Katholieke Universiteit Leuven

Departement Elektrotechniek

ESAT-SISTA/TR 05-214a

Hashing protocol for multipartite entanglement distillation[1]

Erik Hostens, Jeroen Dehaene and Bart De Moor[2]

July 2006
Published in *Proc. of MTNS 2006*

[1]This report is available by anonymous ftp from *ftp.esat.kuleuven.be* in the directory *pub/sista/ehostens/reports/05-214a.pdf*

[2]K.U.Leuven, Dept. of Electrical Engineering (ESAT), Research group SCD, Kasteelpark Arenberg 10, B-3001 Leuven, Belgium, Tel. 32/16/32 86 65, Fax 32/16/32 19 70, WWW: *http://www.esat.kuleuven.be/scd*. E-mail: *erik.hostens@esat.kuleuven.be, jeroen.dehaene@esat.kuleuven.be, bart.demoor@esat.kuleuven.be*.

Abstract

We present a hashing protocol for distilling multipartite CSS states by means of local Clifford operations, Pauli measurements and classical communication. It is shown that this hashing protocol outperforms previous versions by exploiting information theory to a full extent. Using the information-theoretical notion of a strongly typical set, we calculate the asymptotic yield of the protocol as the solution of a linear programming problem.

Hashing protocol for multipartite entanglement distillation

Erik Hostens, Jeroen Dehaene, Bart De Moor

Katholieke Universiteit Leuven, ESAT-SCD
Kasteelpark Arenberg 10, B-3001 Leuven, Belgium
E-mail: erik.hostens@esat.kuleuven.be
Fax: +32 16 321970

July 31, 2006

Abstract

We present a hashing protocol for distilling multipartite CSS states by means of local Clifford operations, Pauli measurements and classical communication. It is shown that this hashing protocol outperforms previous versions by exploiting information theory to a full extent. Using the information-theoretical notion of a strongly typical set, we calculate the asymptotic yield of the protocol as the solution of a linear programming problem.

1 Introduction

Quite recently, a number of very interesting applications of quantum entanglement have been developed. Commonly known examples are teleportation [1], superdense coding [2] and entanglement based quantum cryptography [3]. All these applications require pure entangled states that are shared by a number of remote parties. In practice, however, by the noisy influence of the environment (decoherence), the initial states are disrupted and no longer pure. Therefore, methods are needed to make the applications more robust against decoherence. Both quantum error correcting codes and entanglement distillation were introduced to this purpose. We will focus on the distillation of a particular kind of multipartite stabilizer states.

Stabilizer states and codes are an important concept in quantum information theory. Stabilizer codes [4, 5] play a central role in the theory of quantum error correcting codes, which protect quantum information against decoherence and without which effective quantum computation has no chance of existing. Also in the area of quantum cryptography and quantum communication, both bipartite as multipartite, the number of applications of stabilizer states is abundant. We cite [6, 7, 8, 9, 10], but this is far from an exhaustive list.

Closely related to quantum error correction, entanglement distillation is a means of extracting entanglement from quantum states that have been disrupted by the environment. Many applications require pure multipartite entangled states that are shared by remote parties. In practice, k copies of a pure state are prepared by one party and communicated to the others by imperfect (but stationary) quantum channels. As a result, the copies are no longer in a pure state, but in a mixed state not suited for the application in mind. A distillation protocol then consists of local operations combined with classical communication in order to end up with copies that approach purity and are ready to use in the application. The total entanglement of a quantum system cannot increase under the action of local operations together with classical communication, but it is possible to concentrate the present entanglement in a subsystem. In this setting, this is achieved by first performing local unitary operations such that the states of the copies become statistically dependent, after which the measurement of mk copies yield information on the global system. As a result, the remaining $k(1-m)$ copies are in a more pure state and contain more entanglement.

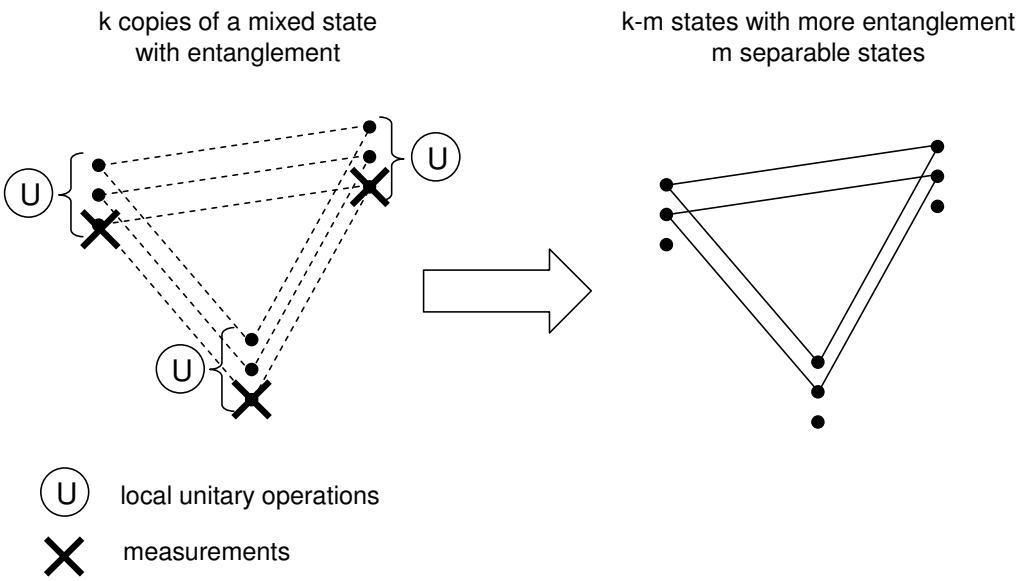

Figure 1: a distillation protocol typically starts with k copies of a mixed state with entanglement, shared by n parties. By applying local unitary operations, the states of the copies become statistically dependent. The measurement of mk copies therefore yield information on the global system. As a result, the remaining $k(1-m)$ copies are in a more pure and entangled state. The mk measured copies are separable and may be discarded. In this figure, we have $n = 3$, $k = 3$ and $m = 1/3$.

The mk measured copies are in a separable, i.e. non-entangled, state and are discarded. This is illustrated in figure 1.

An interesting entanglement distillation protocol is the well-known hashing protocol, introduced for bipartite states (i.e. states involving two parties) in [11], that has its roots in classical information theory. We present a generalization of this hashing protocol from bipartite to multipartite, for a particular but important kind of stabilizer states, called Calderbank-Shor-Steane or CSS states. The basic idea of describing the protocol in a classical information theoretical setting is the same as in [11].

Very similar multipartite hashing protocols have been discussed in [12, 13, 14, 15]. Our protocol improves these protocols in two ways. First, we note that in [12, 13, 14, 15], by not exploiting information theory to a full extent, their protocols result in overkill. In short, demanding that the number of measurements exceeds particular marginal entropies [12, 13, 14] results in too many measurements. In [15], this is partially meeted by relaxing to conditional entropies. Our protocol is optimal in the given setting and is therefore a complete generalization of the hashing protocol. The yield is calculated as the solution of a linear programming problem, and requires a somewhat more involved information-theoretical treatment. A second major difference is that the local unitary operations applied in [12, 13, 14, 15] only consist of CNOT (Controlled-NOT) quantum gates, whereas in some cases a higher yield can be achieved by using more general local unitary operations. However, for clarity reasons we will restrict ourselves in this paper to local unitary operations that are identical and built only of CNOTs, as in [12, 13, 14, 15]. The more general case is treated in [16].

This paper is organized as follows. In section 2, we define the strongly typical set, an information-theoretical concept that is needed to calculate the yield. In section 3, we introduce the binary framework of [17] in which stabilizer states and Clifford operations are efficiently described. In section 4, we show that identical local Clifford operations built from CNOTs result in a permutation of the 2^{nk} k-fold tensor products of an n-qubit CSS state. In section 5, we explain how our hashing protocol works and calculate the yield in section 6. Finally, the protocol

is illustrated and compared to others by an example in section 7. For mathematical details and rigorous proofs, we refer to [16].

2 Strongly typical set

In this section, we introduce the information-theoretical notion of a *strongly typical set*. For an introduction to information theory, we refer to [18].

Let $X = (X_1, \ldots, X_k)$ be a sequence of independent and identically distributed discrete random variables, each having event set Ω with probability function $p : \Omega \mapsto [0, 1] : a \mapsto p(a)$. The strongly typical set $\mathcal{T}_\epsilon^{(k)}$ is defined to be the set of sequences $x = (x_1, \ldots, x_k) \in \Omega^k$ for which the sample frequencies $f_a(x) = |\{x_i \mid x_i = a\}|/k$ are close to the true values $p(a)$, or:

$$x \in \mathcal{T}_\epsilon^{(k)} \;\Leftrightarrow\; |f_a(x) - p(a)| < \epsilon,\ \forall a \in \Omega.$$

It can be verified that $p(\mathcal{T}_\epsilon^{(k)}) \geq 1 - \delta$, where $\delta = O(k^{-1}\epsilon^{-2})$, or $p(\mathcal{T}_\epsilon^{(k)}) \approx 1$ for $k \to \infty$. In words, a random sequence x will almost certainly be contained in the strongly typical set.

Let Ω be partitioned into subsets Ω_j $(j = 1, \ldots, q)$. We define the function

$$y(x) = (\Omega_{j_1}, \ldots, \Omega_{j_k}),\ \text{where } x_i \in \Omega_{j_i},\ \text{for } i = 1, \ldots, k.$$

In section 6, we will encounter the following problem. Given some $u \in \mathcal{T}_\epsilon^{(k)}$, calculate the number $|\mathcal{N}_u|$ of sequences $v \in \mathcal{T}_\epsilon^{(k)}$ that satisfy $y(v) = y(u)$, or

$$\mathcal{N}_u = \{v \in \mathcal{T}_\epsilon^{(k)} \mid y(v) = y(u)\}.$$

It can be verified [16] that

$$|\mathcal{N}_u| \approx 2^{k[H(X) - H(Y)]},$$

where $H(X) = -\sum_a p(a) \log_2 p(a)$ is the entropy of X and $H(Y) = -\sum_j p(\Omega_j) \log_2 p(\Omega_j)$ the entropy of $y(X)$.

3 Stabilizer states, CSS states and Clifford operations

In this section, we present the binary matrix description of stabilizer states and Clifford operations. We show how Clifford operations act on stabilizer states in the binary picture. CSS states are then defined as a special kind of stabilizer states. We will restrict ourselves to definitions and properties that are necessary to the distillation protocols presented in the next sections. In the following, all addition and multiplication is performed modulo 2. For a more elaborate discussion on the binary matrix description of stabilizer states and Clifford operations, we refer to [17].

We use the following notation for Pauli matrices.

$$\sigma_{00} = I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad \sigma_{01} = \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

$$\sigma_{10} = \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \sigma_{11} = \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}.$$

Let $v, w \in \mathbb{Z}_2^n$ and $a = \begin{bmatrix} v \\ w \end{bmatrix}$, then we denote

$$\sigma_a = \sigma_{v_1 w_1} \otimes \ldots \otimes \sigma_{v_n w_n}.$$

The Pauli group on n qubits is defined to contain all tensor products σ_a of Pauli matrices with an additional complex phase factor in $\{1, i, -1, -i\}$. We will only consider Hermitian Pauli operators,

so we may exclude imaginary phase factors. It can also be easily verified that Pauli operators satisfy the following commutation relation:

$$\sigma_a \sigma_b = (-1)^{a^T P b} \sigma_b \sigma_a, \text{ where } P = \begin{bmatrix} 0 & I_n \\ I_n & 0 \end{bmatrix}. \tag{1}$$

A stabilizer state $|\psi\rangle$ on n qubits is the simultaneous eigenvector, with eigenvalues 1, of n commuting Hermitian Pauli operators $(-1)^{b_i}\sigma_{s_i}$, where $s_i \in \mathbb{Z}_2^{2n}$ are linearly independent and $b_i \in \mathbb{Z}_2$, for $i = 1, \ldots, n$. The n Hermitian Pauli operators generate an Abelian subgroup of the Pauli group on n qubits, called the stabilizer $\mathcal{S}$. We will assemble the vectors s_i as the columns of a matrix $S \in \mathbb{Z}_2^{2n \times n}$ and the bits b_i in a vector $b \in \mathbb{Z}_2^n$. Note that it follows from (1) that commutativity of the stabilizer is reflected by $S^T P S = 0$. The representation of $\mathcal{S}$ by S and b is not unique, as every other generating set of $\mathcal{S}$ yields an equivalent description. In the binary picture, a change from one generating set to another is represented by an invertible linear transformation $R \in \mathbb{Z}_2^{n \times n}$ acting on the right on S and acting appropriately on b. We have

$$\begin{array}{rcl} S' & = & SR \\ b' & = & R^T b + d \end{array} \tag{2}$$

where $d \in \mathbb{Z}_2^n$ is a function of S and R but not of b [17]. It can be show that in the context of distillation protocols, d can always be made zero [16].

Each S defines a total of 2^n orthogonal stabilizer states, one for each $b \in \mathbb{Z}_2^n$. As a consequence, all stabilizer states defined by S constitute a basis for $\mathcal{H}^{\otimes n}$, where $\mathcal{H}$ is the Hilbert space of one qubit. In the following, we will refer to this basis as the S-basis.

A Clifford operation Q, by definition, maps the Pauli group to itself under conjugation:

$$Q \sigma_a Q^\dagger = (-1)^\delta \sigma_b.$$

In the binary picture, a Clifford operation is represented by a matrix $C \in \mathbb{Z}_2^{2n \times 2n}$ and a vector $h \in \mathbb{Z}_2^{2n}$, where C is symplectic or $C^T P C = P$ [17]. The image of a Hermitian Pauli operator σ_a under the action of a Clifford operation is then given by $(-1)^\epsilon \sigma_{Ca}$, where ϵ is function of C, h and a. A Clifford operation that is entirely built of CNOT operations, is represented by [17]

$$C = \begin{bmatrix} A & 0 \\ 0 & A^{-T} \end{bmatrix}. \tag{3}$$

If a stabilizer state $|\psi\rangle$, represented by S and b, is operated on by a Clifford operation Q, represented by C and h, $Q|\psi\rangle$ is a new stabilizer state whose stabilizer is given by $Q\mathcal{S}Q^\dagger$. As a result, this stabilizer is represented by

$$\begin{array}{rcl} S' & = & CS \\ b' & = & b + f \end{array} \tag{4}$$

where f is independent of b and can always be made zero, by performing an extra Pauli operator before the Clifford operation [16].

Let $|\psi_1\rangle$ and $|\psi_2\rangle$ be two stabilizer states represented by $S_1 = \begin{bmatrix} S_{1(z)} \\ S_{1(x)} \end{bmatrix}, b_1$ and $S_2 = \begin{bmatrix} S_{2(z)} \\ S_{2(x)} \end{bmatrix}, b_2$ respectively. Then $|\psi_1\rangle \otimes |\psi_2\rangle$ is a stabilizer state represented by

$$\begin{bmatrix} S_{1(z)} & 0 \\ 0 & S_{2(z)} \\ S_{1(x)} & 0 \\ 0 & S_{2(x)} \end{bmatrix}, \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}. \tag{5}$$

Let Q_1 and Q_2 be two Clifford operations represented by $\left[\begin{array}{cc} A_1 & B_1 \\ C_1 & D_1 \end{array}\right]$ and $\left[\begin{array}{cc} A_2 & B_2 \\ C_2 & D_2 \end{array}\right]$ respectively, where all blocks are in $\mathbb{Z}_2^{n\times n}$. Then $Q_1 \otimes Q_2$ is a Clifford operation represented by

$$\left[\begin{array}{cccc} A_1 & 0 & B_1 & 0 \\ 0 & A_2 & 0 & B_2 \\ C_1 & 0 & D_1 & 0 \\ 0 & C_2 & 0 & D_2 \end{array}\right]. \tag{6}$$

A CSS state is a stabilizer state $|\psi\rangle$ whose stabilizer can be represented by

$$S = \left[\begin{array}{cc} S_z & 0 \\ 0 & S_x \end{array}\right],\ b \tag{7}$$

where $S_z \in \mathbb{Z}_2^{n\times n_z}$, $S_x \in \mathbb{Z}_2^{n\times n_x}$ and $n_z + n_x = n$. The stabilizer condition $S^T P S = 0$ is equivalent to $S_z^T S_x = 0$. As S is full rank, S_z and S_x are also full rank. Therefore, once S_z (or S_x) is known, we know S, up to right multiplication with some R.

If the phase factors $(-1)^{b_i}$, for $i = 1, \ldots, n$, of a CSS state represented by (7) are unknown, a σ_z measurement on every qubit reveals b_i, for $i = 1, \ldots, n_z$. Indeed, the measurements project the state on the joint eigenspace of observables $\sigma_z^{(j)} = I_2^{\otimes j-1} \otimes \sigma_z \otimes I_2^{\otimes n-j}$, for $j = 1, \ldots, n$, with eigenvalues $(-1)^{a_j}$ that are determined by the measurements. By linearity, we then have

$$b = \left[\begin{array}{c} S_z^T a \\ * \end{array}\right].$$

After the measurements, the state of each qubit j is no longer part of the original CSS state, but is the eigenstate of σ_z with eigenvalue $(-1)^{a_j}$. Therefore, the last n_x phase factors $*$ are lost due to the fact that all σ_{s_i}, for $i = n_z + 1, \ldots, n$, anticommute with at least one $\sigma_z^{(j)}$. On the other hand, by σ_x measurements on every qubit, with outcomes $(-1)^{a_j}$, we learn that

$$b = \left[\begin{array}{c} * \\ S_x^T a \end{array}\right].$$

4 Local permutations of products of CSS states

In this section, we consider n-qubit CSS states that are all represented by the same S. We have k states that are shared by n remote parties, each holding corresponding qubits of all k states. We study local Clifford operations (local with respect to the partition into n parties) that are identical and built of CNOTs. They result in a permutation of all 2^{nk} possible tensor products of such CSS states.

If $|\psi_i\rangle$ $(i = 1, \ldots, k)$ are represented by

$$S = \left[\begin{array}{cc} S_z & 0 \\ 0 & S_x \end{array}\right],\ b_i$$

according to (5), $|\psi_1\rangle \otimes \ldots \otimes |\psi_k\rangle$ is represented by

$$\left[\begin{array}{cc} I_k \otimes S_z & 0 \\ 0 & I_k \otimes S_x \end{array}\right],\ \tilde{b}' = \left[\begin{array}{c} b_1 \\ \vdots \\ b_k \end{array}\right].$$

However, since it is more convenient to arrange all qubits per party, we rewrite the stabilizer matrix by permuting rows and columns as

$$\left[\begin{array}{cc} S_z \otimes I_k & 0 \\ 0 & S_x \otimes I_k \end{array}\right] = S \otimes I_k,\ \tilde{b} \tag{8}$$

where the entries of $\tilde{b}'$ are permuted appropriately into $\tilde{b} \in \mathbb{Z}_2^{nk}$. All parties perform identical local Clifford operations, built of CNOTs. According to (3) and (6), the overall Clifford operation is generally represented by

$$\left[\begin{array}{cc} I_n \otimes A & 0 \\ 0 & I_n \otimes A^{-T} \end{array} \right], \tag{9}$$

where $A \in \mathbb{Z}_2^{k \times k}$ is invertible.

The local Clifford operations acting on the given state result in a permutation of all 2^{nk} possible tensor products (defined by $\tilde{b}$) if and only if the resulting stabilizer matrix can be transformed into the original form of (8) by multiplication with an invertible $R \in \mathbb{Z}_2^{nk \times nk}$ on the right, or

$$\left[\begin{array}{cc} I_n \otimes A & 0 \\ 0 & I_n \otimes A^{-T} \end{array} \right] (S \otimes I_k) R = S \otimes I_k. \tag{10}$$

Using (2) and (4), the corresponding permutation of the tensor products is then defined by the transformation

$$\tilde{b} \mapsto R^T \tilde{b}. \tag{11}$$

It is easily verified that (10) holds for

$$R = \left[\begin{array}{cc} I_{n_z} \otimes A^{-1} & 0 \\ 0 & I_{n_x} \otimes A^T \end{array} \right]. \tag{12}$$

5 Protocol

In this section, we show how the hashing protocol for CSS states is carried out. As noted in section 3, all 2^n stabilizer states represented by the same $S \in \mathbb{Z}_2^{2n \times n}$ constitute a basis for $\mathcal{H}^{\otimes n}$, which we call the S-basis. The protocol starts with k identical copies of a mixed state ρ that is diagonal in this basis. This mixed state could for instance be the result of distributing k copies of a pure CSS state, represented by S and $b = 0$, via imperfect quantum channels. If ρ is not diagonal in the S-basis, it can always be made that way by performing a local POVM [13]. We have

$$\rho = \sum_{b \in \mathbb{Z}_2^n} p(b) |\psi_b\rangle\langle\psi_b|,$$

where $|\psi_b\rangle$ is the CSS state represented by S and b. The mixed state ρ can be regarded as a statistical ensemble of pure states $|\psi_b\rangle$ with probabilities $p(b)$. Consequently, k copies of ρ are an ensemble of pure states represented by (8) with probabilities

$$p(\tilde{b}) = p(\tilde{b}') = \prod_{i=1}^{k} p(b_i). \tag{13}$$

Recall that the entries of $\tilde{b}$ correspond to the nk phase factors ordered per party instead of per copy like $\tilde{b}'$.

The protocol now consists of the following steps (this is schematically depicted in figure 2):

1. Each party applies local Clifford operations (9) that result in the transformation (11) of $\tilde{b}$. Consequently, all 2^{nk} tensor products represented by the 2^{nk} different $\tilde{b}$ in the ensemble are permuted.

2. A fraction mk of all k copies are measured locally. These copies are divided in two sets with $m_z k$ and $m_x k$ copies respectively ($m_z + m_x = m$). Each of the n parties performs a σ_z measurement on every qubit they have of the first set of copies, and a σ_x measurement on every qubit of the second set.

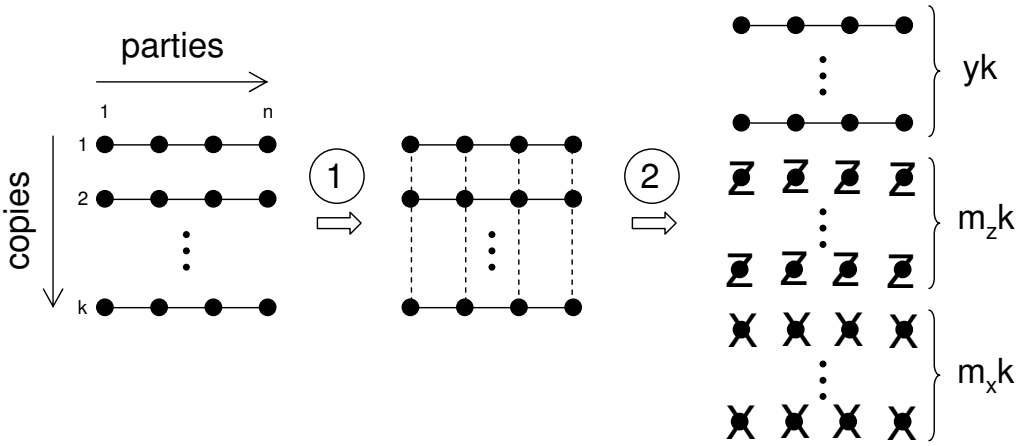

Figure 2: in the first step, local Clifford operations (local with respect to the parties) result in statistically dependent copies. In the second step, some of the copies are measured, providing information on the global state. Afterwards, the measured copies are separable.

The local Clifford operations result in a permutation $\tilde{b} \mapsto R^T \tilde{b}$ of all tensor products such that the ensembles of the different copies become statistically dependent. The measurements provide information on the overall state. The measurement outcomes should contain as much information as possible. Therefore, the outcome probabilities should be uniform. It will be shown in the next section that this is achieved by randomly picking an element of the set of all possible R given by (12). The goal of the protocol is to collect enough information for the $(1-m)k$ remaining copies to approach a pure state (i.e. zero entropy). The yield $\gamma = 1 - m$ of the protocol is the fraction of pure states that are distilled out of k copies, if k goes to infinity.

A way of looking at the ensemble is to regard it as an unknown pure state. The probability that the state is represented by $\tilde{b}$ is then equal to $p(\tilde{b})$. Suppose the unknown pure state is represented by $\tilde{u}$. With probability ≈ 1, $\tilde{u}$ is contained in the set $\mathcal{T}_\epsilon^{(k)}$, defined as in section 2. Here, Ω is the set of all $b \in \mathbb{Z}_2^n$. So with negligible error probability, we may assume that $\tilde{u} \in \mathcal{T}_\epsilon^{(k)}$. After each measurement, we eliminate every $\tilde{b} \in \mathcal{T}_\epsilon^{(k)}$ that is inconsistent with the measurement outcome. The protocol ends when all $\tilde{b} \neq \tilde{u}$ are eliminated from $\mathcal{T}_\epsilon^{(k)}$ and only $\tilde{u}$ is left.

In the next section, we will calculate the yield of the protocol as the solution of the following linear programming problem: $\gamma = 1 - m$, where m is the solution to

$$\begin{array}{ll} \text{minimize} & m = m_z + m_x \\ \text{subject to} & d_z m_z + d_x m_x \geq H - H_{[d_z,d_x]}, \\ & \text{for all } [d_z, d_x] \neq [0,0] \text{ where } 0 \leq d_z \leq n_z \text{ and } 0 \leq d_x \leq n_x. \end{array}$$

H is the entropy of the initial mixed state, or

$$H = -\sum_{b \in \mathbb{Z}_2^n} p(b) \log_2 p(b).$$

The calculation of $H_{[d_z,d_x]}$ is more involved. Define the subspace $\mathcal{J}^\perp = \{w \in \mathbb{Z}_2^n | J^T w = 0\}$ of $\mathbb{Z}_2^n$, where J is a matrix with n rows and defined below. The cosets Ω_j $(j = 1, \ldots, q)$ of this subspace constitute a partition of $\mathbb{Z}_2^n$. This partition has entropy

$$H_{\mathcal{J}^\perp} = -\sum_{j=1}^{q} p(\Omega_j) \log_2 p(\Omega_j).$$

Now $H_{[d_z,d_x]}$ is defined as follows:

$$\min_{\mathcal{G}_z, \mathcal{G}_x} H_{\mathcal{J}^\perp},$$

where the minimum is taken over all subspaces $\mathcal{G}_z$ of $\mathbb{Z}_2^{n_z}$ with dimension $n_z - d_z$ and subspaces $\mathcal{G}_x$ of $\mathbb{Z}_2^{n_x}$ with dimension $n_x - d_x$. The matrix J that defines $\mathcal{J}^\perp$ is function of $\mathcal{G}_z$ and $\mathcal{G}_x$ as follows: let $G_z \in \mathbb{Z}_2^{n_z \times (n_z - d_z)}, G_x \in \mathbb{Z}_2^{n_x \times (n_x - d_x)}$ be matrices whose column spaces are $\mathcal{G}_z, \mathcal{G}_x$ respectively. Then we have

$$J = \begin{bmatrix} G_z & 0 \\ 0 & G_x \end{bmatrix}.$$

6 Calculating the yield

This section is organized as follows. In the first subsection we show that the outcome probabilities of each measurement are uniform. This is used to calculate the probability that some $\tilde{b} \neq \tilde{u}$ is not eliminated after all measurements. In the second subsection we then calculate the minimal number of measurements needed to eliminate all $\tilde{b} \neq \tilde{u}$. This is stated as a linear programming problem.

6.1 Elimination probability

We will first calculate the probability that some $\tilde{b} \neq \tilde{u}$ is not eliminated after one σ_z measurement on the i-th copy. As explained in section 3, this reveals

$$z_j = (R^T \tilde{u})_{(j-1)k+i}, \text{ for } j = 1, \ldots, n_z,$$

while

$$x_j = (R^T \tilde{u})_{(n_z+j-1)k+i}, \text{ for } j = 1, \ldots, n_x,$$

are lost. For a σ_x measurement, it is the other way around. If and only if $(R)^T_{(j-1)k+i}(\tilde{b} + \tilde{u}) = 0$ for $j = 1, \ldots, n_z$, then $\tilde{b}$ is not eliminated. For the measurement outcome, we are only interested in the i-th column of A^{-1}, which we call a. From the randomness of R, it follows that a is uniformly distributed over all possibilities. These are the elements of $\mathbb{Z}_2^k$ (we neglect the possibility that $a = 0$).

We define the matrix $V_z \in \mathbb{Z}_2^{nk \times n_z}$ with columns $(V_z)_j = (R)_{(j-1)k+i}$, for $j = 1, \ldots, n_z$, or

$$V_z = \begin{bmatrix} I_{n_z} \otimes a \\ 0 \end{bmatrix},$$

and $\mathcal{V}_z$ as the set containing all possible values of V_z, which is uniformly distributed too. Note that $\mathcal{V}_z$ is a vector space, because V_z is a linear function of a. Let $\Delta\tilde{b} = \tilde{b} + \tilde{u}$ and $\Delta z = V_z^T \Delta\tilde{b}$. For some fixed $\Delta\tilde{b}$, all values $\Delta z \in \mathcal{Z} = \{V_z^T \Delta\tilde{b} \mid V_z \in \mathcal{V}_z\}$ are equiprobable. Indeed, all cosets of the kernel of the linear map $\mathcal{V}_z \mapsto \mathcal{Z} : V_z \mapsto \Delta z = V_z^T \Delta\tilde{b}$ have the same number of elements. Let $d_z \leq n_z$ be the dimension of the range $\mathcal{Z}$ of this map. Then we have 2^{d_z} possible equiprobable Δz for some fixed $\Delta\tilde{b}$. Only when $\Delta z = 0$, which happens with probability 2^{-d_z}, $\tilde{b}$ is not eliminated from $\mathcal{T}_\epsilon^{(k)}$ by the first measurement. The same reasoning can be done for a σ_x measurement. Note that $d_z = d_x = 0$ only holds for $\tilde{u}$ itself.

6.2 Minimal number of measurements

So far we have given an information-theoretical interpretation of the protocol: we start with an unknown pure state (represented by $\tilde{u}$), which is almost certainly contained in $\mathcal{T}_\epsilon^{(k)}$. Consecutive measurements rule out all inconsistent $\tilde{b} \in \mathcal{T}_\epsilon^{(k)}$. The probability that a particular $\tilde{b} \neq \tilde{u}$ survives this process is $2^{-k(d_z m_z + d_x m_x)}$. Consequently, the probability that any $\tilde{b} \neq \tilde{u}$ survives the proces is equal to

$$\sum_{[d_z, d_x] \neq [0,0]}^{[n_z, n_x]} N^*_{[d_z, d_x]} 2^{-k(d_z m_z + d_x m_x)} \tag{14}$$

where $N^*_{[d_z,d_x]}$ is the number of $\tilde{b} \in \mathcal{T}_\epsilon^{(k)}$ for which $\mathcal{Z}$ has dimension $= d_z$ and $\mathcal{X}$ has dimension $= d_x$. Let $N^*_{[d_z,d_x]} \approx 2^{k\alpha^*_{[d_z,d_x]}}$. Then (14) vanishes if and only if the following inequalities hold:

$$d_z m_z + d_x m_x \geq \alpha^*_{[d_z,d_x]}, \text{ for all } [d_z, d_x] \neq [0,0]. \tag{15}$$

Let $N_{[d_z,d_x]} \approx 2^{k\alpha_{[d_z,d_x]}}$ be the number of $\tilde{b} \in \mathcal{T}_\epsilon^{(k)}$ for which $\mathcal{Z}$ has dimension $\leq d_z$ and $\mathcal{X}$ has dimension $\leq d_x$. Evidently,

$$N_{[d_z,d_x]} = \sum_{d'_z \leq d_z, d'_x \leq d_x} N^*_{[d'_z,d'_x]}. \tag{16}$$

It can be verified that the inequalities

$$d_z m_z + d_x m_x \geq \alpha_{[d_z,d_x]}, \text{ for all } [d_z, d_x] \neq [0,0], \tag{17}$$

are equivalent to (15). Indeed, it follows from (16) that $\alpha_{[d_z,d_x]} \approx \alpha_{[d'_z,d'_x]} \approx \alpha^*_{[d'_z,d'_x]}$ for some $d'_z \leq d_z$ and $d'_x \leq d_x$. Since $d'_z m_z + d'_x m_x \geq \alpha^*_{[d'_z,d'_x]} \approx \alpha_{[d'_z,d'_x]} \approx \alpha_{[d_z,d_x]}$ implies $d_z m_z + d_x m_x \geq \alpha_{[d_z,d_x]}$, a solution to (17) is also a solution to (15) and vice versa.

This leaves us to calculate $N_{[d_z,d_x]}$. Let $G_z \in \mathbb{Z}_2^{n_z \times (n_z - d_z)}$ be a full rank matrix with column space $\mathcal{G}_z$. We define the space $\mathcal{W}_z(\mathcal{G}_z) = \{V_z G_z \mid V_z \in \mathcal{V}_z\}$. Then all elements of $\mathcal{W}_z(\mathcal{G}_z)^\perp = \{\Delta\tilde{b} \in \mathbb{Z}_2^{nk} \mid W_z^T \Delta\tilde{b} = 0, \ \forall W_z \in \mathcal{W}_z(\mathcal{G}_z)\}$ correspond to a $\mathcal{Z}$ with dimension $\leq d_z$, as $G_z^T \Delta z = W_z^T \Delta\tilde{b} = 0, \ \forall \Delta z \in \mathcal{Z}$. We then have

$$N_{[d_z,d_x]} = \mid \bigcup_{\mathcal{G}_z, \mathcal{G}_x} \mathcal{W}_z(\mathcal{G}_z)^\perp \cap \mathcal{W}_x(\mathcal{G}_x)^\perp \cap \mathcal{T}_\epsilon^{(k)} \mid$$

where $\mathcal{G}_z$ and $\mathcal{G}_x$ run through all subspaces of $\mathbb{Z}_2^{n_z}$ and $\mathbb{Z}_2^{n_x}$ with dimension $n_z - d_z$ and $n_x - d_x$ respectively. It follows that

$$N_{[d_z,d_x]} = r \max_{\mathcal{G}_z, \mathcal{G}_x} |\mathcal{W}_z(\mathcal{G}_z)^\perp \cap \mathcal{W}_x(\mathcal{G}_x)^\perp \cap \mathcal{T}_\epsilon^{(k)}|,$$

where $1 \leq r \leq$ the total number of combinations $(\mathcal{G}_z, \mathcal{G}_x)$, which is independent of k. Therefore, $r = O(1)$.

We now calculate $|\mathcal{W}_z(\mathcal{G}_z)^\perp \cap \mathcal{W}_x(\mathcal{G}_x)^\perp \cap \mathcal{T}_\epsilon^{(k)}|$. We have $W_z^T \Delta\tilde{b} = 0 \Leftrightarrow G_z^T V_z^T \Delta\tilde{b} = 0 \Leftrightarrow G_z^T (I_{n_z} \otimes a^T) \Delta\tilde{b} = 0 \Leftrightarrow (G_z^T \otimes a^T) \Delta\tilde{b} = 0$. As a can be any vector in $\mathbb{Z}_2^k$, it follows that $\Delta\tilde{b} \in \mathcal{W}_z(\mathcal{G}_z)^\perp \cap \mathcal{W}_x(\mathcal{G}_x)^\perp$ if and only if

$$\left(\begin{bmatrix} G_z & 0 \\ 0 & G_x \end{bmatrix}^T \otimes I_k \right) \Delta\tilde{b} = (J^T \otimes I_k) \Delta\tilde{b} = 0.$$

We have found that

$$|\mathcal{W}_z(\mathcal{G}_z)^\perp \cap \mathcal{W}_x(\mathcal{G}_x)^\perp \cap \mathcal{T}_\epsilon^{(k)}| = |\{\tilde{b} \in \mathcal{T}_\epsilon^{(k)} | (J^T \otimes I_k) \Delta\tilde{b} = 0\}|.$$

Note that $(J^T \otimes I_k) \Delta\tilde{b} = 0$ is equivalent to $(I_k \otimes J^T) \Delta\tilde{b}' = 0$, or $J^T \Delta b_i = 0$, for $i = 1, \ldots, k$. The cosets Ω_j $(j = 1, \ldots, q)$ of the space $\mathcal{J}^\perp = \{w \in \mathbb{Z}_2^n | J^T w = 0\}$ constitute a partition of $\mathbb{Z}_2^n$. We want to know the number of $\tilde{b} \in \mathcal{T}_\epsilon^{(k)}$ for which b_i is in the same coset as u_i, for all $i = 1, \ldots, k$. We know from section 2 that this number is approximately

$$2^{k[H - H_{\mathcal{J}^\perp}]} \quad \text{where} \quad H = -\sum_{b \in \mathbb{Z}_2^n} p(b) \log_2 p(b)$$
$$\text{and} \quad H_{\mathcal{J}^\perp} = -\sum_{j=1}^{q} p(\Omega_j) \log_2 p(\Omega_j).$$

Choose $\mathcal{G}_z$ (with dimension $n_z - d_z$) and $\mathcal{G}_x$ (with dimension $n_x - d_x$) such that $H_{\mathcal{J}^\perp}$ is minimal. We denote this minimum by $H_{[d_z,d_x]}$. Then it follows that

$$N_{[d_z,d_x]} \approx 2^{k[H - H_{[d_z,d_x]}]}.$$

7 An example

In this section we illustrate the hashing protocol with an example. The 4-qubit cat state (also called GHZ state) is the state

$$\frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)$$

which is stabilized by

$$\begin{gathered}\sigma_z \otimes I_2 \otimes I_2 \otimes \sigma_z \\ I_2 \otimes \sigma_z \otimes I_2 \otimes \sigma_z \\ I_2 \otimes I_2 \otimes \sigma_z \otimes \sigma_z \\ \sigma_x \otimes \sigma_x \otimes \sigma_x \otimes \sigma_x\end{gathered}$$

and thus represented by

$$S_z = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix},\ S_x = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \text{ and } b = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

We formulate the linear programming problem to calculate the yield of the protocol. At the start, the 4 parties share k copies of a state

$$\rho = \sum_{b \in \mathbb{Z}_2^4} p_b |\psi_b\rangle\langle\psi_b|,$$

where $|\psi_b\rangle = \frac{1}{\sqrt{2}}(|b_1, b_2, b_3, 0\rangle + (-1)^{b_4}|b_1+1, b_2+1, b_3+1, 1\rangle)$. We calculate $H_{[d_z,d_x]}$ for different values of d_z, d_x. Evidently, $H_{[3,1]} = H_{[n_z,n_x]} = 0$. It is also easily verified that

$$H_{[0,1]} = -\sum_{b_{123} \in \mathbb{Z}_2^3} (\sum_{b_4 \in \mathbb{Z}_2} p_b) \log_2 (\sum_{b_4 \in \mathbb{Z}_2} p_b).$$

In both cases $d_z = 1$ and $d_z = 2$, we have to calculate $H_{\mathcal{J}^\perp}$ for seven different subspaces $\mathcal{J}^\perp$, and take the minimum. For $d_z = 1$, we run through

$$G_z = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

For $d_z = 2$, we run through

$$G_z = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}.$$

As an example, let $d_z = 1, d_x = 1$ and

$$G_z = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

The cosets of $\mathcal{J}^\perp$ are then:

$$\{\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}\}, \quad \{\begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}\},$$

$$\{\begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}\}, \quad \{\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}\}.$$

For this example, we have compared our protocol to those of [14, 15]. We start with copies of the 4-qubit cat state, prepared by the first party. The second, third and fourth qubit of each copy is sent through identical depolarizing channels to the corresponding parties. The action of each channel is

$$\rho \mapsto F\rho + \frac{1-F}{3}(\sigma_x\rho\sigma_x^\dagger + \sigma_y\rho\sigma_y^\dagger + \sigma_z\rho\sigma_z^\dagger).$$

and we call F the fidelity of the channels. It can be verified that this yields a mixture with probabilities:

$$\begin{bmatrix} p_{0000} \\ p_{0001} \\ p_{0010} \\ p_{0011} \\ p_{0100} \\ p_{0101} \\ p_{0110} \\ p_{0111} \\ p_{1000} \\ p_{1001} \\ p_{1010} \\ p_{1011} \\ p_{1100} \\ p_{1101} \\ p_{1110} \\ p_{1111} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 3 & 0 \\ 0 & 3 & 0 & 1 \\ 0 & 1 & 2 & 1 \\ 0 & 1 & 2 & 1 \\ 0 & 1 & 2 & 1 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \\ 0 & 1 & 2 & 1 \end{bmatrix} \begin{bmatrix} F^3 \\ F^2\frac{1-F}{3} \\ F\left(\frac{1-F}{3}\right)^2 \\ \left(\frac{1-F}{3}\right)^3 \end{bmatrix}.$$

The yield of our protocol for this example is plotted as a function of the fidelity of the channels in figure 3. So is the yield of the protocol of [14]:

$$1 - \max_{j=1,2,3}[H(b_j)] - H(b_4)$$

and the yield of the improved protocol of [15]:

$$\max \quad \Big(1 - \max_{j=1,2,3}[H(b_j)] - H(b_4|b_1,b_2,b_3), \\ 1 - \max_{j=1,2,3}[H(b_j|b_4)] - H(b_4)\Big).$$

8 Conclusion

We have presented a hashing protocol to distill multipartite CSS states, an important class of stabilizer states. Starting with k copies of a mixed state that is diagonal in the S-basis, the protocol consists of local Clifford operations that result in a permutation of all 2^{nk} tensor products of CSS states, followed by Pauli measurements that extract information on the global state. With the aid of the information-theoretical notion of a strongly typical set, it is possible to calculate the minimal number of copies that have to be measured in order to end up with copies of a pure CSS state, for k approaching infinity. As a result, the yield of the protocol is formulated as the solution of a linear programming problem.

This research is funded by a Ph.D. grant of the Institute for the Promotion of Innovation through Science and Technology in Flanders (IWT-Vlaanderen). Dr. Bart De Moor is a full professor at the Katholieke Universiteit Leuven, Belgium. Research supported by Research Council KUL: GOA AMBioRICS, CoE EF/05/006 Optimization in Engineering, several PhD/postdoc & fellow grants; Flemish Government: FWO: PhD/postdoc grants, projects, G.0407.02 (support vector machines), G.0197.02 (power islands), G.0141.03 (Identification and cryptography),

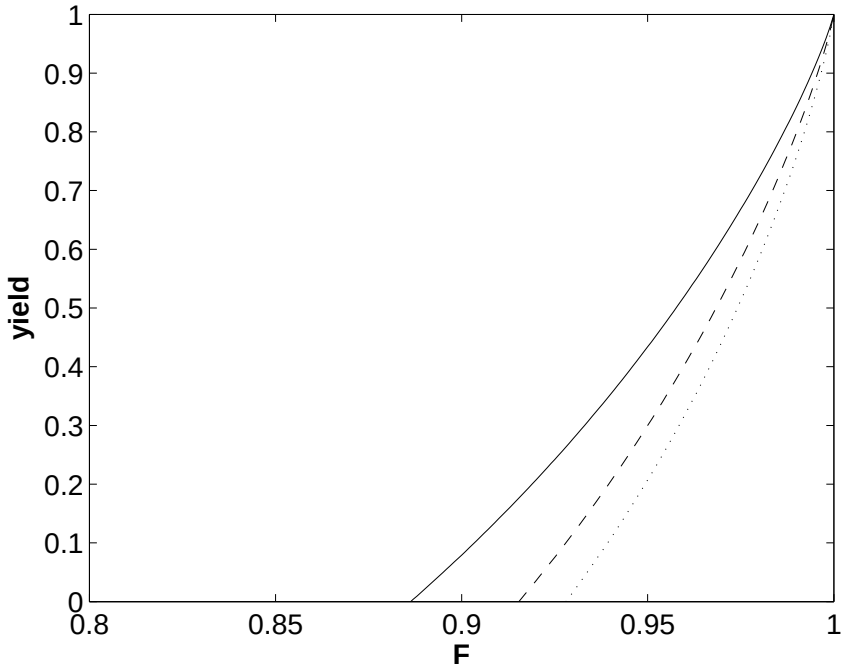

Figure 3: comparison of different protocols for the given cat state example. The dotted line gives the yield of the protocol of [14], the dashed line of that of [15] and the solid line of our protocol, as a function of the fidelity F of the depolarizing channels.

G.0491.03 (control for intensive care glycemia), G.0120.03 (QIT), G.0452.04 (new quantum algorithms), G.0499.04 (Statistics), G.0211.05 (Nonlinear), G.0226.06 (cooperative systems and optimization), G.0321.06 (Tensors), G.0553.06 (VitamineD), research communities (ICCoS, ANMMM, MLDM); IWT: PhD Grants, GBOU (McKnow), Eureka-Flite2; Belgian Federal Science Policy Office: IUAP P5/22 ('Dynamical Systems and Control: Computation, Identification and Modelling', 2002-2006) ; PODO-II (CP/40: TMS and Sustainability); EU: FP5-Quprodis; ERNSI; Contract Research/agreements: ISMC/IPCOS, Data4s, TML, Elia, LMS, Mastercard.

References

[1] C.H. Bennett, G. Brassard, C. Crépeau, R. Josza, A. Peres, and W.K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70:1895, 1993.

[2] C.H. Bennett and S.J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.*, 69:2881, 1992.

[3] A. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67:661, 1991.

[4] D. Gottesman. *Stabilizer Codes and Quantum Error Correction*. PhD thesis, Caltech, 1997. quant-ph/9705052.

[5] D. Gottesman. A theory of fault-tolerant quantum computation. *Phys. Rev. A*, 57:127, 1998.

[6] W. Dür, J. Calsamiglia, and H.-J. Briegel. Multipartite secure state distribution. *Phys. Rev. A*, 71:042336, 2005.

[7] A. Karlsson, M. Koashi, and N. Imoto. Quantum entanglement for secret sharing and secret splitting. *Phys. Rev. A*, 59:162, 1999.

[8] M. Hillery, V. Buzek, and A. Berthiaume. Quantum secret sharing. *Phys. Rev. A*, 59:1829, 1999.

[9] R. Cleve, D. Gottesman, and H.-K. Lo. How to share a quantum secret. *Phys. Rev. Lett.*, 83:648, 1999.

[10] C. Crépeau, D. Gottesman, and A. Smith. Secure multi-party quantum computing. In *Proc. STOC*, 2002. quant-ph/0206138.

[11] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters. Mixed-state entanglement and quantum error correction. *Phys. Rev. A*, 54:3824, 1996.

[12] W. Dür, H. Aschauer, and H.-J. Briegel. Multiparticle entanglement purification for graph states. *Phys. Rev. Lett.*, 91:107903, 2003.

[13] H. Aschauer, W. Dür, and H.-J. Briegel. Multiparticle entanglement purification for two-colorable graph states. *Phys. Rev. A*, 71:012319, 2005.

[14] E.N. Maneva and J.A. Smolin. Improved two-party and multi-party purification protocols. quant-ph/0003099.

[15] K. Chen and H.-K. Lo. Multi-partite quantum cryptographic protocols with noisy GHZ states. quant-ph/0404133.

[16] E. Hostens, J. Dehaene, and B. De Moor. Hashing protocol for distilling multipartite Calderbank-Shor-Steane states. *Phys. Rev. A*, 73:042316, 2006.

[17] J. Dehaene and B. De Moor. The Clifford group, stabilizer states, and linear and quadratic operations over GF(2). *Phys. Rev. A*, 68:042318, 2003.

[18] T.M. Cover and J.A. Thomas. *Elements of Information Theory.* John Wiley & Sons, Inc., 1991.