordinates the action of the local agents and is the only party (besides the customer that placed the order) that knows the graph state which is being purified. The customers' order consists in the graph G and the desired basis index $\boldsymbol{\mu}$, as well as an additional secret random bit string of suitable size [14]. After receiving the order, the central party prepares M two-colorable graph states corresponding to the graph G and chooses the basis indices $|\boldsymbol{m}_i\rangle_G$ randomly from a uniform distribution. For any graph G, the set of graph states is complete, i.e., $\Sigma_{\boldsymbol{m}}|\boldsymbol{m}\rangle_G\langle\boldsymbol{m}|=\mathbb{1}$. This implies that the completely mixed ensemble of states corresponding to two different graphs G_1 and G_2, $\{|\boldsymbol{m}_i\rangle_{G_1}\}_{i=1,2,\ldots,M}$ and $\{|\boldsymbol{m}_i\rangle_{G_2}\}_{i=1,2,\ldots,M}$, is indistinguishable, as the corresponding density operator (i.e., the proper description of the ensemble for any observer not possessing the information about $\boldsymbol{m}_i$) is the completely mixed state ($\propto\mathbb{1}$) [15]. The states $|\boldsymbol{m}_i\rangle$ are then distributed through noisy channels to the local agents A_j. Purification of these states takes place by a protocol (see below) where no information about the indices $\boldsymbol{m}_i$ or the graph G is revealed, which ensures that at any stage of the protocol the ensemble of states corresponding to different graphs remains indistinguishable by the local agents. Finally, the state $|\boldsymbol{\mu}\rangle_G$ is delivered to the end users.

The first step in the purification protocol is to ensure that the mixed state ρ—which arises after sending the state $|\boldsymbol{m}\rangle_G$ through the noisy channels $\mathcal{E}_1,\mathcal{E}_2,\ldots,\mathcal{E}_N$—is diagonal in the specific graph state basis $\{|\boldsymbol{n}\rangle_G\}$. In standard purification protocols, this is enforced by depolarizing the transmitted state. Instead, here we depolarize the channels $\mathcal{E}_j$ to a Pauli-diagonal form [16]. This can be accomplished by applying probabilistically the operators σ_i (σ_i^T) before (after) sending a particle through the channel in a correlated way (here $\{\sigma_i\}_{i=0,\ldots,3}=\{\mathbb{1},\sigma_x,\sigma_y,\sigma_z\}$). Given a general initial channel $\mathcal{E}\rho=\Sigma_{i,j=0}^{3}\lambda_{ij}\sigma_i\rho\sigma_j$, the resulting depolarized channel $\tilde{\mathcal{E}}$ is then given by $\tilde{\mathcal{E}}\rho=\Sigma_{j=0}^{3}\lambda_{jj}\sigma_j\rho\sigma_j$. Moreover, the action of a Pauli operator in party A_k on a graph state results in another graph state: $\sigma_i^{(A_k)}|\boldsymbol{m}\rangle_G\langle\boldsymbol{m}|\sigma_i^{(A_k)}=|\boldsymbol{m}\oplus\boldsymbol{n}_i^G\rangle_G\langle\boldsymbol{m}\oplus\boldsymbol{n}_i^G|$, where $\boldsymbol{n}_i^G$ depends on the neighborhood of particle A_k specified by the graph G [9]. That is, sending $|\boldsymbol{m}\rangle_G$ through the depolarized channels also results—independently of the graph G—in the creation of a graph-diagonal state in this specific graph state basis [17]. Additionally, by writing $|\boldsymbol{m}\rangle_G=\sigma_z^{\boldsymbol{m}_A}\sigma_x^{\boldsymbol{m}_B}|\boldsymbol{0}\rangle_G$, where $\boldsymbol{m}=(\boldsymbol{m}_A,\boldsymbol{m}_B)$ and $\sigma_i^{\boldsymbol{m}_A}$ denotes the action of σ_i on all parties $j\in A$ for which $m_j=1$, we find that if

$$\rho_{\boldsymbol{0}}=\mathcal{E}_1\cdots\mathcal{E}_N|\boldsymbol{0}\rangle_G\langle\boldsymbol{0}|=\sum_{\boldsymbol{n}}\lambda_{\boldsymbol{n}}|\boldsymbol{n}\rangle_G\langle\boldsymbol{n}| \tag{2}$$

is the state resulting from sending $|\boldsymbol{0}\rangle_G$ through the channels, then the resulting state $\rho_{\boldsymbol{m}}$ when sending a different basis state $|\boldsymbol{m}\rangle_G$ is given by a simple basis shift of $\rho_{\boldsymbol{0}}$, i.e.,

$$\rho_{\boldsymbol{m}}=\mathcal{E}_1\cdots\mathcal{E}_N|\boldsymbol{m}\rangle_G\langle\boldsymbol{m}|=\sum_{\boldsymbol{n}}\lambda_{\boldsymbol{n}}|\boldsymbol{n}\oplus\boldsymbol{m}\rangle_G\langle\boldsymbol{n}\oplus\boldsymbol{m}|. \tag{3}$$

These are nontrivial properties of states diagonal in a graph state basis that follow from the description of these states in terms of their stabilizers and from the commutation relations of the Pauli matrices. At this stage, the local agents A_j thus share the M states $\{\rho_{\boldsymbol{m}_i}\}_{i=1,\ldots,M}$ [18].

We now introduce modified multipartite recurrence protocols $P1'$, $P2'$ that give the same performance as the protocols $P1$, $P2$ of Refs. [8,9], but operate on states $\rho_{\boldsymbol{m}}$, $\rho_{\boldsymbol{n}}$ [which are obtained by a basis shift from $\rho_{\boldsymbol{0}}$ according to Eq. (3)] and fulfill our security requirements. We start with protocol $P1'$, where in a first step local controlled-NOT (CNOT) operations [19] with the particles of the first (second) state acting as source (target), respectively, are applied by all parties. It is easy to check that the action of such multilateral CNOT operations is given by

$$|\boldsymbol{m}_A,\boldsymbol{m}_B\rangle|\boldsymbol{n}_A,\boldsymbol{n}_B\rangle\rightarrow|\boldsymbol{m}_A,\boldsymbol{m}_B\oplus\boldsymbol{n}_B\rangle|\boldsymbol{m}_A\oplus\boldsymbol{n}_A,\boldsymbol{n}_B\rangle. \tag{4}$$

All particles of the second state are then measured in the eigenbasis $\{|0\rangle_x,|1\rangle_x\}$ of σ_x, yielding results $(-1)^{\xi_i}$ which are publicly announced. From ξ_i, the expectation values of all correlation operators K_j with $j\in A$ can be calculated at the central station C. The result is taken as a successful purification step if the calculated expectation values correspond to $\boldsymbol{m}_A\oplus\boldsymbol{n}_A$. In this case, one finds that the resulting state is again diagonal in the graph state basis, with new coefficients

$$\tilde{\lambda}_{\boldsymbol{\gamma}_A\oplus\boldsymbol{m}_A,\boldsymbol{\gamma}_B\oplus\boldsymbol{m}_B\oplus\boldsymbol{n}_B}=\frac{1}{2K}\sum_{\{(\boldsymbol{\nu}_B,\boldsymbol{\mu}_B)|\boldsymbol{\nu}_B\oplus\boldsymbol{\mu}_B=\boldsymbol{\gamma}_B\}}\lambda_{\boldsymbol{\gamma}_A,\boldsymbol{\nu}_B}\lambda_{\boldsymbol{\gamma}_A,\boldsymbol{\mu}_B}, \tag{5}$$

where K is a normalization constant. Note that these coefficients are exactly the same as in the situation where we apply the original protocol $P1$ to two copies of $\rho_{\boldsymbol{0}}$, only the basis of the resulting state is shifted by $(\boldsymbol{m}_A,\boldsymbol{m}_B\oplus\boldsymbol{n}_B)$ [as done in Eq. (3)]. Similarly, the protocol $P2'$ consists of local CNOTs in the opposite direction, followed by measurement of all particles of the second state in the eigenbasis $\{|0\rangle_z,|1\rangle_z\}$ of σ_z. From the measurement outcomes, the expectation values of all correlation operators K_j, $j\in B$ can be calculated at the central station C. The result is interpreted as a successful step if the calculated expectation values correspond to $\boldsymbol{m}_B\oplus\boldsymbol{n}_B$. Again, one can determine the action of this protocol on two states $\rho_{\boldsymbol{m}}\otimes\rho_{\boldsymbol{n}}$ and finds that the resulting state is up to a basis shift $(\boldsymbol{m}_A\oplus\boldsymbol{n}_A,\boldsymbol{m}_B)$ the same as the one obtained by the protocol $P2$ applied to $\rho_{\boldsymbol{0}}^{\otimes 2}$. The purification procedure takes place by an alternating application of protocols $P1'$, $P2'$, where at each step the central station randomly chooses the pairs to combine. In particular, also pairs resulting from unsuccessful purification rounds are further processed. We remark that this substantially reduces the yield of the entanglement purification protocol as compared to the original

scheme. The reachable fidelity and error thresholds, however, are exactly the same as those of protocols $P1$, $P2$ investigated in Refs. [8,9]. The only difference from the original scheme for the central party C is that it has to keep track of the basis shift for each state and modify the decision about successful/unsuccessful purification steps (which are not publicly announced) accordingly. We remark that in order to determine the basis shifts for final copies, knowledge of the initial basis shifts $\{\boldsymbol{m}_i\}$ and the history of the purification procedure is required for each state, i.e., $\boldsymbol{n}_i = f_i(\boldsymbol{m}_i)$. At the end of the procedure, additional independent random basis shifts are applied to all states (this can be accomplished by letting the local agents apply appropriate Pauli operators), where for a specific copy, say 1, resulting from a successful purification branch (i.e., all purification steps successful), a basis shift $\boldsymbol{n}_1 \oplus \boldsymbol{\mu}$ is performed. This guarantees that copy 1 is in the basis $\boldsymbol{\mu}$ and hence corresponds to the required state. The order of the copies is randomly chosen by C in such a way that copy 1 is located at a position specified by the additional secret bit string which is shared with the end users. All states (also the ones resulting from unsuccessful purification steps) are then handed over to the end users. This ensures that it remains unknown to all involved parties (except C and the end users) which of the copies correspond to successful branches. Finally, all states but copy 1 are measured, either in the eigenbasis of σ_x or σ_z, and the measurement results are publicly announced. This allows the central station to check the trustfulness of the local agents, as, e.g., for states corresponding to a successful purification procedure the expectation values of the correlation operators K_j^G and hence the fidelity of the produced states can be determined by C [13]. Depending on the results of this verification procedure, C uses another shared random bit to secretly announce whether the remaining copy can be used for the desired security application. We note that distrustful local agents or an eavesdropper can always prevent a successful generation of the desired state, e.g., by simply not taking place in the purification procedure as requested or by adding additional noise. However, if the state passed the verification procedure, it can be guaranteed that it has the required fidelity and that the local agents have not learned information about the target state.

2. Security of direct multiparty entanglement purification

We now discuss the security of this modified protocol by analyzing the scheme from the point of view of the local agents (or eavesdropper). We first remark that the entanglement purification protocol is carefully constructed in such a way that absolutely no information about the state to be purified is revealed during the protocol. In contrast to original protocols $P1$, $P2$, the protocols are symmetric, i.e., no information about the two-coloring of the graph is revealed. The randomly chosen basis states $\{\boldsymbol{m}_i\}$ guarantee that at any stage of the protocol no information about the structure of the graph can be learned from measurement statistics, as any statistics is randomized due to random basis shifts. Even the information of whether a given purification step is successful or not is kept secret. This is guaranteed on the one hand by randomly combining copies of the state after each purification round, and on the other hand by delivering the whole ensemble of states rather than a single copy (which the local agents would otherwise identify as the resulting state of several successful purification rounds). Although it seems unlikely that such a tiny amount of information could be used by the local agents and eavesdropper to learn about the identity of the graph state, it cannot be excluded that there exists a strategy which allows them to make use of this information. One may, e.g., imagine that by means of a graph state analyzer they were able to learn information about the basis index $\boldsymbol{m}_i$ for this specific state, which—together with the information that the state results from several successful purification rounds—could then be used to exclude the graphs that are incompatible with the measurement outcomes obtained in the purification protocol. Hence, we have modified the purification protocol in the way described above, which guarantees that *no* additional information can be learned from the protocol itself. In fact, from the point of view of the local agents, the protocol they should perform (as well as all measurement outcomes, etc.) is the same for all graph states. It follows that the secrecy of the graph state to be purified is still guaranteed by the fact that the corresponding ensembles of states for two different graph states are indistinguishable, as they are both described by the identity. Naturally, this still holds if one considers the transmitted ensemble of states $\{\rho_{\boldsymbol{m}_i}\}$ instead of $\{\boldsymbol{m}_i\}$: it is safe to attribute the noise in the channel to the actions of an eavesdropper and/or the agents.

We finally remark that unconditional security can only be guaranteed if we keep the information whether the required state has been successfully created or not secret. Otherwise there exists an (indirect) strategy for a possible eavesdropper to learn about the graph: by varying the noise in the channel (we assume that Eve has complete control over the channel), Eve together with the local agents can prevent the purification of certain states (e.g., states with high degree) as for these states the channel noise (or noise in local control operations) is above the threshold value where purification is possible. As the threshold values depend on the graph, knowing whether the purification procedure was successful or not would provide Eve with some information about the graph, e.g., about its (local) degree. This is just a single bit of information which might well be negligible in many cases as there exist exponentially many different graph states which are potential target states. By keeping the information of whether the procedure was successful or not secret, we prevent Eve from learning even this single bit of information. The validation stage in our protocol only serves to detect possible attempts of the local agents to prevent the production of the state with required fidelity. The secrecy of the states is guaranteed by other means (the random basis shifts). In principle, one may use the validation stage also to detect possible attempts of Eve or the local agents to gain information about the final graph, which clearly leads to corruption of the states and hence to reduced fidelity. In approach (iii), we will discuss a strategy which guarantees security even when the success or failure of the protocol is publicly known. The strategy of (iii) can immediately be adopted to the protocol described above.

The influence of noisy local operations can easily be analyzed. From the point of view of the central station C, we

essentially have entanglement purification protocols $P1$, $P2$ with imperfect means with the corresponding properties discussed in Refs. [8,9]. In particular, entanglement purification is still possible even for errors of local operations at the order of (several) percent. Only the reachable fidelity of the target state is limited. From the point of view of the local agents, the additional noise in their operations will not enable them to learn more information about the state to be purified than they would be able to learn if their operations are noiseless (they still would have to distinguish between two ensembles of states which are both—from their point of view—the identity at all stages of the protocol). Thus the produced state remains secret and the required procedure can be followed in a real-world scenario. The secrecy of the states at all stages is guaranteed by the random basis shifts $\{\boldsymbol{m}_i\}$, which on the one hand ensure that the input ensemble is the maximally mixed state, and on the other hand that measurement statistics and any association of specific outcomes with the graph structure during the protocol itself are randomized. The second statement follows from the nontrivial property of two-colorable graph states that basis shifts can be effectively propagated through both the channels and the purification protocols, resulting in output states with shifted bases.

C. Purification of enlarged states

We now turn to scenario (iii), the purification of enlarged states. Instead of creating the desired graph state $|\boldsymbol{\mu}\rangle_G$ directly and sending several copies through the noisy channels to the local agents, the central station can also create enlarged graph states $|\mathbf{0}\rangle_{\tilde{G}}$ of $2N$ qubits in such a way that each vertex of the initial graph is connected to an additional, independent vertex. That is, if $G=(V,E)$ is the graph of vertices $\{1,2,\ldots,N\}$, then the graph $\tilde{G}$ corresponding to the enlarged state is given by vertices $\{1,2,\ldots,2N\}$ with edges $\tilde{E}=E\cup\{(k,k+N)\}$ with $k=1,2,\ldots,N$. The qubits corresponding to vertices 1 to N are sent through the noisy channels to the local agents, while qubits $N+1$ to $2N$ are kept by the central party C. The bases randomization of initial states done in approach (ii) is replaced here by additional quantum correlations between C and A_j. In principle, C could introduce random basis shifts on the states of A_j by performing suitable measurements [reducing the protocol to the one discussed in (ii)]. However, the quantum correlations are more powerful than classical correlations, which allow us to further simplify the purification protocol. The purification takes place by a multipartite protocol and hence offers advantages (e.g., higher reachable fidelity) as compared to scheme (i) based on channel purification. When compared to scheme (ii), one finds a higher robustness of the states against channel noise for uncorrelated channels. It is easy to check that the state $|\mathbf{0}\rangle_{\tilde{G}}$ can be written as

$$|\mathbf{0}\rangle_{\tilde{G}}=\frac{1}{\sqrt{2^N}}\sum_{\boldsymbol{m}}|\boldsymbol{m}\rangle_G\otimes|\boldsymbol{m}\rangle, \tag{6}$$

where $|\boldsymbol{m}\rangle_G$ is a graph state corresponding to graph G of particles 1 to N, while $|\boldsymbol{m}\rangle=|m_1m_2\cdots m_N\rangle$ with $m_j\in\{0,1\}$ are orthogonal product states of particles $N+1$ to $2N$ and the sum runs over all possible binary vectors $\boldsymbol{m}$. We have that $|m_k\rangle$ denotes the eigenstate with eigenvalue $(-1)^{m_k}$ of the operator σ_z if $k\in A$ [σ_x if $k\in B$], where A,B correspond to the two-coloring of the graph $\tilde{G}$.

The resulting noisy graph states are then purified using multipartite entanglement purification protocols $P1'$, $P2'$ described above, which can be applied because the graph $\tilde{G}$ is two-colorable whenever the initial graph G is two-colorable. While the local agents publicly announce their measurement outcomes, the central party C keeps its measurement outcomes secret. The expectation value of each correlation operator K_j—which determines whether a purification step is successful or not—depends on the measurement outcome in particle j and its neighbors. For $j>N$, particle j itself is held by C, while for $j<N$ the neighboring particle $(j+N)$ is held by C, which implies that the expectation value of K_j $\forall j$ cannot be determined by the local agents. The additional qubits held at C act as a randomizer for all measurement outcomes of the local agents. After several successful purification rounds (where in this case always two pairs resulting from a successful purification round can be combined), all but a single copy is measured in the eigenbasis of σ_x or σ_z, where again only the measurement outcomes of local agents are announced. From the measurement outcomes, C can calculate expectation values for the correlation operators K_j and hence verify whether the required fidelity of the states was achieved. If the states passed the validation step, i.e., the required fidelity is achieved, the local agents hand the particles of the remaining copy over to the end users. Finally, all qubits in C of the remaining copy are measured in the eigenbasis of σ_z (σ_x) if they are in A (B), where A, B corresponds to the two-coloring of the graph $\tilde{G}$. If the final states were pure, i.e., $|\mathbf{0}\rangle_{\tilde{G}}$, it follows from Eq. (6) that for a measurement outcome corresponding to $\boldsymbol{m}=m_1m_2\cdots m_N$ with $m_j\in\{0,1\}$, the resulting state shared by the end users would be given by $|\boldsymbol{m}\rangle_G$. Announcing publicly the bit string $\boldsymbol{m}\oplus\boldsymbol{\mu}$ allows the end users to shift the basis such that they finally hold the state $|\boldsymbol{\mu}\rangle_G$. Note that $\boldsymbol{m}\oplus\boldsymbol{\mu}$ is a random string from the point of view of local agents and an eavesdropper, and does not contain information since $\boldsymbol{\mu}$ is secret. We consider now the case where the final state is mixed, i.e., $\rho_{\tilde{G}}=\sum_{\boldsymbol{\mu}\boldsymbol{\nu}}\lambda_{\boldsymbol{\mu}\boldsymbol{\nu}}|\boldsymbol{\mu}\boldsymbol{\nu}\rangle_{\tilde{G}}\langle\boldsymbol{\mu}\boldsymbol{\nu}|$, where $\boldsymbol{\mu}$ corresponds to vertices 1 to N (i.e., the particles held by the local agents) while $\boldsymbol{\nu}$ refers to vertices $N+1$ to $2N$ (i.e., the particles held by C). In the case where the outcome of all measurements is $(+1)$, we have that the state after the measurements in C is given by

$$\rho_{\mathbf{0}}=\sum_{\boldsymbol{\mu}}\left(\sum_{\boldsymbol{\nu}}\lambda_{\boldsymbol{\mu}\boldsymbol{\nu}}\right)|\boldsymbol{\mu}\rangle_G\langle\boldsymbol{\mu}|, \tag{7}$$

while for other measurement outcomes $\boldsymbol{m}$ the basis is shifted by $\boldsymbol{m}$, i.e., we obtain $\rho_{\boldsymbol{m}}$. Note that the fidelity ${}_G\langle\boldsymbol{m}|\rho_{\boldsymbol{m}}|\boldsymbol{m}\rangle_G$ with respect to the graph state corresponding to the graph G is larger than the fidelity of the initial (enlarged) state with respect to the graph state $|\mathbf{00}\rangle_{\tilde{G}}$, which is given by $\lambda_{\mathbf{00}}$.

1. Security of purification of enlarged states

We now discuss the security of this protocol. We have that the reduced density operator of particles 1 to N held by the

local agents (or an eavesdropper) is given by $\Sigma_{\boldsymbol{m}}|\boldsymbol{m}\rangle_G\langle\boldsymbol{m}|$, which is the identity for *any* graph G. This implies that even if several copies of the state are available to the local agents, they are not able to distinguish between different graphs. In fact, the state $|\mathbf{0}\rangle_{\tilde{G}}$ [Eq. (6)] is maximally entangled between systems C and the local agents. This implies that by an appropriate unitary operation in C, one can change the subgraph G in A to any other subgraph G'. This can be seen from the fact that for a maximally entangled state $|\Phi\rangle_{CA}$, $U_C^T\otimes\mathbb{1}_A|\Phi\rangle=\mathbb{1}_A\otimes U_A|\Phi\rangle$. In other words, C has in principle the freedom to change the delivered state until the last moment, i.e., after the last copy is delivered to the end users, which clearly makes it impossible for the local agents or any eavesdropper to determine the state. For these states it is also irrelevant whether the local agents learn if the final state is the result of several successful purification rounds. While in the purification of the initial graph state $|\mathbf{0}\rangle_G$ this information (together with the knowledge of basis) would have allowed the local agents to exclude certain graphs (as they are not compatible with the values for correlation operators K_j^G calculated from the measurement outcomes), here the value of each correlation operator $K_j^{\tilde{G}}$ depends on the unknown, random measurement outcome of a qubit in C and hence is unknown (and completely random) from the point of view of the local agents or eavesdropper. Hence, one can in this case deliver only a single copy of the state to the end users (thereby revealing that this copy is the result of several successful purification rounds) as well as only combine copies resulting from a previous successful purification step without compromising security of the protocol.

The only possibility left to the eavesdropper to gain information about the graph is the indirect attack outlined in the description of protocol (ii), Sec. III B. That is, Eve may adjust the noise in channels and local operations in such a way that only certain states can be purified (group 1), while others cannot (group 2). From the fact whether the purification protocol was successful or not, one bit of information about the graph could be obtained in this way (namely whether the graph belongs to group 1 or 2). However, this approach necessarily forces Eve to modify channel noise and/or noise in local control operations, which can be detected by the central party C. To this aim, C uses an enhanced validation procedure which in this case serves not only to guarantee the fidelity of the states to be purified, but is aimed to detect any possible attempts of the eavesdropper to modify the noise processes. This can be done, e.g., by sending parts of maximally entangled states as probe states at certain instances instead of multipartite states to be purified (the position of these probe states remains unknown to the eavesdropper). Measurements of observables σ_x and σ_z—which occur naturally in the purification protocol—can be used to perform channel tomography (at early instances of the protocol) and process tomography (at later stages of the protocol) and hence to detect any attempts of the eavesdropper to increase noise. Note that it is sufficient to send parts of a maximally entangled state through channels to perform complete channel tomography [20]. Measurements of the two observables are sufficient in this case, as additional basis changes (and hence effective measurements of other observables) can be enforced by C at the local agents during the initial channel depolarization. Local agents can in this case not distinguish whether the requested unitary operations correspond to a channel depolarization procedure or to a real basis change. The procedure is aborted if anything is not as expected (i.e., additional noise in channels or local operations occurred), even if the purification of $|\mathbf{0}\rangle_{\tilde{G}}$ was successful.

Alternatively (or additionally), C may prepare and purify not only the enlarged graph state $|\mathbf{0}\rangle_{\tilde{G}}$, but also several copies of other graph states $|\mathbf{0}\rangle_{\tilde{G}'}$ corresponding to different graphs $\tilde{G}'$ (with different threshold values). The positions of these states are randomly chosen. In the validation step, C checks if the purification of these probe states was successful. This allows C to draw conclusions about attempts of Eve to introduce additional noise and eventually to abort the procedure. We remark that one typically has a hierarchy of states with respect to their fragility to noise. That is, if the purification of a certain state was successful, one can conclude that also several other states (corresponding to different graphs) are purificable. In particular, C can be sure that Eve cannot distinguish between the graph G and any graph $\tilde{G}'$ for which purification succeeded. We remark that the same procedure can also be used in the context of protocol (ii).

IV. SUMMARY AND CONCLUSIONS

The purified states, created by one of the procedures (i), (ii), and (iii), serve as a resource for a variety of (security) tasks. Graph states are, for instance, an algorithmic-specific resource, i.e., depending on which state is produced, a different quantum algorithm can be applied by a simple sequence of local measurements [2]. Other possible applications include secure evaluation of a (secret) function, secret sharing among some of the parties, and multipartite voting schemes. The tasks that can be performed strongly depend on the structure of the graph state being produced, and thus remain unknown to any outside party.

We have introduced the distribution of an unknown multipartite entangled state with high fidelity as a basic quantum primitive, which can be accomplished in a real-world scenario where quantum channels as well as local control operations are noisy. We have presented three alternative ways to achieve this aim, based on channel purification and teleportation or direct multipartite entanglement purification, respectively. While the first approach is conceptually simpler, the second and third offer advantages with respect to reachable fidelities and tolerable errors.

ACKNOWLEDGMENTS

H.-J. Briegel would like to thank J. Oppenheim for discussions. This work was supported by the FWF, the European Union (IST-2001-38877, IST-2001-39227, IST-2004-15714), the DFG, and the Österreichische Akademie der Wissenschaften through project APART (W.D.).

[1] H.-J. Briegel and R. Raussendorf, Phys. Rev. Lett. **86**, 910 (2001).
[2] R. Raussendorf, D. E. Browne, and H.-J. Briegel, Phys. Rev. A **68**, 022312 (2003).
[3] Kai Chen and Hoi-Kwong Lo, e-print quant-ph/0404133.
[4] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996); C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[5] D. Deutsch, A. Ekert, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
[6] M. Murao, M. B. Plenio, S. Popescu, V. Vedral, and P. L. Knight, Phys. Rev. A **57**, R4075 (1998).
[7] E. N. Maneva and J. A. Smolin, in *Quantum Computation and Quantum Information*, edited by J. Samuel and J. Lomonaco (American Mathemathical Society, Providence, RI, 2002), Vol. 305 of *AMS Contemporary Mathematics*; see also e-print quant-ph/0003099.
[8] W. Dür, H. Aschauer, and H.-J. Briegel, Phys. Rev. Lett. **91**, 107903 (2003).
[9] H. Aschauer, W. Dür, and H.-J. Briegel, Phys. Rev. A **71**, 012319 (2005).
[10] H. Aschauer and H. J. Briegel, Phys. Rev. Lett. **88**, 047902 (2002).
[11] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[12] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998); W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, Phys. Rev. A **59**, 169 (1999).
[13] The desired state $|\mathbf{0}\rangle_G$ is the unique eigenstate of *all* correlation operators K_j with eigenvalue $+1$. Hence, expectation values $\langle K_j\rangle < 1$ indicate that the system is not sufficiently close to the desired pure state. From expectation values $\langle K_j\rangle$, one can derive lower and upper bounds on the fidelity of the produced states (and hence decide whether the state can be used for security application). Using that for $\forall \boldsymbol{\mu} \neq \mathbf{0}$, $-N \leqslant \Sigma_j \mathrm{tr}(K_j|\boldsymbol{\mu}\rangle_G\langle\boldsymbol{\mu}|) \leqslant N-2$, we obtain $(\Sigma_j\langle K_j\rangle - N - 2)/2 \leqslant F \leqslant [(1/N)\Sigma_j\langle K_j\rangle + 1]/2$. Note, however, that the information about all N expectation values is not sufficient to determine (diagonal elements of) the resulting state.
[14] (One of) the customers has to secretly convey the order of G and $\boldsymbol{\mu}$ to the central station C, e.g., by using a secure classical channel. One can hence assume that an additional secret bit string can be exchanged along with the order.
[15] An eavesdropper might learn (a slight amount) of information about the actual value of $\boldsymbol{m}_i$ at the expense of disturbing the states, however it is impossible to learn any information about the graph G. As the graph G specifies the (entanglement) properties of the state, the created resource remains unknown to any eavesdropper or distrustful local agents.
[16] W. Dür, M. Hein, and H.-J. Briegel (unpublished).
[17] The diagonal coefficients of the resulting state are, in general, different for the two depolarization procedures. For the widely used class of Pauli channels, the diagonal coefficients are the same and in fact no depolarization is required.
[18] One arrives at exactly the same conclusions in the situation where the channels are not independent, i.e., $\mathcal{E} \neq \mathcal{E}_1\mathcal{E}_2, \ldots, \mathcal{E}_N$, which could arise, for example, during an eavesdropping attack.
[19] The CNOT operation is defined by $|i\rangle_A|j\rangle_B \rightarrow |i\rangle_A|i \oplus j\rangle_B$.
[20] J. I. Cirac, W. Dür, B. Kraus, and M. Lewenstein, Phys. Rev. Lett. **86**, 544 (2001).