# Quantum Information Processing and Diagrams of States

***September 17th 2009, AFSecurity***

Sara Felloni

*sara@unik.no / sara.felloni@iet.ntnu.no*

**Quantum Hacking Group**: ***http://www.iet.ntnu.no/groups/optics/qcr/***

UNIK – University Graduate Center

NTNU, Department of Electronics and Telecommunications

ERCIM UNIK NTNU



# Quantum Information Processing

# Quantum Computing



...is the study of the information processing tasks performed by means of **quantum-mechanical systems**:

- The elementary physical carrier of information is a **qubit** – described by a $2$-dimensional Hilbert space
- The state of a **n-qubit register** lives in a $2^n$-dimensional Hilbert space – tensor product of $n$ $2$-dimensional spaces
- By imitating classical computations, **quantum computations** comprise three steps in sequence:
  - **Preparation** of the **initial state** of the register
  - **Computation** by **quantum gate arrays** – unitary transformations of the register state
  - **Output** of the final result – by probabilistic **measurement** of all or part of the register

# Quantum Information Processing



...exploits the **peculiar properties** of quantum systems:

- The **superposition principle** – superpositions of different input states are processed simultaneously
- Quantum **interference** – information behaves and propagates as interactions of wave patterns
- Quantum **entanglement** – non-classical correlations exist between observable physical properties of spatially separated systems

...in order to:

- solve several **computational problems** more efficiently than by classical computers
- open up new possibilities for **communication** and **cryptography**
- efficiently **simulate physical systems**

# Quantum Algorithms

...can currently be enumerated under few classes:

- Basic/**early quantum algorithms** – explorations of the features later exploited by more powerful algorithms, Deutsch's algorithm for global properties of functions sets
- Algorithms based on **amplitude amplification** – Grover's search in unstructured databases, quantum amplitude estimation and quantum counting
- Algorithms with a **super-polynomial speed-up** – the quantum Fourier transform, Shor's factoring and period finding algorithm
- Algorithms for the **simulation of dynamical systems** – natural exploitation of the inherent quantum-mechanical behavior

# Quantum Information Protocols



...include several practical applications in **communication** and **information theory**:

- **Quantum cryptography** – no-cloning allows eavesdropping detection in ideal key generation/distribution protocols
- **Quantum cloning** – imperfect cloning of information allows state estimation and (partial) eavesdropping
- **Dense coding** – entanglement enhances communication of classical information
- **Quantum teleportation** – entanglement and classical communication allow reconstruction of quantum information
- **Entanglement purification** – distillation of nearly perfect (from many imperfect) entangled states
- Optimal compression of quantum information, reliable transmissions in noisy channels, quantum error correction...

# Possibilities of Quantum Computing

... have not yet been completely determined.



| Known | Not yet known |
|---|---|
| ▲ Appropriately devised quantum computations can be **more efficient** than their classical counterparts | ▲ The **ultimate efficiency** of quantum computers<br>▲ A **general approach** to devise quantum algorithms and protocols |

Analyzing in depth the functioning of known quantum computations helps understand how to successfully exploit

- ▲ the **computational resources** offered by quantum-mechanical systems
- ▲ the **hidden structure** of the considered problems

# Quantum Information Representations



...have a key role in helping **understand the functioning** of quantum **algorithms** and **protocols**:

## Quantum Circuits

- Horizontal lines represent single **qubits**
- **Quantum gates** are applied from left (input) to right (output)
- They naturally provide **physical feasibility** of computations and a straightforward link to **physical implementation**

## Diagrams of States

- Horizontal lines represent **quantum states** (of the computational basis)
- **State transformations** corresponding to quantum gates are illustrated from left (input) to right (output)
- They are to be used **in addition to** mathematical **formalism** and **quantum circuits** – too synthetic to visualize the information processing

# Single qubit states

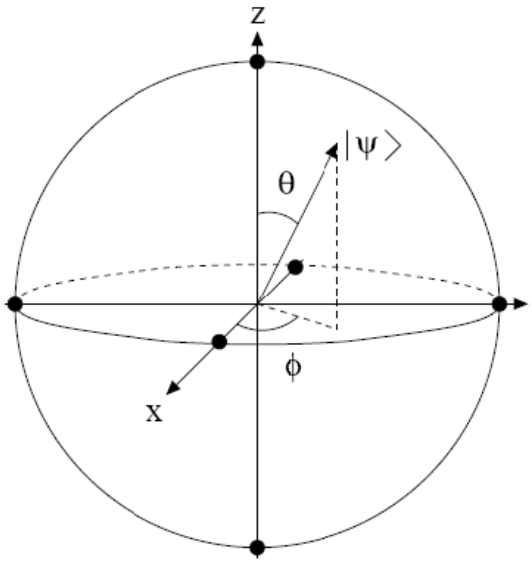
...can be represented by the **Bloch sphere representation**:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

**Spherical coordinates**:

$$|\Psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\Phi}\sin\frac{\theta}{2}|1\rangle = \begin{bmatrix} \cos\frac{\theta}{2} \\ e^{i\Phi}\sin\frac{\theta}{2} \end{bmatrix}$$

**Cartesian coordinates** in the three-dimensional space embedding the **Bloch sphere**:

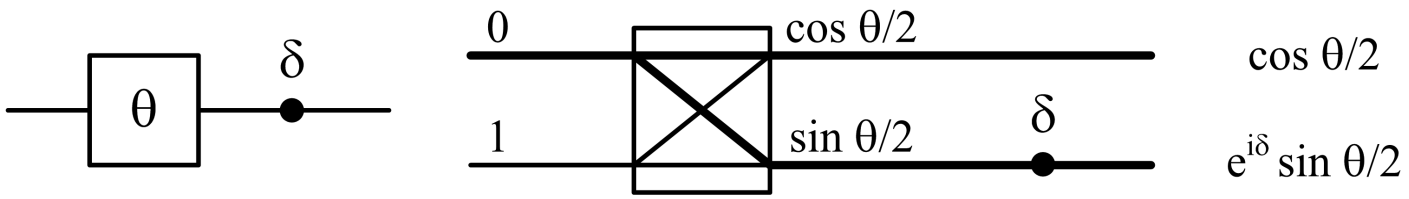


# Generation of single-qubit states



...is obtained by applying a $\theta-$**rotation** about the $y$ axis of the Bloch sphere and a **phase-shift** gate with initial state $|0\rangle$:

$$|\Psi\rangle = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{bmatrix} \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \cos\frac{\theta}{2} \\ e^{i\delta}\sin\frac{\theta}{2} \end{bmatrix}$$




**Quantum circuit** (left) and **Diagram of states** (right)

- The initial state $|0\rangle$ determines the **active information**
- From left to right, **active information** flows on the **thick lines**, while thin lines correspond to absence of information

# Diagrams of States: Practical Applications

# Quantum Diagrams of States



... **graphically represent** and analyze how the **information** encoded in **quantum states** is **processed** during computations performed by quantum circuits.

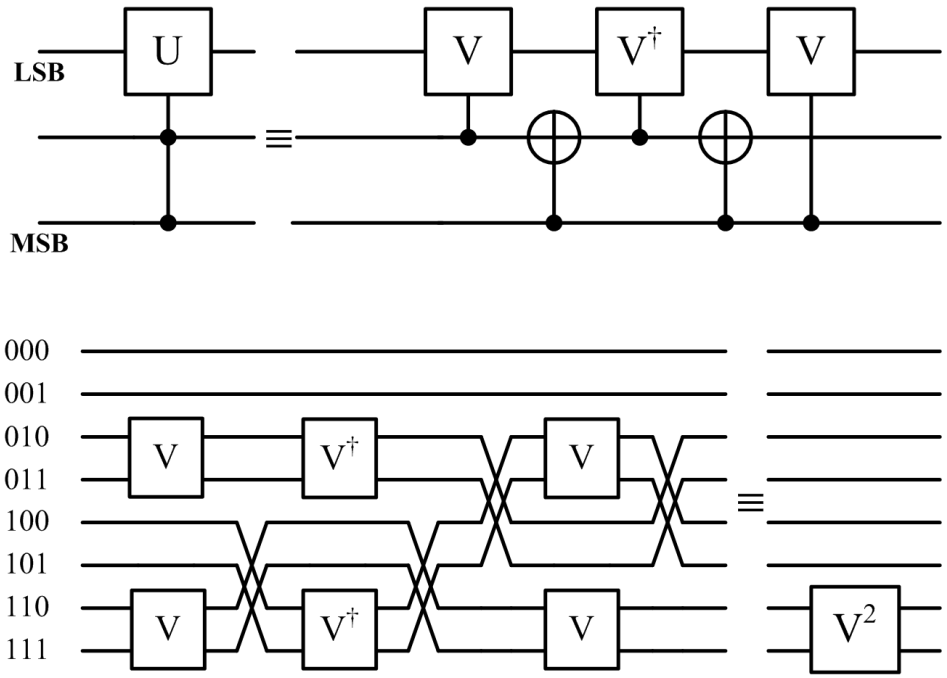
To **analyze** given quantum processes:

- **Derive complete diagrams** directly from implementations by quantum circuits
- **Rearrange** into **simplified diagrams** to visualize the overall effects of computations

To **conceive** new quantum computations:

- **Describe** schematically the **desired manipulations** of information by simple diagrams
- **Expand** into the equivalent complete diagrams to obtain implementations by **quantum circuits**

# Synthesis of Multi-qubit Gates




A **general three-qubit controlled** $U-$**gate**, with control from the two most significant qubits, is obtained by applying two CNOT gates and three controlled $V-$gates with control from a single-qubit.

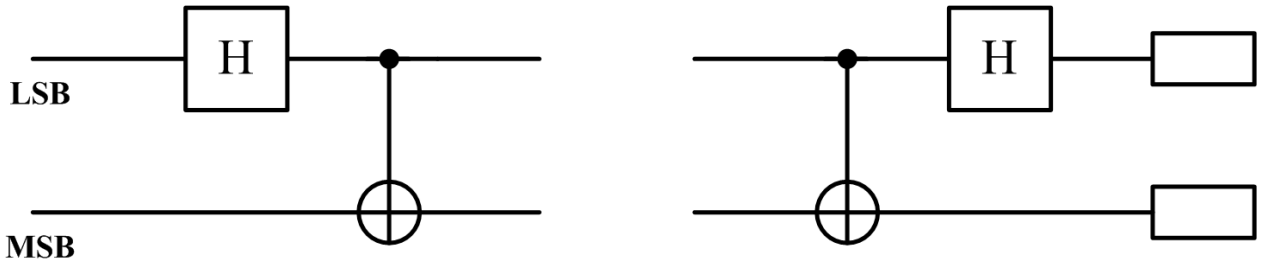
- The diagram replaces a five $8 \times 8$-dimensional matrix multiplication
- The controlled unitary matrix $V$ is such that $V^2 = U$

# Bell States

Bell states are defined as **maximally entangled states** of two qubits:

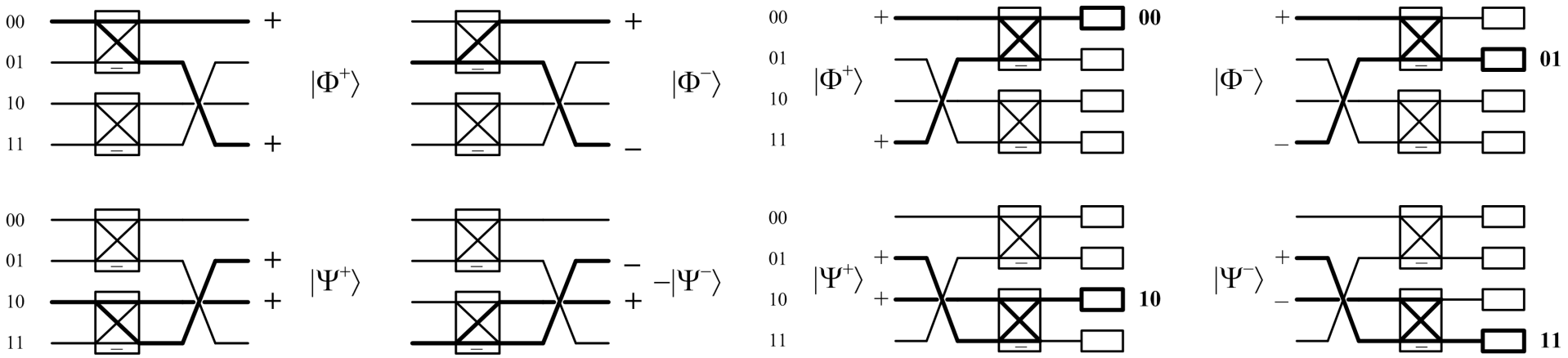
$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}\{|01\rangle \pm |10\rangle\} \qquad |\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}\{|00\rangle \pm |11\rangle\}$$

- **Perfectly correlated** even when **spatially separated** – EPR phenomenon
- Fundamental **resources** for several main algorithms and experiments: quantum teleportation, dense coding, entanglement-based cryptography, entanglement-based protocols...




- **Bell states generation** from the computational basis states (left)
- **Bell measurements** – measurements in respect to Bell basis (right)

# Bell States: Diagrams of States

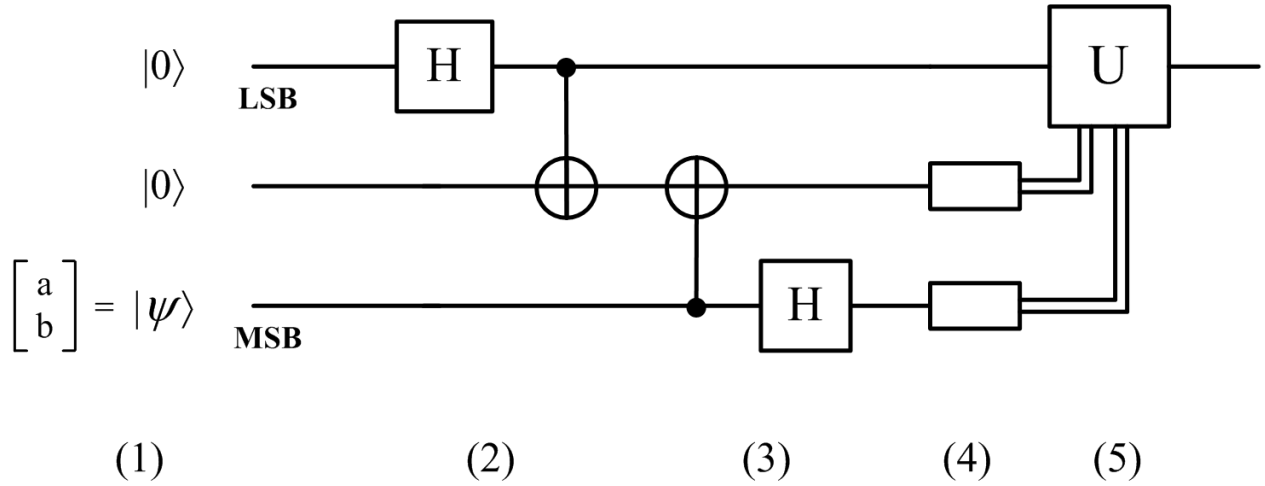



**Bell states generation** (left) and **Bell measurements** (right)

- The initial state determines the **active information** lines
- Output states are determined by **constructive** and **destructive interference** in the active lines caused by Hadamard gates

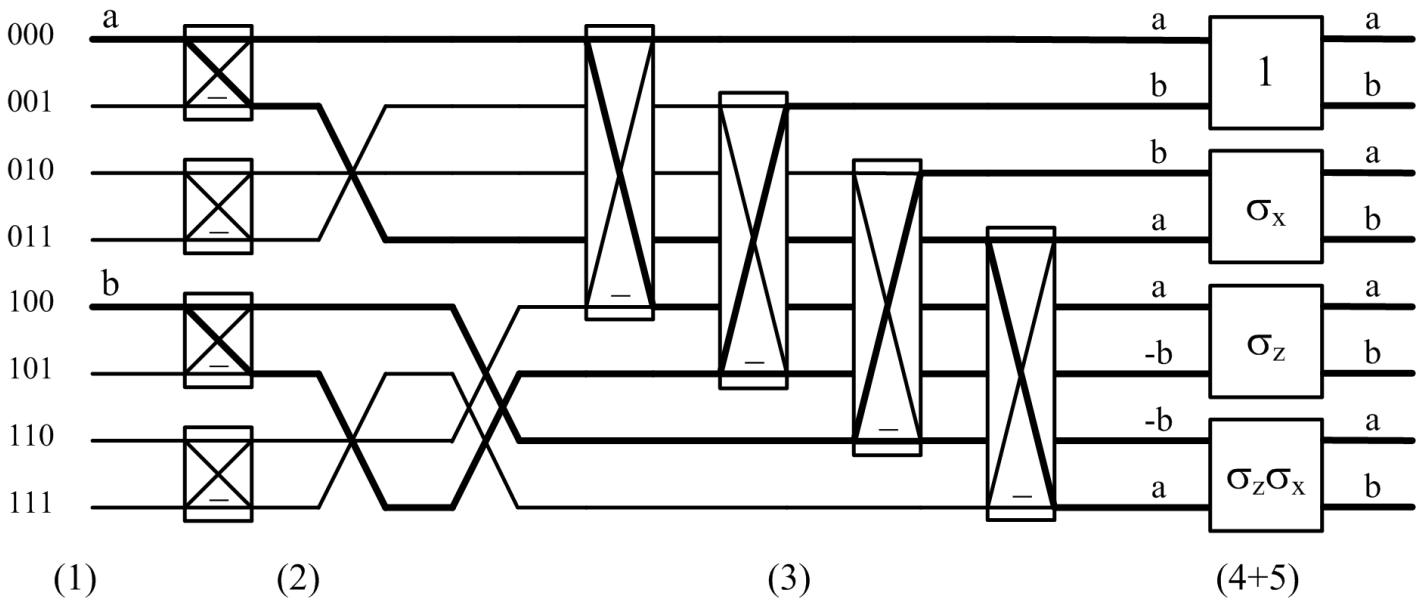
# Quantum Teleportation

- An **unknown quantum state** $|\psi\rangle$ is transferred by **classical communication** and by sharing a **Bell state**
- A direct **measurement** of the quantum system would **perturb** its state, offering **too little information** to reconstruct the state $|\psi\rangle$




(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 (sender); (5) action on the least significant qubit (receiver) determined by the sender's measurement results (double lines denote classical information).

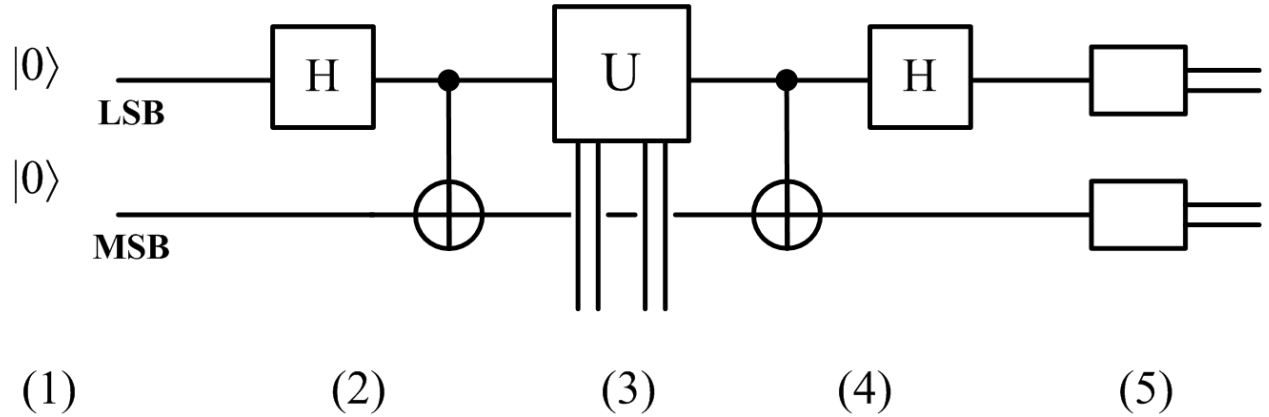
# Teleportation: Diagram of States




- The initial state parameters $a, b$ determine the **active information** lines
- The active information is **spread** by Hadamard gates
- The action on the least significant qubit (receiver) is determined by the sender's measurement results
- The state $|\psi\rangle$ is **perfectly reconstructed** in output

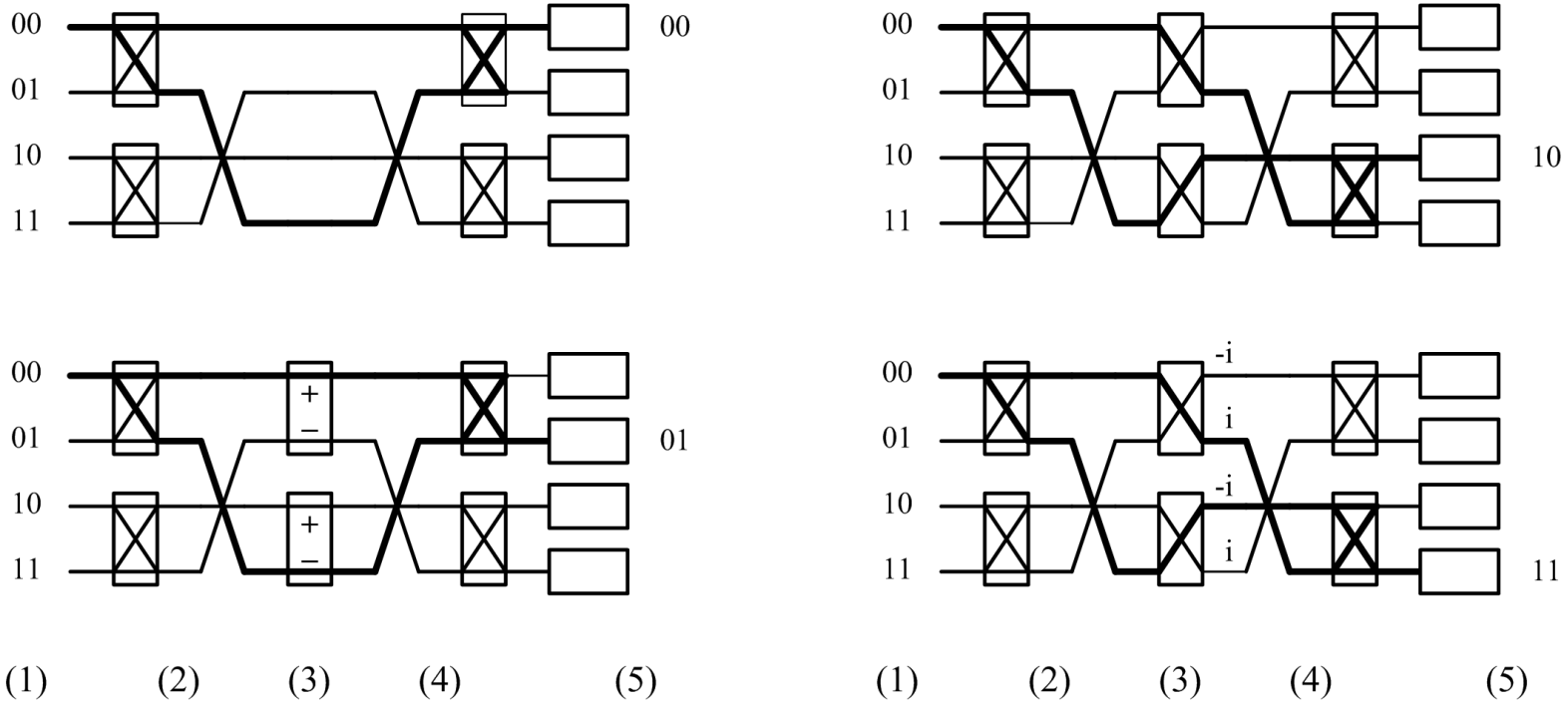
# Quantum Dense Coding

- **Two classical bits** of information are communicated by actually **transmitting** only **one quantum bit** of information
- A direct **measurement** of one quantum bit would give only **a single classical bit** of information




(1) definition of initial states; (2) Hadamard and CNOT gates to generate the Bell state $|\Phi^+\rangle$; (3) unitary operation (sender) on half entangled pair, according to the two classical bits to communicate; (4) CNOT and Hadamard gates to perform Bell measurements; (5) measurement in the computational basis.

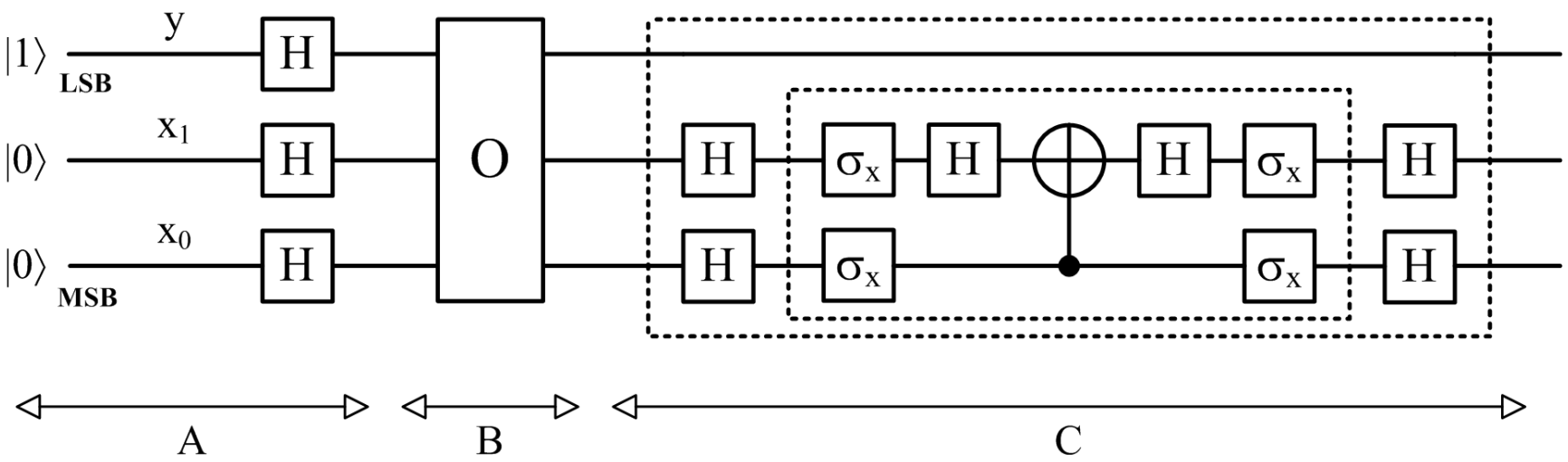
# Dense Coding: Diagrams of States




- **Four possible unitary operations** are performed by the sender according to the two classical bits to communicate
- Output states are determined by **constructive** and **destructive interference** caused by Hadamard gates and by the sender's operation
- The two desired classical bits are **communicated** with **unit probability**

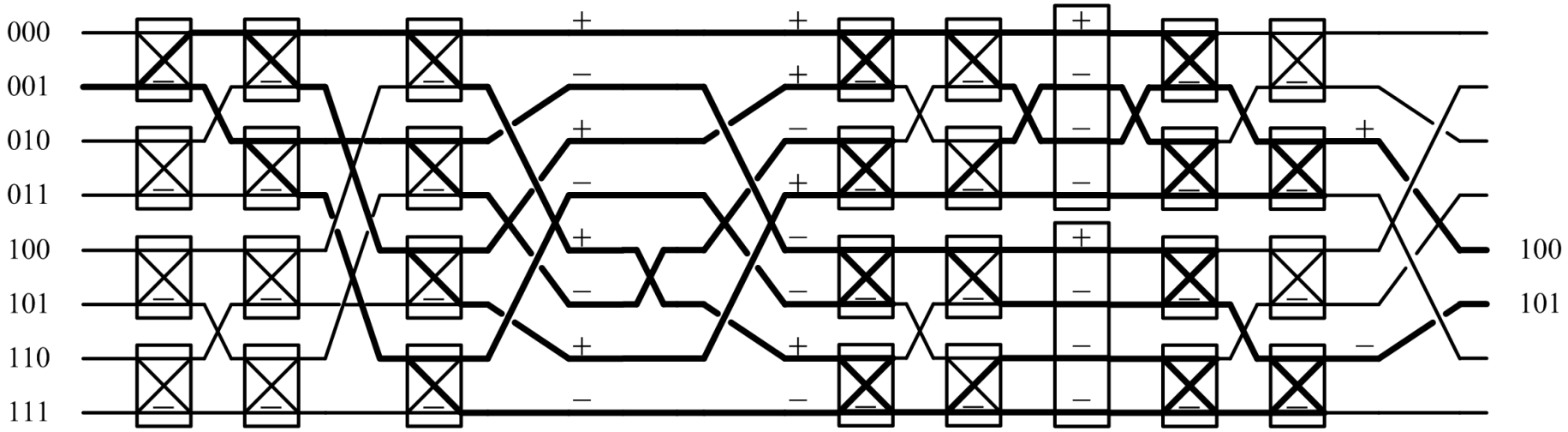
# Grover's Search Algorithm

- Main representative of search heuristics for **unstructured problems**
- It addresses the problem of searching for **one marked item** inside an unstructured database of $N = 2^n$ items
- **Quadratic speed up** in resolution of general search problems




A quantum circuit implementing Grover's algorithm to find one item out of $N = 4$, represented by two qubits: "A" - preparation of the state of the register and ancillary qubits; "B" - oracle query; "C" - main instruction.

# Grover's Algorithm: Diagram of States




- Information in **thick lines** is spread by the Hadamard gates and subsequently manipulated by the **oracle function**
- The output state is determined by **constructive** and **destructive interference** caused by Hadamard gates
- The final **active output lines** correspond to basis states $|100\rangle$ and $|101\rangle$: **Measurement** gives as outcome the **marked item** "$10$" with **certainty**
- The search problem is solved with a **single query** of the **oracle function** $f$

# Entanglement Purification

ERCIM UNIK NTNU

# Reliable Quantum Transmissions



- A fundamental problem in quantum communication is how to **reliably transmit** information through **noisy channels**:
  - **decoherence** – undesired interactions between qubits carrying information and the environment
  - **imperfections** in the quantum components implementing the communication apparatus
  - **eavesdropping** operations performed on the qubits carrying information in a cryptographic scenario
- In communication and cryptographic protocols the communicating parties **resources** are **spatially separated**
- Any information reconciliation or error-correcting procedure must be LOCC – **local operations** and **classical communication**

# Entanglement Purification



When considering **entanglement-based communication** protocols, special LOCC protocols – also entanglement-based – can be used to:

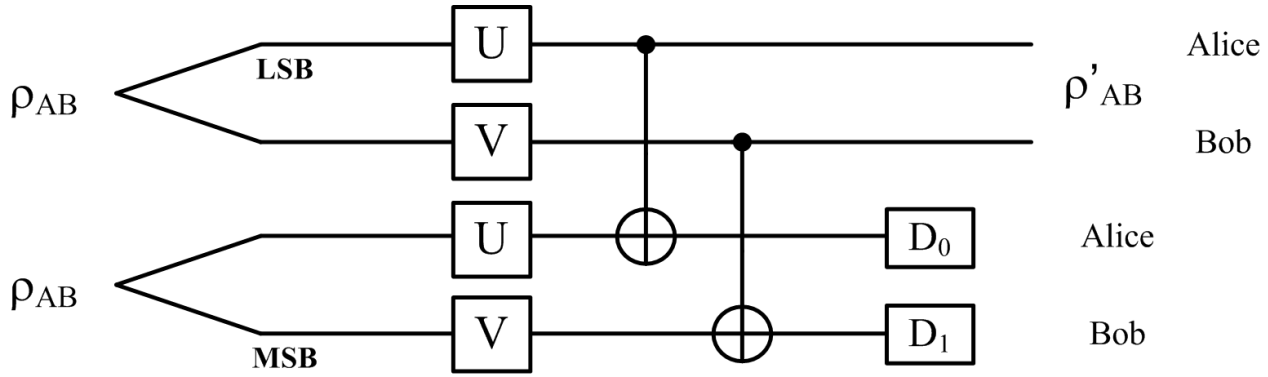
- improve the **quality** and the **amount** of **entanglement** in the initially imperfect shared pairs
  - in protocols requiring **high-quality entanglement**: teleportation, quantum repeaters...
- **reduce** the **entanglement** with any **outside system** to arbitrarily low values
  - **eliminating eavesdropping** in cryptography...

*D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu and A. Sanpera*
*Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels – Phys. Rev. Lett. 77, 2818 (1996)*

# Quantum Privacy Amplification

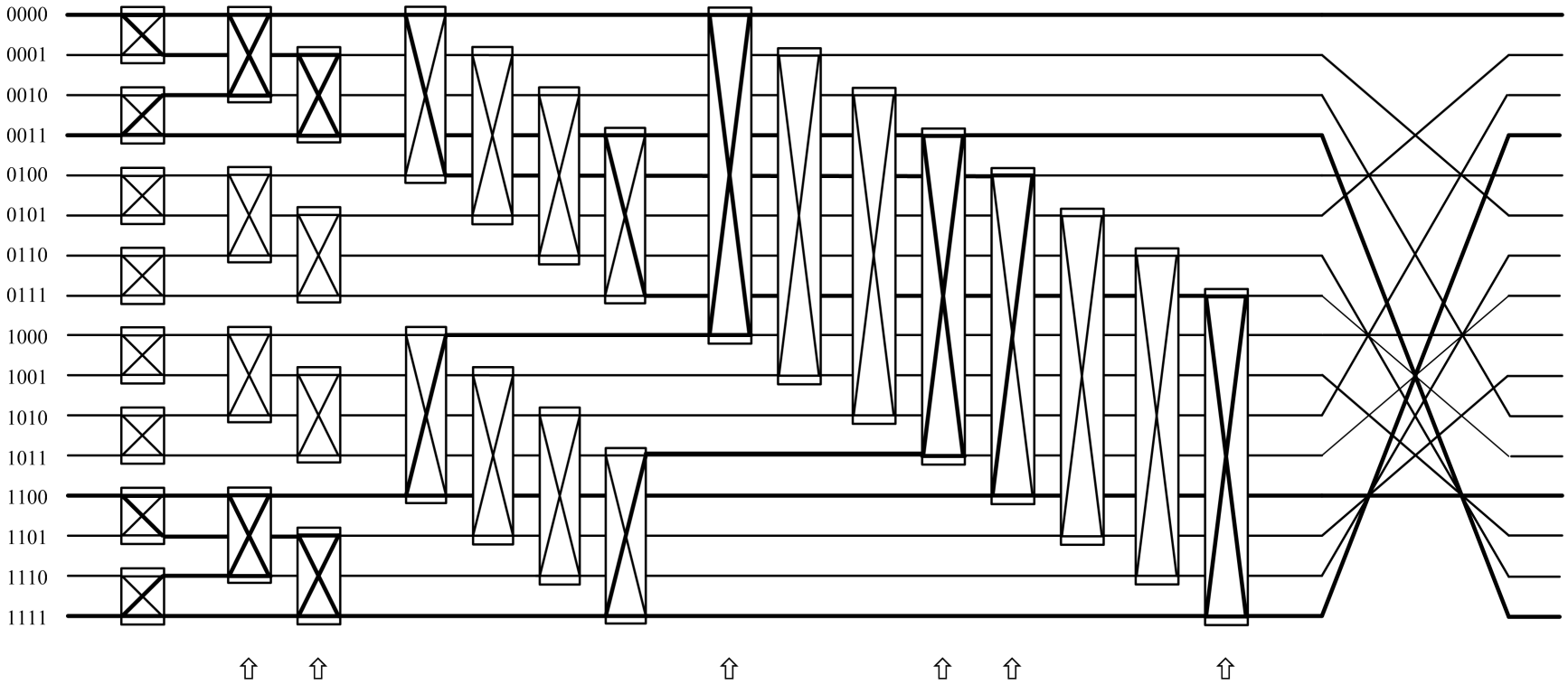


The QPA protocol **purifies entanglement** by creating **nearly perfect** EPR states out of exponentially many **partially entangled** states:



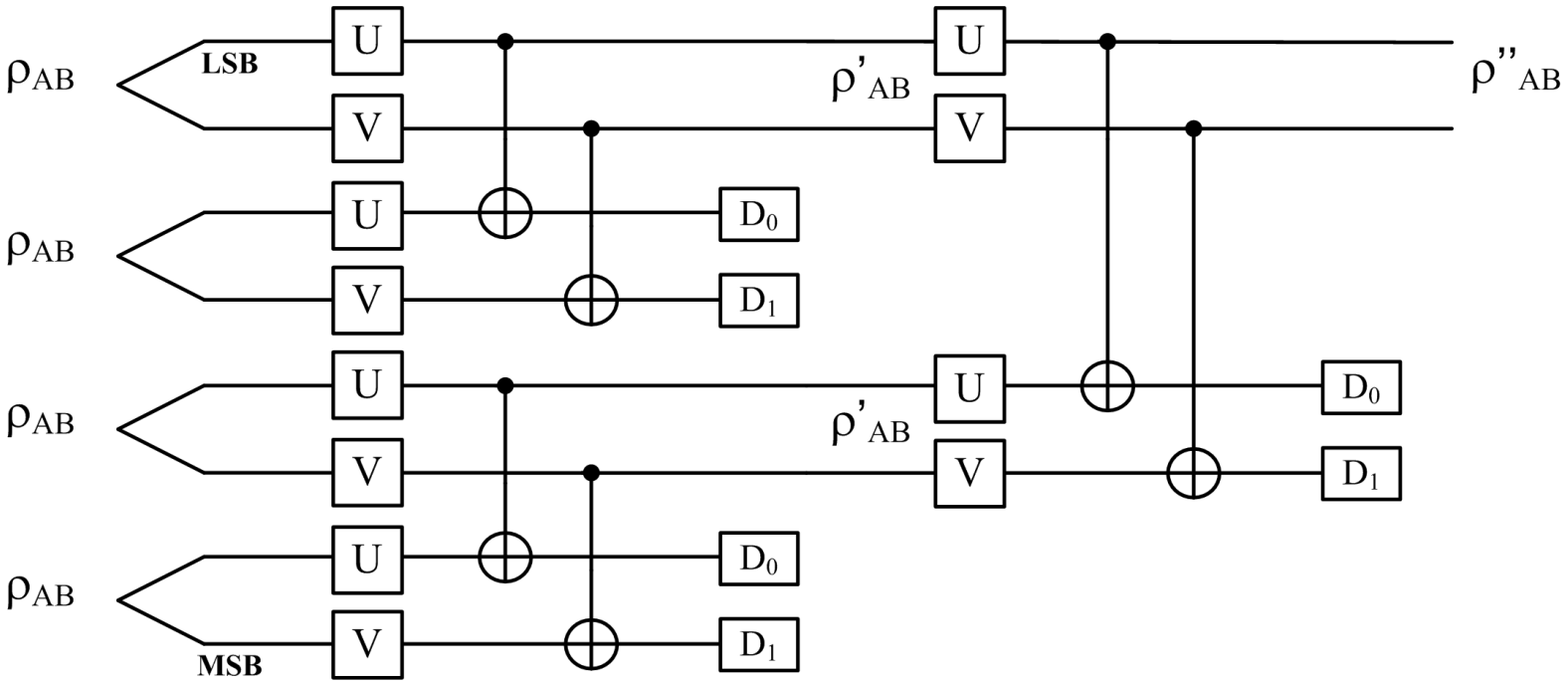

- The initial mixed pairs are described by the density matrices $\rho_{AB}$
- The two communicating parties locally perform rotations and CNOT gates
- The two most significant qubits are measured
- The final output is a purified state $\rho'_{AB}$, when the detectors $D_0$ and $D_1$ give the same outcomes

# QPA Protocol: Diagram of States



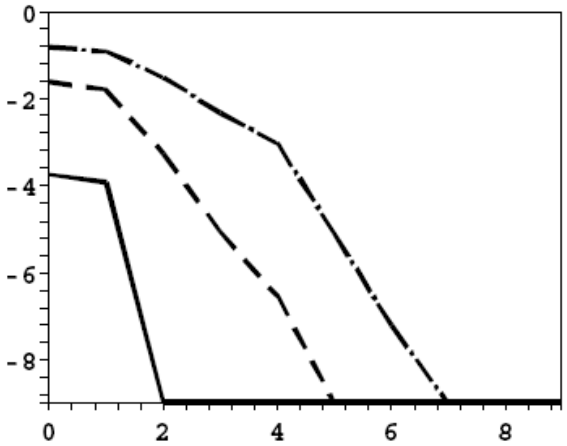

- Purification of imperfect state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- $|\Phi^+\rangle$ components determine the **active information** lines
- The purified output state is determined by **constructive** and **destructive interference** caused by Hadamard gates (arrows at the bottom)

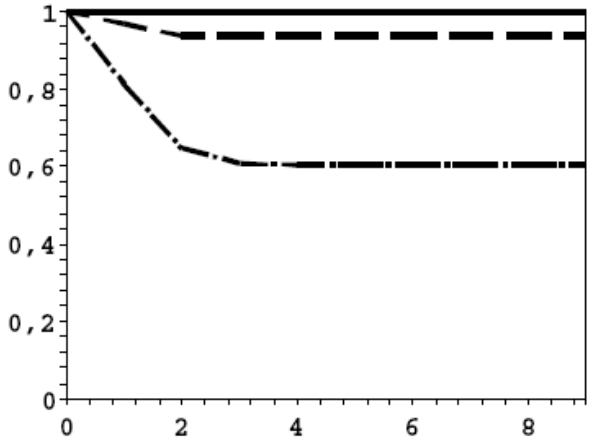
# QPA Iterations




- Quantum circuit implementing **two iterations** of the QPA protocol
- At least $2^n$ **imperfect pairs** are needed in input to obtain in output one purified pair after $n$ **iterations**
- This number can be significantly larger – pairs must be **discarded** whenever Alice and Bob obtain **different measurement outcomes**

# Fidelity and Survival Probability




**Deviation** $1 - F$ of the **fidelity**

$$F = \langle \Phi^+ | \, \rho'_{AB} \, | \Phi^+ \rangle$$

from its optimal value $F = 1$ on a logarithmic scale

**Survival probability**

$$P(n) = \prod_{i=1}^{n} p_i$$

with $p_i =$ probability of coinciding outcomes at step $i$

...both as a function of the number of iterations $n$ (horizontal axis)

- The protocol is successful for weak (solid line), middle (dashed line) and strong (dot-dashed line) eavesdropping intrusion or noise perturbation

# Conclusions and Bibliography

# Conclusive Remarks

- For any given quantum computation, **diagrams of states** offer both:
  - a **detailed description** of each gate action (complete diagram)
  - an **overall visualization** from input to output (simplified diagram)
- The diagram dimension **grows exponentially** in respect to the dimension of the examined quantum system:
  - **Clearer visualization** in respect to traditional descriptions
- Diagrams of states are **most useful** whenever quantum operations are described by **sparse matrices**:
  - Only **non-null entries** of matrices are associated with diagram lines
  - Only **significant information flow** and **processing** are shown
  - This requirement is indeed **satisfied by most quantum computations**

# References



[*] **Quantum Hacking Group**: http://www.iet.ntnu.no/groups/optics/qcr/, Department of Electronics and Telecommunications, NTNU, and UNIK – University Graduate Center.

[*] This work was carried out during the tenure of an **ERCIM** "Alain Bensoussan" **Fellowship Programme**.

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

[2] G. Benenti, G. Casati, G. Strini, *Principles of Quantum Computation and Information, Volume II: Basic Tools And Special Topics*, World Scientific, 2007.

[3] M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.

[4] S. Felloni, A. Leporati, G. Strini, *Diagrams of states in quantum information: An illustrative tutorial*, International Journal of Unconventional Computing, to appear.

[5] S. Felloni, A. Leporati, G. Strini, *Evolution of quantum systems by diagrams of states*, manuscript.

[6] S. Felloni, G. Strini, *Entanglement-based computations by diagrams of states*, manuscript.

[7] S. Felloni, G. Strini, *Quantum algorithms by diagrams of states: Deutsch's and Grover's algorithms*, submitted for publication.

[8] G. Benenti, S. Felloni, G. Strini, *Effects of single-qubit quantum noise on entanglement purification*, Eur. Phys. J. D 38, p. 389, 2006.