International Journal of Engineering, Mathematical and Physical Sciences
ISSN: 2517-9934
Vol:3, No:9, 2009

Entanglement-based Quantum Computing by Diagrams of States

Sara Felloni and Giuliano Strini

Abstract—We explore entanglement in composite quantum systems and how its peculiar properties are exploited in quantum information and communication protocols by means of *Diagrams of States*, a novel method to graphically represent and analyze how quantum information is elaborated during computations performed by quantum circuits.
We present quantum diagrams of states for Bell states generation, measurements and projections, for dense coding and quantum teleportation, for probabilistic quantum machines designed to perform approximate quantum cloning and universal NOT and, finally, for quantum privacy amplification based on entanglement purification.
Diagrams of states prove to be a useful approach to analyze quantum computations, by offering an intuitive graphic representation of the processing of quantum information. They also help in conceiving novel quantum computations, from describing the desired information processing to deriving the final implementation by quantum gate arrays.

Keywords—Diagrams of states, entanglement, quantum circuits, quantum information.

I. Introduction

WE explore entanglement in composite quantum systems and how its peculiar properties are exploited in quantum information and communication protocols by means of *Diagrams of States*. The representation by diagrams of states is a novel method to graphically represent and analyze how quantum information is elaborated during computations performed by quantum circuits. In the widely-used representation by quantum circuits, horizontal lines represent single qubits constituting the considered quantum system. In contrast, in diagrams of states we draw a horizontal line for each state of the computational basis. Therefore, diagrams of states are less synthetic in respect to quantum circuits, but allow a clear and straightforward visualization of the quantum information processing.

We previously introduced this method by defining basic representations for standard quantum operations and providing examples of basic practical quantum computations [1]. Subsequently, we applied this representation to investigate the main processes involved in the evolution of quantum systems, also developing a general description of single-qubit decoherence channels [2]. In this paper, diagrams of states are applied to explore the properties and applications of entanglement in quantum information and communication, from generation, measurement and distillation of maximally entangled states, to quantum teleportation, dense coding, approximate cloning and approximate universal NOT. As in previous related works [1], [2], [3], diagrams of states will be used both as a novel approach to investigate quantum computations, in addition to (or in substitution of) standard methods like analytical study and representation by quantum circuits, and as an auxiliary tool to construct novel quantum computations from the desired manipulation of quantum states.

This paper is organized as follows. In Section II we illustrate by diagrams of states the basic processes related to maximally entangled two-qubit states: generation of Bell states, measurement in the Bell basis and projections into Bell states. In Section III we investigate by diagrams of states two of the most renowned applications of entanglement to quantum information, that is, quantum teleportation and dense coding. In Section IV we describe two probabilistic quantum machines which deal with basic limitations of quantum mechanics by approximately processing the two forbidden operations of general quantum cloning and universal NOT. In Section V, diagrams of states are used to investigate the processing of information performed by an entanglement purification procedure [4], which offers useful applications in both quantum cryptography and quantum communication. Finally, in Section VI we present our conclusions.

Throughout this paper, in order to perform the analysis of given quantum processes, we shall directly derive diagrams of states from the quantum circuits associated with the physical implementation of the processes. These diagrams can easily be rearranged into new simpler diagrams, which better visualize the overall manipulation of information from input to output: We shall refer to the former as *complete* diagrams and to the latter as *simplified* diagrams.

Any sequence of logic gates must be read from left (input) to right (output), both for conventional quantum circuits and for their representations by means of diagrams of states. From top to bottom, qubits run from the least significant (LSB) to the most significant (MSB).

II. Maximally Entangled States

Entanglement is a fundamental resource for quantum information processing, often exploited in order to perform computational and communication tasks otherwise impossible for classical systems.

Prototypical instances of entangled states are the so-called Bell states [5], defined as maximally entangled states of two qubits:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\{\,|00\rangle + |11\rangle\},$$

S. Felloni is a postdoctoral fellow at the Department of Electronics and Telecommunications (IET), Norwegian University of Science and Technology (NTNU), NO-7491, Trondheim, NO, and UNIK - University Graduate Center, NO-2027 Kjeller, NO; *sara.felloni@iet.ntnu.no*; *www.sarafelloni.com*.

G. Strini is associated professor in experimental physics at the Department of Physics, University of Milan, 20133 Milano, IT; *giuliano.strini@mi.infn.it*.

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}\{|00\rangle - |11\rangle\}.$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}\{|01\rangle + |10\rangle\},$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\{|01\rangle - |10\rangle\}, \quad (1)$$

Even when spatially separated, Bell states exhibit perfect, non-classical correlations. In this section, we illustrate and explore the generation of Bell states, the measurement in the Bell basis and the projections into Bell states.

A. Bell States Generation

Starting from the two-qubit computational basis states $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$, Bell states can be synthesized by means of the quantum circuit in Figure 1 (left), whose overall transformation is described by the operator:

$$B = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 1 \\ 1 & -1 & 0 & 0 \end{bmatrix}. \quad (2)$$

Applying the operator B to each one of the four states of the computational basis, we obtain in output the corresponding Bell states: $|00\rangle \rightarrow |\Phi^+\rangle$, $|01\rangle \rightarrow |\Phi^-\rangle$, $|10\rangle \rightarrow |\Psi^+\rangle$ and $|11\rangle \rightarrow -|\Psi^-\rangle$.

The process to generate Bell states is graphically illustrated by the diagrams of states in Figure 2. Requiring no further analytical study, each one of the four diagrams shows in output the Bell state determined by the computational state chosen in input. Starting from the input state, the active information is contained in diagram lines highlighted by a thick pattern, while thin lines correspond to absence of information. From left to right, the active information is the processed along thick lines, until the desired Bell state is obtained in output at the rightmost end of the diagram. We shall adopt this graphic notation in all the diagrams of states contained in this paper.

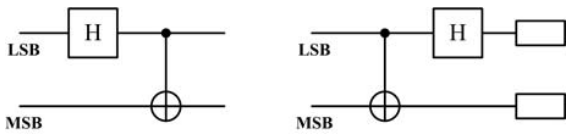

Fig. 1. Quantum circuits representing Bell states generation (left) and measurement in respect to Bell basis (right).

B. Bell Measurements

Bell measurements, that is, measurements in respect to the basis constituted by Bell states, are a set of joint quantum-mechanical two-qubit measurements, performed to determine the probability that a two-qubit state is one of the four Bell states.

Bell measurements can be represented in the computational basis by applying a process inverse to Bell states generation. Thus, we now require the quantum circuit illustrated in Figure 1 (right), whose overall transformation is described by the operator $B^\dagger$, conjugate to the operator B:

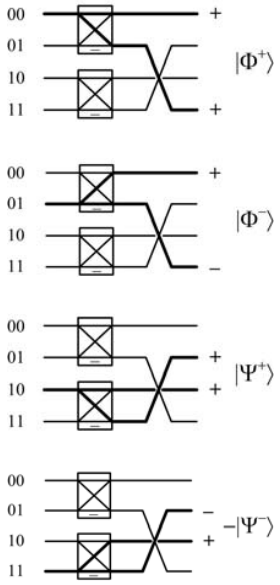

Fig. 2. Diagrams of states representing Bell states generation, corresponding to the quantum circuit of Figure 1 (left). Starting from the input state, active information is processed along thick lines, while thin lines correspond to absence of information. The desired Bell states are obtained in output at the rightmost end of each diagram (since an arbitrary quantum state is defined by neglecting a common phase, the "-1" factor does not affect the generation of the Bell state $|\Psi^-\rangle$).

$$B^\dagger = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \\ 0 & -1 & 1 & 0 \end{bmatrix}. \quad (3)$$

Applying the operator $B^\dagger$ to each one of the four Bell states, we obtain in output the corresponding computational basis states: $|\Phi^+\rangle \rightarrow |00\rangle$, $|\Phi^-\rangle \rightarrow |01\rangle$, $|\Psi^+\rangle \rightarrow |10\rangle$ and $|\Psi^-\rangle \rightarrow -|11\rangle$.

The process to perform Bell measurements is graphically illustrated by the diagrams of states in Figure 3. Requiring no further analytical study, each one of the four diagrams shows in output the computational state determined by the Bell state chosen in input. All diagrams of states clearly visualize the fundamental role played by the constructive and destructive interference caused by the Hadamard gates on diagram lines containing active information.

C. Bell Projections

A Bell projection consists in the process of projecting into a Bell state a general two-qubit state which is not maximally entangled before the measurement, as a consequence of the wave-function collapse. Thus, Bell projections can be considered as probabilistic extractions of maximally entangled states from less entangled states.

Bell projections can be achieved by means of the quantum circuit and diagrams of states illustrated in Figures 4-6. Two

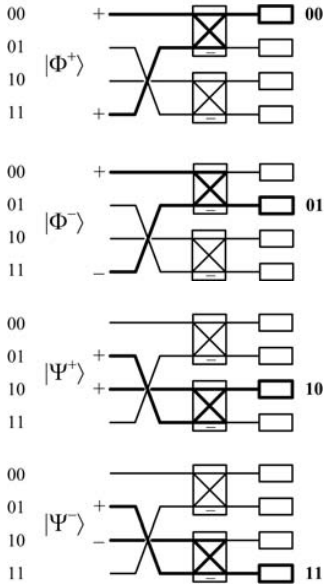

Fig. 3. Diagrams of states representing Bell measurements, corresponding to the quantum circuit of Figure 1 (right). Starting from the input state, active information is processed along thick lines. In each diagram, constructive and destructive interference caused by the Hadamard gates gives in output the desired computational basis state.

ancillary qubits are added in the most significant positions to the initial two-qubit state, which is to be projected into one of the Bell states. After applying the sequence of operations represented in Figure 4, each projection in the corresponding Bell state is determined by the measurement result of the two ancillary qubits. The diagrams of states clearly visualize the four possible Bell projections determined by the four possible measurement results. Requiring no further analytical study, projections are obtained as results of the four active information patterns, determined by constructive and destructive interference caused by the Hadamard gates.

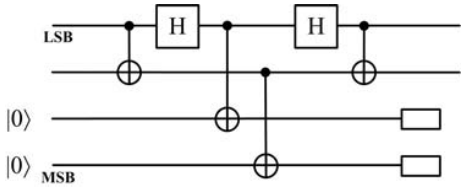

Fig. 4. Quantum circuit representing projections into Bell states. At the rightmost end of the circuit, the measurement results determine the output state as a consequence of the wave-function collapse.

III. Quantum Teleportation and Dense Coding

Quantum teleportation is one of the most renowned applications of quantum entanglement to information processing (see, *e.g.*, [6], pages 208-211): Entangled states act as a quantum communication channel and quantum information is transferred by actually transmitting only classical information. Teleportation plays a very important role in several

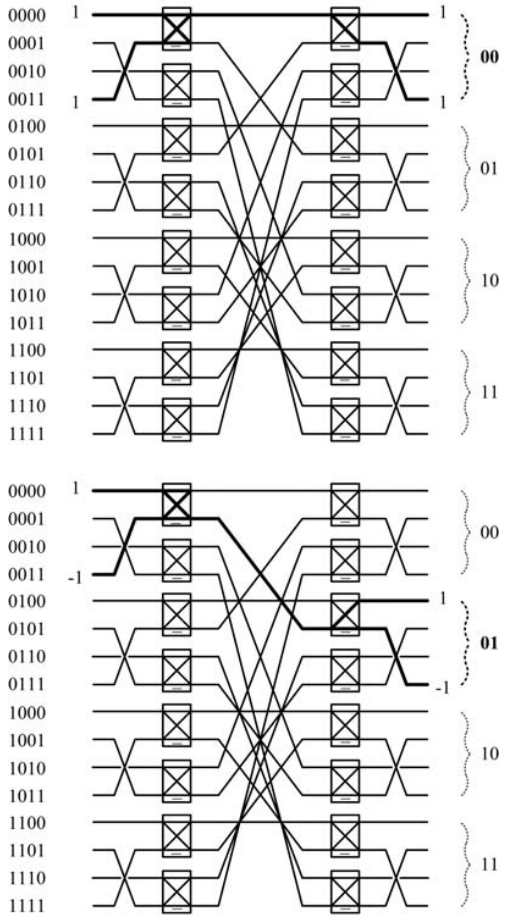

Fig. 5. Diagrams of states representing projections into Bell states, corresponding to the quantum circuit of Figure 4. The diagrams show the projections in the Bell state respectively determined by the measurement results 00 and 01 of the ancillary two most significant qubits. Constructive and destructive interference caused by the Hadamard gates on the active information allows the desired components to survive as output, and the measurement selects the appropriate subspace of information.

communication protocols (for instance, see [7], [8]): also, it is of great practical interest in experimental implementation, being a powerful tool to transfer quantum information from one system to another, as is required in quantum computers made of several independent units. Moreover, teleportation and single-qubit operations are sufficient to achieve universal quantum computation [7].

The inverse process to quantum teleportation is known as dense coding, one of the simplest yet nontrivial example of how entanglement properties can be exploited in quantum communication to outperform its classical counterpart (see, *e.g.*, [6], pages 205-208). By sharing a maximally entangled state, it is possible to transfer two classical bits of information by actually sending only one quantum bit of information.

The diagram-of-states representations for teleportation and dense coding are presented in the following sections. These representations also suggest interesting applications related to approximate quantum cloning and universal NOT, which we

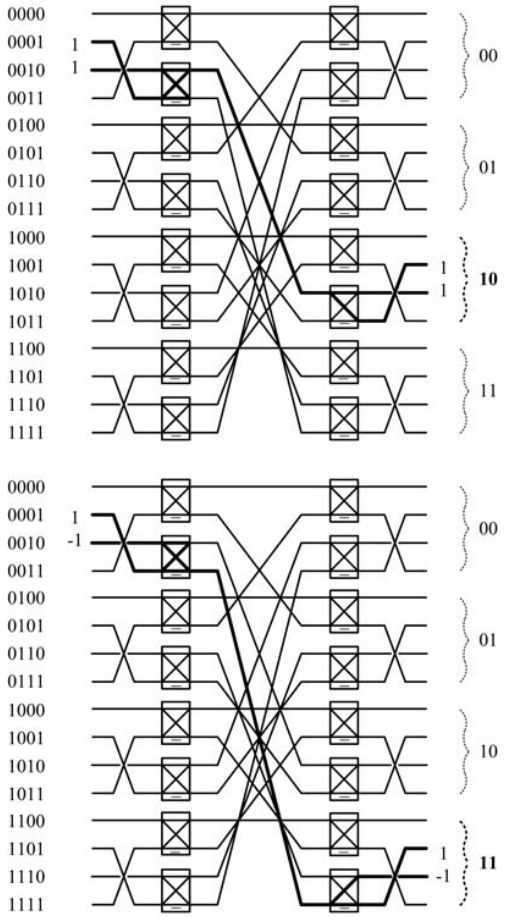

Fig. 6. Diagrams of states representing projections into Bell states, corresponding to the quantum circuit of Figure 4. The diagrams show the projections in the Bell state respectively determined by the measurement results 10 and 11 of the ancillary two most significant qubits. Constructive and destructive interference caused by the Hadamard gates on the active information allows the desired components to survive as output, and the measurement selects the appropriate subspace of information.

illustrate in Section IV.

Throughout this section, we denote classical bits with double lines and quantum bits with single lines.

A. The Teleportation Protocol

In the simplest instance of teleportation, a sender (Alice) owns a two-level system set in some unknown state $|\varphi\rangle$, which is to be communicated to a receiver (Bob) by only using a classical communication channel and sharing with him an entangled state $|\Phi^+\rangle$.

It is well known that a direct measurement of the quantum system would perturb its state, and from this measurement Alice could obtain only a single bit of information, while reconstructing the quantum state $|\varphi\rangle$ generally requires an infinite amount of classical information. On the contrary, by applying the quantum circuit in Figure 7, quantum teleportation allows the perfect transfer of the desired quantum state.

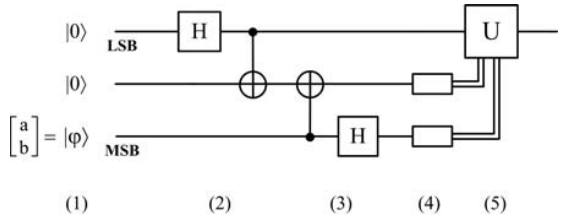

Fig. 7. Quantum circuit to represent quantum teleportation. From left (input) to right (output): (1) definition of initial states; (2) Hadamard and CNOT gates to generate the Bell state $|\Phi^+\rangle$; (3) CNOT and Hadamard gates to perform Bell measurements; (4) measurement in the computational basis of the two most significant qubits (performed by the sender); (5) action on the least significant qubit (owned by the receiver), as determined by the sender's measurement results. The final output is the state $|\varphi\rangle$ perfectly reconstructed. Here and in the following circuits and diagrams of this section, double lines denote classical bits and single lines denote quantum bits.

The information processing performed in quantum teleportation is clearly represented by the complete and simplified diagrams of states in Figure 8. In both diagrams, the active information is given by the parameters a, b of the initial state $|\varphi\rangle$ to be transmitted. This information is appropriately spread by the Hadamard gates along thick lines. At the rightmost end of the diagrams, the state $|\varphi\rangle$ is perfectly reconstructed by the receiver performing the appropriate Pauli operation according to the classical information which has been communicated by the sender. All final amplitudes are equal to $\frac{1}{2}$.

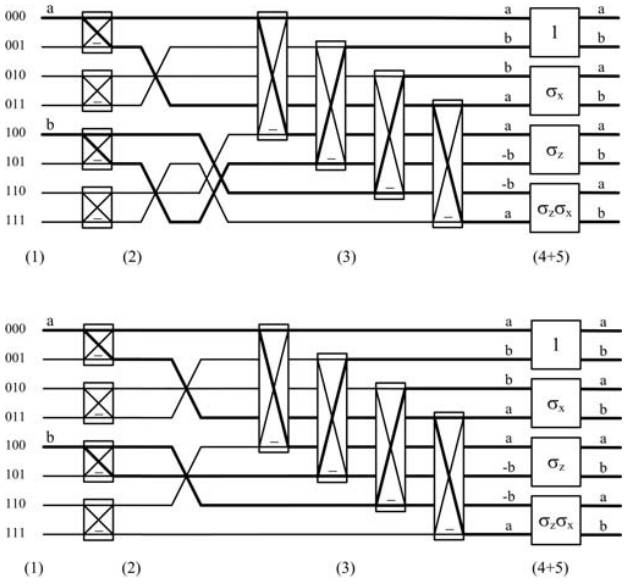

Fig. 8. Complete (upper) and simplified (lower) diagrams of states representing quantum teleportation. In both diagrams, from left (input) to right (output), the sequence of operations is the same of the quantum circuit of Figure 7: (1) definition of the initial states; (2) generation of Bell state $|\Phi^+\rangle$; (3) CNOT and Hadamard gates to perform Bell measurements; (4) measurement in the computational basis of the two most significant qubits (performed by the sender) and (5) action on the least significant qubit (owned by the receiver) determined by the sender's measurement results, both "included" in the appropriate application of Pauli operators.

B. The Dense Coding Protocol

In its simplest instance, the dense coding protocol allows a sender (Alice) to communicate two classical bits of information to a receiver (Bob), by actually transmitting only one quantum bit of information. It is well known that a direct measurement of one quantum bit would only yield a single classical bit of information. On the contrary, by applying the quantum circuit in Figure 9, dense coding allows the communication of the desired pair of classical bits with unit probability.

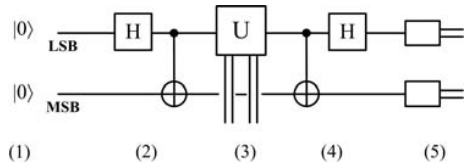

Fig. 9. Quantum circuit representing dense coding. From left (input) to right (output): (1) definition of initial states; (2) Hadamard and CNOT gates to generate the Bell state $|\Phi^+\rangle$; (3) unitary operation performed by the sender on her half of the entangled pair, according to the one out of four possible values of the two classical bits that she wishes to send to the receiver; (4) CNOT and Hadamard gates to perform Bell measurements; (5) measurement in the computational basis. The two desired classical bits are obtained in output with unit probability.

The information processing performed in dense coding is clearly represented by the diagrams of states in Figure 10. Requiring no further analytical study, the diagrams show the four possible unitary operations performed by Alice on her half of the entangled pair, according to the value of the two classical bits that she wishes to send to Bob. More precisely, to communicate the classical pair of bits $00, 01, 10$ or 11, Alice respectively performs the unitary operation $U = I, \sigma_z, \sigma_x$ or σ_y, where I denotes the identity matrix. The constructive and destructive interference of information caused by the Hadamard gates acts on the active information originated by the input state and flowing along thick lines. Interference allows only the desired components to survive as output, thus leading to the desired measurement result at the rightmost end of the diagrams[1].

IV. Probabilistic Quantum Machines

In this section we investigate two universal operations which are known to be impossible in quantum information and we describe two probabilistic quantum machines which deal with these limitations by approximately processing the forbidden operations. Both machines combine together the processes of Bell states generation and Bell measurements, similarly to the previously illustrated teleportation and dense coding protocols.

It is well known that a fundamental impossibility in quantum information is perfect cloning of unknown general states [11]. However, such no-cloning theorem only forbids perfect cloning: Approximate copies [12] are indeed allowed and

[1]The diagram-of-states representation leads us to observe that the application of the two Hadamard gates can be considered as an extension of the Mach-Zehnder interferometer [9], [10], as these gates select one of the four possible outcomes by processing information in one of the four possible corresponding ways, as illustrated in the respective diagrams.

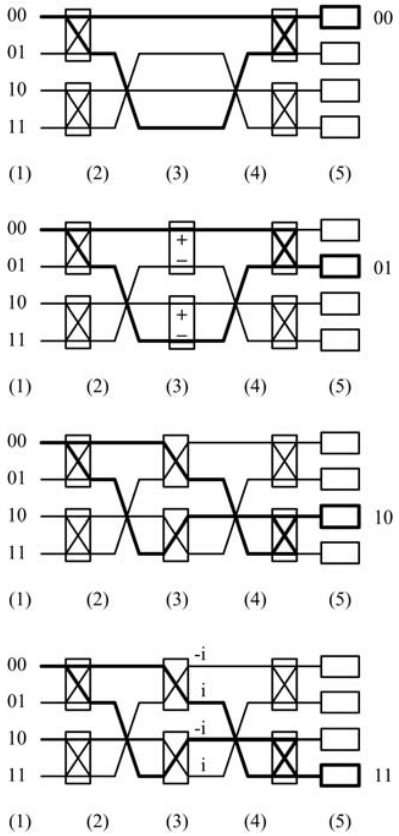

Fig. 10. Diagrams of states representing dense coding. To communicate to the receiver the classical pair of bits $00, 01, 10$ or 11, the sender respectively performs the unitary operation $U = I, \sigma_z, \sigma_x$ or σ_y, where I denotes the identity matrix. In all diagrams, from left (input) to right (output), the sequence of operations is the same of the quantum circuit of Figure 9: (1) definition of initial states; (2) Hadamard and CNOT gates to generate the Bell state $|\Phi^+\rangle$; (3) unitary operation performed by the sender on her half of the entangled pair; (4) CNOT and Hadamard gates to perform Bell measurements; (5) measurement in the computational basis.

they actually have useful employment in several applications, such as state estimation and partial eavesdropping in quantum cryptographic protocols.

A second fundamental limitation in quantum information, based on the complete positivity of any quantum operation and conceivably related to perfect cloning, forbids the realization of a universal NOT (UNOT) transformation, that is, the operation of flipping exactly any input qubit into its orthogonal [13]. However, similarly to what happens for quantum cloning, imperfect approximations to the UNOT operation are indeed possible [14], [15].

In the following, we outline by diagrams of states two possible protocols to approximately copy general quantum states and to approximately perform the UNOT operation.

A. A Probabilistic Quantum Cloning Machine

A probabilistic quantum cloning machine can be implemented by means of the quantum circuit illustrated in Figure 11. In order to perform this probabilistic cloning procedure,

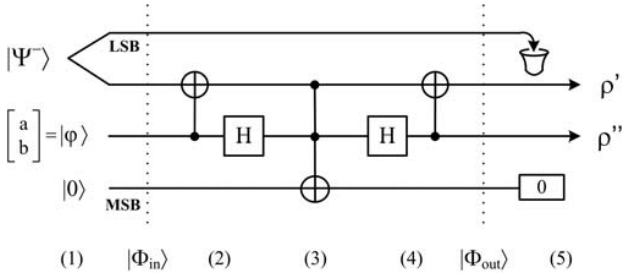

Fig. 11. Quantum circuit representing a probabilistic cloning operation. From left (input) to right (output): (1) definition of the input states, where $|\varphi\rangle$ is the initial state to be cloned; (2) CNOT and Hadamard gates to perform Bell measurements; (3) Toffoli gate; (4) Hadamard and CNOT gates to reconstruct Bell states; (5) measurement in the computational basis of the most significant qubit. The final outputs are ρ' and ρ'', both density matrices of imperfect clones of the initial state $|\varphi\rangle$.

two communicating parties (Alice and Bob) share an entangled pair initially set in the Bell state $|\Psi^-\rangle$. Alice owns a qubit in the state $|\varphi\rangle$, which is to be cloned, and an ancillary qubit in the state $|0\rangle$. After applying the sequence of operations illustrated in Figure 11, she measures the most significant qubit in the computational basis, while Bob's qubit, corresponding to half of the initial entangled pair $|\Psi^-\rangle$, is simply discarded at the end of the process. When the measurement outcome is "0", they obtain the output states ρ' and ρ'', which are imperfect clones of the initial state $|\varphi\rangle$.

The information processing performed in the cloning procedure is clearly illustrated by the diagram of states in Figure 12. The initial state is given by:

$$|\Phi_{\text{in}}\rangle = |0\rangle \otimes \{a|0\rangle + b|1\rangle\} \otimes |\Psi^-\rangle. \tag{4}$$

Requiring no further analytical study, the diagram of states clearly visualize how the active information determined by the input state $|\Phi_{\text{in}}\rangle$ is processed along thick lines until the final output state $|\Phi_{\text{out}}\rangle$ is obtained at the rightmost end of the diagram. Once again, the constructive and destructive interference of information caused by the Hadamard gates selects the components which are allowed to survive as output, when the desired outcome is obtained in correspondence with measurement result "0":

$$|\Phi_{\text{out}}\rangle = \frac{1}{\sqrt{2}}\left[\begin{array}{cccccccc} 0 & a & -\frac{a}{2} & \frac{b}{2} & -\frac{a}{2} & \frac{b}{2} & -b & 0 \end{array}\right]^T. \tag{5}$$

The probability to measure the value "0" is given by:

$$\langle\Phi_{\text{out}}|\Phi_{\text{out}}\rangle = \frac{3}{4}. \tag{6}$$

Furthermore, since density matrices can be expressed as follows by means of Pauli operators $\boldsymbol{\sigma}$:

$$\rho \equiv \frac{1}{2}\left[I + \boldsymbol{\lambda}\boldsymbol{\sigma}\right] = \frac{1}{2}\left[\begin{array}{cc} 1+Z & X-iY \\ X+iY & 1-Z \end{array}\right], \tag{7}$$

where $\boldsymbol{\lambda}$ is the vector of the Bloch sphere coordinates of the described quantum state, the non-normalized density matrix of

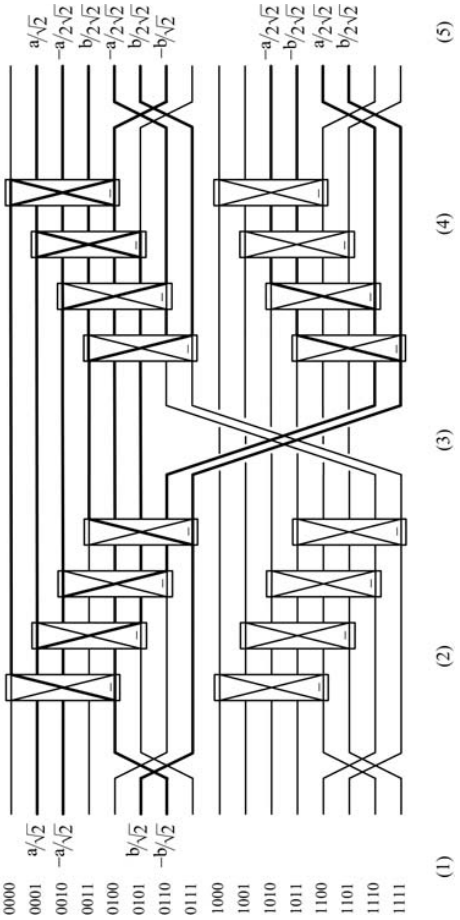

Fig. 12. Diagrams of states representing a probabilistic cloning operation. From left (input) to right (output), the sequence of operations is the same of Figure 11: (1) definition of the input states, where a, b are the parameters of the initial state to be cloned; (2) application of CNOT and Hadamard gates to perform Bell measurements; (3) Toffoli gate; (4) Hadamard and CNOT gates to reconstruct the selected Bell states; (5) measurement in the computational basis of the most significant qubit.

Alice's output states is given by:

$$\rho_{\text{out}} = \frac{1}{8}\begin{bmatrix} 2(1+Z) & X-iY & X-iY & 0 \\ X+iY & 1 & 1 & X-iY \\ X+iY & 1 & 1 & X-iY \\ 0 & X+iY & X+iY & 2(1-Z) \end{bmatrix}. \tag{8}$$

Thus, we can derive by partial tracing the re-normalized density matrices of the two imperfect copies of the input state $|\varphi\rangle$. These density matrices are identical and equal to:

$$\rho' = \rho'' = \frac{1}{2}\begin{bmatrix} 1+\frac{2}{3}Z & \frac{2}{3}(X-iY) \\ \frac{2}{3}(X+iY) & 1-\frac{2}{3}Z \end{bmatrix}. \tag{9}$$

Both the cloned states are thus represented by a Bloch vector contracted of a $\frac{2}{3}$ factor in respect to the Bloch vector of the original state.

B. A Probabilistic UNOT *Machine*

An approximate UNOT operation can be implemented by means of the quantum circuit illustrated in Figure 13. In order

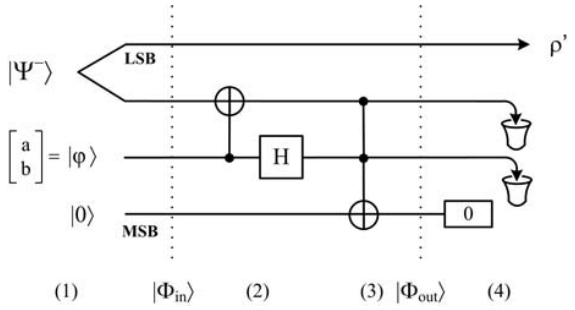

Fig. 13. Quantum circuit representing a probabilistic universal NOT (UNOT) operation. From left (input) to right (output): (1) definition of the input states, where $|\varphi\rangle$ is the initial state on which the UNOT transformation is to be applied; (2) CNOT and Hadamard gates to perform Bell measurements; (3) Toffoli gate; (4) measurement in the computational basis of the most significant qubit. The final output is given by the single-qubit density matrix ρ_{out}, while the remaining qubits are discarded at the end of the process.

to perform this probabilistic UNOT operation on an assigned general quantum state $|\varphi\rangle$, an entangled pair is initially set in the Bell state $|\Psi^-\rangle$ and an additional ancillary state is set to $|0\rangle$. After applying the sequence of operations illustrated in Figure 13, the most significant qubit is measured in the computational basis, while the other two most significant qubits are discarded at the end of the process. When the measurement outcome is "0", the performed transformation yields output state ρ_{out}.

The information processing performed in the UNOT operation is clearly illustrated by the diagram of states in Figure 14. The initial state is given by:

$$|\Phi_{\text{in}}\rangle = |0\rangle \otimes \{a|0\rangle + b|1\rangle\} \otimes |\Psi^-\rangle. \tag{10}$$

Requiring no further analytical study, the diagram of states clearly visualize how the active information determined by the input state $|\Phi_{\text{in}}\rangle$ is processed along thick lines until the final output state $|\Phi_{\text{out}}\rangle$ is obtained at the rightmost end of the diagram. The upper Hadamard gates appropriately spread the

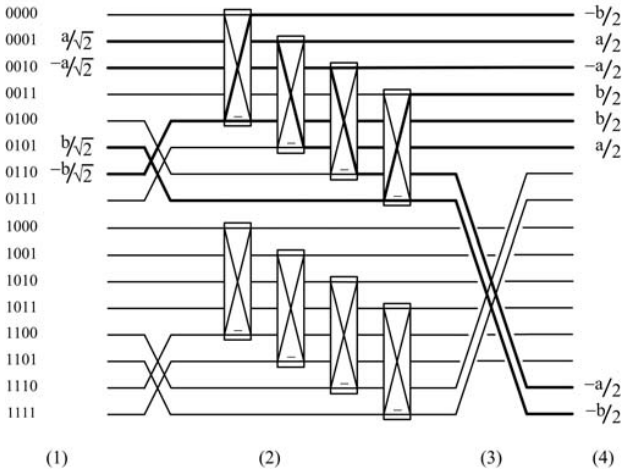

Fig. 14. Diagram of states representing a probabilistic UNOT operation. From left (input) to right (output), the sequence of operations is the same of Figure 13: (1) definition of the input states, where $\{a, b\}$ are the parameters of the initial state on which the UNOT transformation is to be applied; (2) CNOT and Hadamard gates to perform Bell measurements; (3) Toffoli gate; (4) measurement of the most significant qubit in the computational basis.

active information in thick lines, yielding the desired output state in correspondence with measurement result "0":

$$|\Phi_{\text{out}}\rangle = \begin{bmatrix} -\frac{b}{2} & \frac{a}{2} & -\frac{a}{2} & \frac{b}{2} & \frac{b}{2} & \frac{a}{2} & 0 & 0 \end{bmatrix}^T. \tag{11}$$

The probability to measure the value "0" is given by:

$$\langle\Phi_{\text{out}}|\Phi_{\text{out}}\rangle = \frac{3}{4}. \tag{12}$$

With the previously recalled Bloch sphere coordinates notation, the density matrix of the output state is given by:

$$\rho_{\text{out}} = \frac{1}{8}\begin{bmatrix} 3-Z & -X+iY \\ -X-iY & 3+Z \end{bmatrix} \tag{13}$$

and, after re-normalizing to obtain unitary trace, by:

$$\rho_{\text{out}} = \frac{1}{2}\begin{bmatrix} 1-\frac{Z}{3} & -\frac{1}{3}(X-iY) \\ -\frac{1}{3}(X+iY) & 1+\frac{Z}{3} \end{bmatrix}. \tag{14}$$

Thus, we derive the corresponding transformation in the Bloch sphere coordinates:

$$\begin{cases} X' = -\frac{1}{3}X \\ Y' = -\frac{1}{3}Y \\ Z' = -\frac{1}{3}Z \end{cases} \tag{15}$$

Since the final density matrix of a quantum state on which the ideal UNOT operation were performed would have been:

$$\rho_{\text{id}} = \frac{1}{2}\begin{bmatrix} 1-Z & -(X-iY) \\ -(X+iY) & 1+Z \end{bmatrix}, \tag{16}$$

the approximate UNOT operation is actually obtained with a fidelity factor equal to $\frac{2}{3}$. More precisely, for any pure initial state the fidelity of the transformation is:

$$Tr\{\rho_{\text{id}}\,\rho_{\text{out}}\} = \frac{2}{3}. \tag{17}$$

V. Entanglement Purification

A central problem in quantum communication consists in how to reliably transmit information through noisy channels. In communication and cryptographic protocols, the communicating parties are very likely to be located far away from each other; consequently, the resources on which they can operate to perform the desired tasks are spatially separated, and this prevents the application of usual quantum error correction techniques.

Any information reconciliation or error-correcting procedure for quantum communication must only be based on local quantum operations, possibly supplemented by (public) exchange of classical information. The class of protocols which fulfill these conditions is denoted as LOCC – local operations and classical communication. Moreover, if the considered communication protocols are based on the properties of entangled states, special LOCC protocols which also exploit the properties of entanglement can be used to reduce any undesirable effects of noise. Such procedures are known as entanglement distillation or purification (see, *e.g.*, [16], pages 500-511).

In this section, we explore by means of the diagram-of-states representation a useful instance of entanglement purification procedure, the so-called DEJMPS protocol, initially proposed by Deutsch et al. [4] in order to achieve quantum privacy amplification in a cryptographic scenario.

A. The DEJMPS Protocol

In entanglement-based cryptography, two communicating parties (Alice and Bob) share a source of entangled pairs and operate on their own member of each generated pair. Noise in the channel, or the perturbation caused by an eavesdropper (Eve), degrades the quality and amount of entanglement in the initially perfect shared pairs. As a result, Alice and Bob share only partially entangled states, since each pair is now entangled with the environment, or with the eavesdropper's qubits. At this point, Alice and Bob can iteratively apply the DEJMPS protocol in order to purify the entanglement of their shared pairs. Since a perfectly entangled pair is a pure state automatically de-entangled from the environment, they can reduce the entanglement of their states with any outside system to arbitrarily low values, thus eliminating any external perturbation, or gain of information by a potential eavesdropper.

Figure 15 illustrates the quantum circuit implementing a single iteration of the DEJMPS protocol. At each step, the imperfect entangled pairs are combined in groups of two. Alice applies to her qubits a $\frac{\pi}{2}$- rotation around the x-axis, described by the unitary matrix:

$$U = R_x\left(\frac{\pi}{2}\right) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & -i \\ -i & 1 \end{bmatrix}, \qquad (18)$$

while Bob applies to his qubits the inverse operation:

$$V = U^{-1} = R_x\left(-\frac{\pi}{2}\right) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}. \qquad (19)$$

Both Alice and Bob apply a CNOT gate on their own member of the two entangled pairs and they subsequently measure the z-components of their own target qubit. Finally, they compare the measurement outcomes by means of a public classical communication channel. If the outcomes coincide, the control pair is kept for the next iteration and the target pair is discarded. Otherwise, both pairs are discarded.

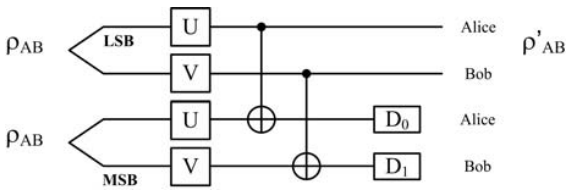

Fig. 15. Quantum circuit representing a single iteration of the DEJMPS entanglement purification protocol. The initial mixed pairs are described by the density matrices ρ_{AB}. From left (input) to right (output), the two communicating parties locally perform the appropriate sequence of unitary operations. The two most significant qubits are measured and the final output is a purified state ρ'_{AB}. The density matrix ρ'_{AB} describes the actual output only when the detectors D_0 and D_1 yield coinciding outcomes.

The information processing performed by a single iteration of the DEJMPS entanglement purification protocol is clearly illustrated by the complete and simplified diagrams of states in Figures 16 and 17, derived from the quantum circuit in Figure 15. The simplified diagram also visualizes how the active information is elaborated along thick lines by considering the specific case in which we would like to obtain a maximally entangled state $|\Phi^+\rangle$ by purification of two corresponding imperfect entangled states. Once again, a fundamental role is played by the constructive and destructive interference of information caused by the rotation gates. Interference allows the appropriate components to survive as output, until the desired purified state is obtained at the rightmost end of the diagram when the detectors D_0 and D_1 yield coinciding outcomes.

Thus, starting from a sufficiently large number of initial imperfect entangled pairs, Alice and Bob can distill asymptotically pure maximally entangled pairs. However, it should be noted that this quantum privacy amplification procedure is rather wasteful, since at least half of the pairs are lost at every iteration. More precisely, to extract in output one pair close to the ideal Bell state after n steps, at least 2^n mixed pairs are needed in input (see Figure 18, which illustrates two iterations of the DEJMPS protocol). Moreover, this number could be significantly larger, since pairs must be discarded also whenever Alice and Bob obtain different measurement outcomes.

Finally, we stress that both the entanglement purification procedure described here and the projections into Bell states illustrated in Section II can be applied to obtain maximally entangled states from less entangled states. However, since Bell projections require non-local operations, only the DEJMPS protocol can be used in the framework of quantum cryptography and communication.

VI. Conclusions and Future Developments

We have explored entanglement and some of its most renowned applications in quantum information and commu-

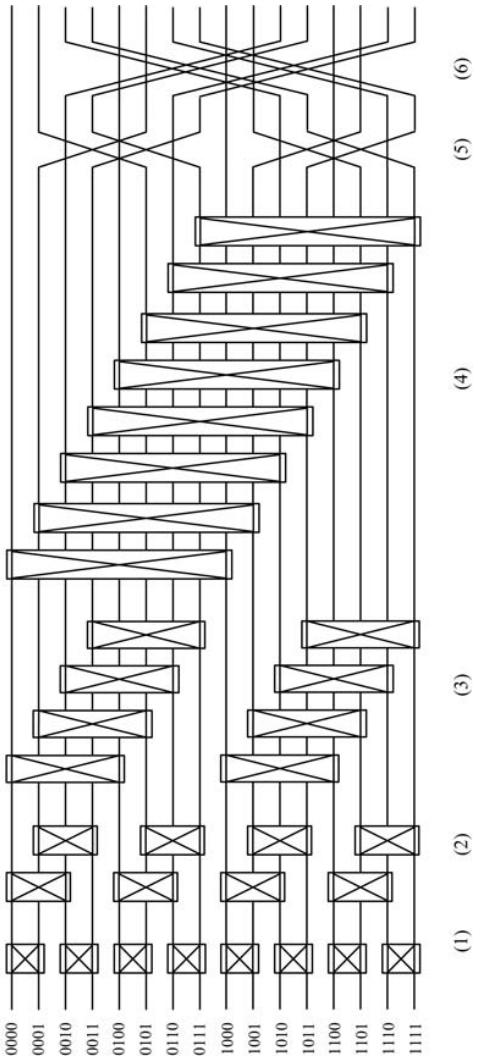

Fig. 16. Complete diagram of states representing a single iteration of the DEJMPS entanglement purification protocol. From left (input) to right (output), the sequence of operations is the same of Figure 15: (1) Alice applies to her least significant qubit a $\frac{\pi}{2}$-rotation around the x-axis; (2) Bob applies to his least significant qubit a $-\frac{\pi}{2}$-rotation around the x-axis; (3) Alice applies to his most significant qubit a $\frac{\pi}{2}$-rotation around the x-axis; (4) Bob applies to his most significant qubit a $-\frac{\pi}{2}$-rotation around the x-axis; (5,6) Alice and Bob apply a CNOT gate on their own member of the two entangled pairs.

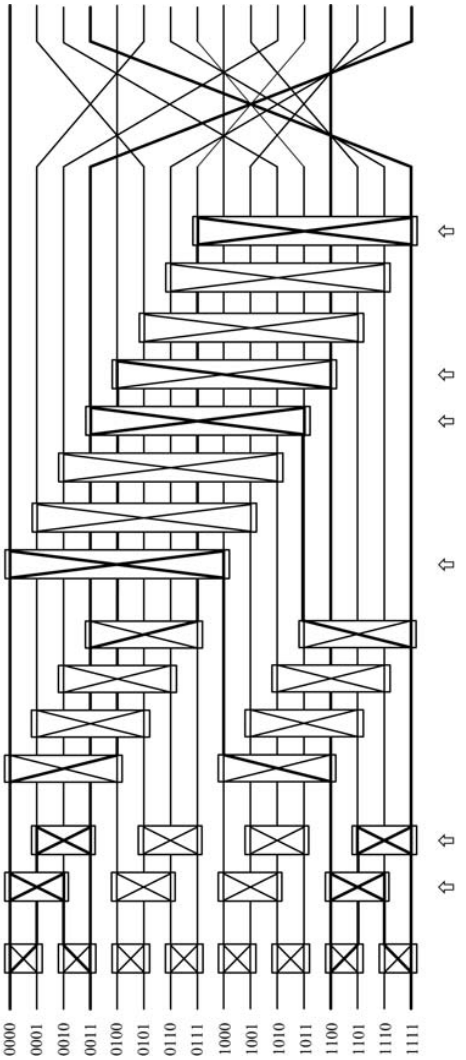

Fig. 17. Simplified diagram of states representing a single iteration for the purification into the maximally entangled state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, as performed by the DEJMPS protocol. Starting from the input state, the active information determined by the imperfect input states is processed along thick lines. The components corresponding to the state $|\Phi^+\rangle$ are selected by the destructive interference caused by the rotation gates, marked by arrows at the bottom. The desired purified state is obtained at the rightmost end of the diagram, when the detectors D_0 and D_1 yield coinciding outcomes.

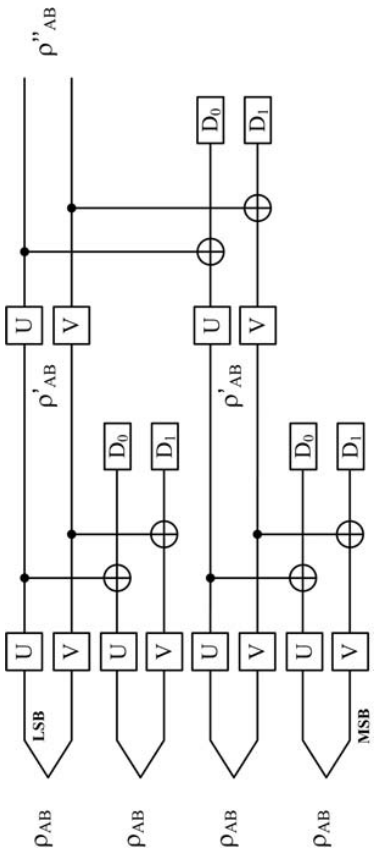

Fig. 18. Quantum circuit representing two iterations of the DEIMPS entanglement purification protocol. The initial imperfect pairs are described by a first set of density matrices (here denoted with ρ_{AB}). The two communicating parties locally perform the appropriate sequence of unitary operations on each couples of imperfect pairs, obtaining a second set of density matrices (here denoted with ρ'_{AB}); subsequently, they apply once again the same sequence of operations on the partially purified states, finally obtaining one final purified density matrix (ρ''_{AB}). All density matrices describe actual outputs only when the detectors D_0 and D_1 yield coinciding outcomes.

nication by means of *Diagrams of States*, a novel method to graphically represent and analyze how quantum information is elaborated during computations performed by quantum circuits. We have offered complete and detailed descriptions by diagrams of states of Bell states generation, measurements and projections, dense coding and quantum teleportation, probabilistic machines to approximate two impossible operations in quantum information, that is, cloning of general quantum states and universal NOT, and, finally, quantum privacy amplification based on entanglement purification.

In our opinion, diagrams of states can be used as an auxiliary or as an alternative approach to standard methods, both to investigate and to conceive quantum computations. Analytical study and quantum circuits alone are often too synthetic to clearly visualize how quantum information is processed by computations. On the contrary, the dimension of the graphic representation of states grows exponentially in respect to the dimension of the examined quantum system, thus offering a complete and detailed visualization of the computational process.

Diagrams of states appear to be most useful whenever the quantum operations to be analyzed are described by very sparse matrices, since only non-null entries of matrices are associated with diagram lines which contain active information. This way, the resulting diagrams show clearly and immediately the significant pattern along which quantum information is processed by the computation from input to output. Indeed, several quantum computations actually involve operations satisfying this requirement, and evidence of this is also provided by the processes illustrated in this paper.

Further computations are going to be explored by this graphic representation, among which quantum algorithms [17] and models for two-qubit decoherence and errors.

ACKNOWLEDGMENTS

The authors wish to thank Samuel L. Braunstein, Alberto O. Leporati and Roberto Suardi for their kind contributions to the development and improvement of this paper.

Sara Felloni acknowledges support by ERCIM, as this work was partially carried out during the tenure of an ERCIM “Alain Bensoussan” Fellowship Programme.

REFERENCES

[1] S. Felloni, A. Leporati and G. Strini, Diagrams of states in quantum information: An illustrative tutorial, *International Journal of Unconventional Computing*, to be published; arXiv:0904.2656v1[quant-ph].

[2] S. Felloni, A. Leporati and G. Strini, Evolution of quantum systems by diagrams of states, submitted for publication.

[3] S. Felloni and G. Strini, A graphic representation of states for quantum copying machines, *Electronic Journal of Theoretical Physics* 3, Vol. 11, p. 159, 2006.

[4] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu and A. Sanpera, Quantum privacy amplification and the security of quantum cryptography over noisy channels, *Physical Review Letters* 77, p. 2818, 1996.

[5] J. S. Bell, On the Einstein Podolsky Rosen paradox, *Physics* 1, p. 195, 1964.

[6] G. Benenti, G. Casati and G. Strini, *Principles of Quantum Computation and Information, Vol. 1: Basic Concepts*, World Scientific, Singapore, 2004.

[7] D. Gottesman and I. L. Chuang, Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations, *Nature* 402, p. 390, 1999.
[8] E. Knill, R. La and G. J. Milburn, A scheme for efficient quantum computation with linear optics, *Nature* 409, p. 46, 2001.
[9] L. Zehnder, *Z. Instrumentenkunde* 11, p. 275, 1891.
[10] L. Mach, *Z. Instrumentenkunde* 12, p. 89, 1892.
[11] W. K. Wootters and W. H. Zurek, A single quantum state cannot be cloned, *Nature* 299, p. 802, 1892.
[12] V. Bužek and M. Hillery, Quantum copying: beyond the No-Cloning Theorem, *Physical Review A* 54, p. 1844, 1996.
[13] N. Gisin and S. Popescu, Spin flips and quantum information for anti-parallel spins, *Physical Review Letters* 83, p. 432, 1999.
[14] V. Bužek, M. Hillery and R. F. Werner, Optimal manipulations with qubits: Universal NOT gate, *Physical Review A* 60, R2626, 1999.
[15] V. Bužek, M. Hillery and R. F. Werner, Universal-NOT gate, *Journal of Modern Optics* 47, p. 211, 2000.
[16] G. Benenti, G. Casati and G. Strini, *Principles of Quantum Computation and Information, Vol. 2: Basic Tools and Special Topics*, World Scientific, Singapore, 2007.
[17] S. Felloni and G. Strini, Quantum algorithms by diagrams of states: Deutsch's and Grover's algorithms, submitted for publication.

Sara Felloni is a postdoctoral fellow at the Department of Electronics and Telecommunications of the Norwegian University of Science and Technology NTNU and UNIK - University Graduate Center, Norway. Working in Quantum Information Processing, she graduated cum laude in Mathematics in 2005 at the University of Milano and achieved a PhD degree in Informatics at the University of Milano–Bicocca in 2009. Her current post-doctoral position is supported by the *European Research Consortium for Informatics and Mathematics* in the framework of the ERCIM "Alain Bensoussan" Fellowship Programme.

Giuliano Strini is associated professor in Experimental Physics at the Department of Physics, University of Milan, Italy. He is also member of the *Italian Physical Society* and the *Optical Society of America*. He has been teaching several courses of Quantum Computation at the University of Milan. His publications concern nuclear reactions and spectroscopy, detection of gravitational waves, quantum optics and quantum computing. From 1963, he has been involved in construction and development of the Cyclotron of Milan. Together with G. Benenti and G. Casati, he is co-author of *Principles of Quantum Computation and Quantum Information, Vol. I: Basic Concepts*, and *Vol. II: Basic Tools and Special Topics*, World Scientific, Singapore, 2004 and 2007.