

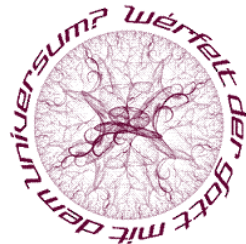
# Quantum Computing Workshop

Limiti e possibilità dei calcolatori quantistici  
Confronto tra diversi approcci ed implementazioni

La giornata di lavori sul calcolo quantistico è dedicata alla presentazione ed alla discussione di differenti approcci, metodi computazionali, teorie ed implementazioni sperimentali.

**Giovedì 27 Marzo 2008**

Dipartimento di Informatica, Sistemistica e Comunicazione  
Università di Milano - Bicocca  
Viale Sarca 336/14, 20126 Milano



## Programma

09.30	<i>Apertura</i>
09.45	Prima sessione
11.25	<i>Coffee break</i>
11.40	Seconda sessione
13.20	<i>Pranzo</i>
15.00	Terza sessione
16.40	<i>Coffee break</i>
16.55	Quarta sessione
18.30	<i>Chiusura</i>

## Prima Sessione

### **Il ruolo dell'universalità nelle diverse forme di quantum computing**

Si propone una riflessione critica sul ruolo della nozione di universalità e sulla Tesi di Church-Turing nella computazione naturale ed in particolare nelle diverse forme di computazione quantistica.

**Ignazio Licata**

*ISEM - Institute for Scientific Methodology, Palermo*

### **Il calcolo quantistico verso il mondo reale: la sfida dell'integrazione fotonica**

L'implementazione ottica dei futuri processori quantistici può essere competitiva rispetto alla maggior parte delle tecnologie concorrenti. Gli ultimi sviluppi della nanofotonica integrata rendono ancora più agevole tale percorso.

**Flavio Fontana**

*Cattedra Pirelli di Ingegneria Ottica e Fotonica*

*Dipartimento di Ingegneria Elettronica, Università di Pavia*

## Seconda Sessione

### **Two approaches to quantum estimation**

We present two approaches to two different problems of quantum estimation, the one based on a Maximum Likelihood reconstruction algorithm the other to the minimum Kullback relative entropy principle.

**Stefano Olivares**

*Applied Quantum Mechanics*

*CNISM UdR Milano Università*

*Dipartimento di Fisica, Università di Milano*

### **Local quantum estimation and applications**

In all the branches of physics, many quantities of interest are not directly accessible, either in principle or due to experimental impediments. In these cases, the determination of the most precise estimator unavoidably involves an optimization procedure.

**Matteo G. A. Paris**

*Applied Quantum Mechanics*

*Dipartimento di Fisica, Università di Milano*

## Terza Sessione

### Quantum Circuits Architecture

A method for optimizing quantum circuits architecture is presented. It is based on the notion of "quantum comb", a circuit board with inserted variable subcircuits, which corresponds to a generalization of the notions of quantum operation and POVM.

#### **Giacomo M. D'Ariano**

*Quantum Information Theory Group  
Istituto Nazionale di Fisica della Materia, Unità di Pavia  
Dipartimento di Fisica, Università di Pavia*

### Entanglement, randomness and chaos

Entanglement is not only the most intriguing feature of quantum mechanics, but also a key resource in quantum information science. We will discuss the relationship between entanglement, randomness and chaos.

#### **Giuliano Benenti**

*Center for Nonlinear and Complex Systems  
Dipartimento di Fisica e Matematica, Università dell'Insubria*

## Quarta Sessione

### Decoherence, inaccuracy and errors in quantum cryptography

We present a general single-qubit error model to study decoherence and noise effects in quantum information processing. We then perform a realistic noisy simulation of a cryptographic privacy amplification protocol based on entanglement purification.

#### **Sara Felloni**

*Dipartimento di Informatica, Sistemistica e Comunicazione, Università di Milano - Bicocca*

### Simulations of quantum systems and noisy error correcting codes

All possible single-qubit errors are applied to a quantum simulator for the resolution of the Schroedinger equation and standard error-correction codes are studied in the presence of multiple errors.

#### **Giuliano Strini**

*Dipartimento di Fisica, Università di Milano*

# Il ruolo dell'universalità nelle diverse forme di quantum computing

**Ignazio Licata**

*ISEM - Institute for Scientific Methodology, Palermo*

Si propone una riflessione critica sul ruolo della nozione di universalità e sulla Tesi di Church-Turing nella computazione naturale ed in particolare nelle diverse forme di computazione quantistica. La breve storia del QC ha posto in evidenza un apparente paradosso: pur essendo la fisica quantistica più generale e fondamentale della fisica classica, le capacità del QC non sembrano differire sostanzialmente da quelle della computazione tradizionale, se non per un mero fattore quantitativo.

La controversa questione delle capacità non-Turing del QC mostra una dipendenza critica dalla fisica del sistema considerato e notevoli differenze dalla potenzialità della computazione quantistica standard, se si considera un approccio basato sulla teoria quantistica dei campi.

L'universalità del QC diventa dunque un criterio per dirimere due tipologie di trattamento dell'informazione nei sistemi fisici, basate rispettivamente sulla QM e sulla QFT. Ciò porta a interessanti riflessioni sul legame profondo tra modello fisico e modello computazionale e sulla nozione di informazione quantistica dal punto di vista della QFT. Il paradosso della QC può quindi essere risolto riconsiderando il ruolo della tesi di Church-Turing nello studio dei processi di elaborazione dell'informazione nei sistemi fisici e classificando i modelli computazionali in base alla fisica del sistema considerato.



*Ignazio Licata è un fisico teorico, direttore dell'ISEM, Institute for Scientific Methodology per gli studi interdisciplinari a Palermo.*

*Si occupa di fondamenti della fisica quantistica, cosmologia, teoria dei sistemi, epistemologia, modelli matematici dei processi cognitivi e teoria della computazione nei sistemi fisici e biologici. Ha elaborato un nuovo approccio grupale alla cosmologia quantistica, ha proposto un modello di gas neurale evolutivo ed ha studiato gli aspetti Non-Turing dei processi informativi nel quantum computing e nei sistemi biologici.*

*Editor dell'Electronic Journal of Theoretical Physics e di QuantumBioSystems, è autore di Osservando la Sfinge (Di Renzo Editore, Roma, 2003) e di Mente & Computazione (Bologna, 2004).*

*E' uno degli organizzatori del progetto europeo Enhancing Research on Neural Networks and Cognitive Modelling based on Principles of Quantum Mechanics.*

## Il calcolo quantistico verso il mondo reale: la sfida della integrazione fotonica

**Flavio Fontana**

*Cattedra Pirelli di Ingegneria Ottica e Fotonica  
Dipartimento di Ingegneria Elettronica, Università di Pavia*

L'implementazione ottica dei futuri processori quantistici può essere competitiva rispetto alla maggior parte delle tecnologie concorrenti.

Gli ultimi sviluppi della nanofotonica integrata rendono ancora più agevole tale percorso.



*Flavio Fontana ha partecipato fin dall'inizio, come ricercatore presso i laboratori del Gruppo Pirelli, allo sviluppo dei sistemi di trasmissione ottica basati su amplificatori in fibra drogata con Erblio, contribuendo al successo mondiale di tale tecnologia, oggi universalmente diffusa.*

*Si è successivamente occupato di ottica nonlineare in fibra, con particolare riferimento alla generazione di impulsi ultracorti ad altissima frequenza di ripetizione, ed ha coordinato come Chief Scientist di Pirelli Labs importanti ricerche nell'ambito dell'Ottica Quantistica e della Nanofotonica.*

*Attualmente è titolare della Cattedra Pirelli di Ingegneria Ottica e Fotonica presso l'Università di Pavia, dove continua le sue attività di studio nelle aree del calcolo quantistico ottico e dei dispositivi a cristallo fotonico e ad alto contrasto d'indice.*

## Two approaches to quantum estimation

**Stefano Olivares**

Applied Quantum Mechanics  
CNISM UdR Milano Università  
Dipartimento di Fisica, Università di Milano

In all the branches of physics, many quantities of interest are not directly accessible, either in principle like the measurement of all fields or due to experimental impediments. In these cases, one should resort to indirect measurements, thus obtaining a parameter estimation problem. We present two approaches to two different problems of quantum estimation, the one based on a Maximum Likelihood reconstruction algorithm the other to the minimum Kullback relative entropy principle.



Stefano Olivares è ricercatore (CNISM) presso il gruppo di Applied Quantum Mechanics del Dipartimento di Fisica dell'Università degli Studi di Milano, dove ha conseguito il Dottorato di Ricerca in Fisica e, in seguito, ha lavorato nello stesso gruppo per quattro anni come post-doc.

E' un fisico teorico e lavora nell'ambito dell'informazione quantistica e dell'ottica quantistica. I suoi contributi principali riguardano i campi della stima quantistica di stati e operazioni, della generazione e di applicazioni dell'entanglement, della gestione e della manipolazione dell'informazione quantistica e della decoerenza. Collabora attivamente con diversi gruppi teorici e sperimentali sia nazionali che internazionali.

Nel 2005 è stato insignito del premio "Le Scienze" per l'Ottica Quantistica e della medaglia del Presidente della Repubblica Italiana.

# Local quantum estimation and applications

**Matteo G. A. Paris**

*Applied Quantum Mechanics  
Dipartimento di Fisica, Università di Milano*

In all the branches of physics, many quantities of interest are not directly accessible, either in principle like the measurement of all fields or due to experimental impediments. In these cases, one should resort to indirect measurements, thus obtaining a parameter estimation problem whose solution, the determination of the most precise estimator, unavoidably involves an optimization procedure.

After reviewing classical Cramer-Rao inequality we address local quantum estimation and evaluate the quantum Fisher information in several situations of interest for quantum information processing. Connection with global quantum estimation is explored and properties of Bayesian estimators are illustrated.



*Matteo Paris è ricercatore presso il dipartimento di Fisica dell'Università di Milano, dove coordina un gruppo di ricerca in quantum information composto attualmente da cinque persone.*

*Si occupa di teoria quantistica dell'informazione e della stima e delle applicazioni in sistemi ottico-quantistici.*

*Insegna quantum information agli studenti della laurea magistrale in Fisica.*

# Quantum circuits architecture

**Giacomo M. D'Ariano**

Quantum Information Theory Group  
Istituto Nazionale di Fisica della Materia, Unità di Pavia  
Dipartimento di Fisica, Università di Pavia

A method for optimizing quantum circuits architecture is presented.

The method is based on the notion of "quantum comb", which describes a circuit board in which one can insert variable subcircuits, and mathematically corresponds to a generalization of the notions of quantum operation and POVM.

The method allows to address novel kinds of quantum processing tasks, such as optimal storing-retrieving and cloning of channels, optimal quantum circuit board testers.

Quantum combs also describe single party strategies in quantum protocols, and quantum algorithms. A proposal for a provable optimal algorithm minimizing the number of oracle calls is presented.



*Giacomo Mauro D'Ariano is a Professor of Quantum Optics, Physics and Theory of Information, and Foundations of Quantum Mechanics.*

*He is also founder and leader of the Quantum Optics and Information Group (currently QUIT) of the Istituto Nazionale di Fisica della Materia (INFN) at Pavia.*

*He started Quantum Optics and Quantum Information at Pavia University, conceived and developed the first exact quantum homodyne tomographic method, generalized the method to arbitrary quantum system and arbitrary ensemble average. He conceived the first feasible method for experimental characterization of quantum devices. He introduced novel theoretical methods to deal with covariant measurements and transformations, which has recently lead him and his group to the solution of the long-standing problems of phase-estimation and broadcasting of mixed states of qubits.*

# Entanglement, randomness and chaos

**Giuliano Benenti**

Center for Nonlinear and Complex Systems  
Dipartimento di Fisica e Matematica, Università dell'Insubria

Entanglement is not only the most intriguing feature of quantum mechanics, but also a key resource in quantum information science. In particular, for quantum algorithms multipartite (many-qubit) entanglement is necessary to achieve an exponential speedup over classical computation. The entanglement content of random pure quantum states is almost maximal; such states find applications in various quantum information protocols.

The preparation of a random state or, equivalently, the implementation of a random unitary operator, requires a number of elementary one- and two-qubit gates that is exponential in the number  $N$  of qubits, thus becoming rapidly unfeasible when increasing  $N$ . On the other hand, pseudo-random states approximating to the desired accuracy the entanglement properties of true random states may be generated efficiently, that is, polynomially in  $N$ . In particular, quantum chaotic maps are efficient generators of multipartite entanglement among the qubits, close to that expected for random states.

We will discuss the relationship between entanglement, randomness and chaos. In particular, we will show that the entanglement generated by chaotic maps is robust when taking into account the unavoidable noise sources affecting a quantum computer. We also discuss the detection of the entanglement of random states using witness operators. Our results can be also used to explain the emergence of classicality in coarse grained quantum chaotic dynamics.



*Giuliano Benenti è ricercatore in fisica teorica presso l'Università degli Studi dell'Insubria, sede di Como, dal 2002.*

*Ha conseguito la laurea in fisica presso l'Università di Pavia (1993) e il dottorato in fisica presso l'Università di Milano (1998). Post-doc a Saclay, Francia (1998-2000); visiting presso il CNRS, Tolosa (2000, 2002), l'ITP, Santa Barbara (2001), l'Istituto Poincaré, Parigi (2006).*

*E' coautore, insieme a Giulio Casati e Giuliano Strini, di Principles of Quantum Computation and Information, Vol. I: Basic Concepts (World Scientific, Singapore, 2004) e Vol. II: Basic Tools and Special Topics (World Scientific, Singapore, 2007).*

# Decoherence, inaccuracy and errors in quantum cryptography

**Sara Felloni**

*Dipartimento di Informatica, Sistemistica e Comunicazione,  
Università di Milano-Bicocca*

We present a general single-qubit error model to study decoherence and noise effects in quantum information processing. Since a general transformation of a single-qubit density matrix can be described by twelve parameters, we associate a noise channel to each parameter and we represent each channel by means of quantum circuits and density matrices transformations.

After the characterization of all physically possible single-qubit errors, we perform a realistic noisy simulation of a privacy amplification protocol in quantum cryptography, based on entanglement purification. We assume that two communicating parties use an EPR cryptographic protocol, in which decoherence, noise effects or eavesdropping attacks can reduce the quality of information. Entanglement purification is then operated by means of the quantum privacy amplification protocol.

We study the stability under quantum noise effects of this quantum cryptographic protocol by presenting a systematic numerical study of the impact of all possible single-qubit noise channels. We find that both the qualitative behavior of the fidelity of the purified state as a function of the number of purification steps and the maximum level of noise that can be tolerated by the protocol strongly depend on the specific noise channel applied. The protocol shows good performances even in the presence of strong errors and without the application of any errors correction.



*Sara Felloni graduated cum laude in Mathematics in 2005 at the University of Milano. Now she is a PhD student with ministerial scholarship in Informatics, at the University of Milano - Bicocca, since November 2005.*

*She is working on a PhD thesis in Quantum Computing entitled “Decoherence, Inaccuracy and Errors in Quantum Information Processing”, supervised by Prof. Giuliano Strini (Dipartimento di Fisica, Università degli Studi di Milano) and Dr. Alberto Leporati (Dipartimento di Informatica, Sistemistica e Comunicazione, Università degli Studi di Milano - Bicocca).*

# Simulations of quantum systems and noisy error correcting codes

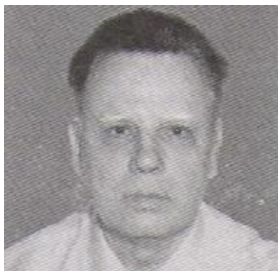
**Giuliano Strini**

*Dipartimento di Fisica, Università di Milano*

The first quantum computers are predicted to be very noisy. After the characterization of all single-qubit errors, here we describe some simulations aiming to understand the possible effects of various source of quantum noise.

All physically possible single-qubit errors are first applied to a quantum simulator for the solution of the Schrodinger equation. We find that only six qubits are sufficient to build a quantum simulator able to simulate interesting dynamics. This exceptionally small number of qubits also allows to include our single-qubit error model and to describe the system by means of the density matrix representation. Surprising results are found: the quantum system can be successfully treated even if affected by strong perturbation and shows good performances without requiring any errors correction. Furthermore, we find a tolerable noise threshold much higher in respect to the theoretical noise threshold necessary for more general fault-tolerant quantum computations.

Similar studies are then performed on widely known quantum error correcting codes, to discover which noise channels might be more dangerous for the considered codes. We aim to explore the effects of multiple errors on error correcting codes: some preliminary computations had been performed and the results seem to be promising.



*Giuliano Strini è professore associato in Fisica Sperimentale ed è titolare di corsi di Calcolatori Quantistici presso l'Università degli Studi di Milano.*

*Dal 1963 ha collaborato alla costruzione e allo sviluppo del Ciclotrone di Milano. E' membro dell'Italian Physical Society e dell'Optical Society of America.*

*Le sue pubblicazioni sono inerenti a nuclear reactions, nuclear spectroscopy, gravitational waves detection, quantum optics, quantum computing.*

*E' coautore, insieme a Giuliano Benenti e Giulio Casati, di Principles of Quantum Computation and Information, Vol. I: Basic Concepts (World Scientific, Singapore, 2004) e Vol. II: Basic Tools and Special Topics (World Scientific, Singapore, 2007).*