# Quantum Information Science

## *16 August to 17 December 2004*

***Report from the Organisers:***
*CH Bennett (IBM), DP DiVincenzo (IBM), N Linden (Bristol) and S Popescu (Bristol)*

*CH Bennett, N Linden and S Popescu*

## *Scientific Background*

Quantum information science is a new field of science and technology to which physicists, mathematicians, computer scientists and engineers have made major contributions. It undertakes to develop the theory and practice of information processing for information carriers (in the simplest case, 2-state quantum systems or 'qubits') that, unlike the bits of classical information theory, but like the real physical systems they exemplify, are capable of superposition and entanglement. Deep links between the previously unrelated disciplines of quantum physics and computer science/information theory have been forged, leading on the one hand to insights into fundamental issues in physics and on the other to hitherto unsuspected kinds of computation and communication. New technologies have arisen offering the potential for unconditionally secure communications and dramatic speedups of some computational tasks such as integer factorisation and search.

Quantum information science is one of the most dynamic areas in the physical sciences, with new ideas and phenomena appearing at a remarkable rate. There are also very many open questions and fundamental issues to be understood. Some of the questions and challenges on which the programme focussed were:

- characterising and quantifying non-local properties of quantum states and operations;
- understanding which features of quantum mechanics are responsible for the power of quantum computation and communication;
- developing new quantum algorithms;
- identifying novel tasks in which the physical nature of the qubit is important (recent examples include reference frame alignment and clock synchronisation);
- calculating the capacities of quantum channels, and identifying new communication tasks, particularly in multi-party settings;
- investigating distributed and interactive computation;
- identifying cryptographic tasks which are candidates for novel quantum protocols.

## *Structure of the Programme*

The programme was large and multi-faceted, including 43 long-stay visitors (of whom 12 were from the UK), 112 short-stay visitors (40 from the UK), five workshops (several of which were filled to capacity or overbooked), a Rothschild lecture, other lectures and tutorials, regular seminars, satellite meetings, and new collaborations establishing links between different communities.

S Wilkinson

*Participants at the 'Special Week on Quantum Cryptography'*

# Workshops

## *Quantum Information Theory: Present Status and Future Directions*

**Workshop, 23–27 August 2004**

Organisers: S Massar, N Linden and S Popescu

This workshop, held strategically near the start of the programme in order to give an overview of the field, was one of the main events. It consisted of about 30 invited talks by the leading experts in the theory of quantum information, and brought together theoretical physicists, computer scientists and mathematicians to discuss the current status of the field and present important recent developments. Despite substantial progress in the last few years, there are also very many open questions and fundamental issues to be understood. For this reason the speakers were encouraged to review in their talks the major challenges in the field.

Subjects covered by the workshop included quantum algorithms and algorithmic techniques, quantum communication and quantum cryptography, quantum entanglement and non-locality, fault-tolerant quantum information processing and communication, quantum information processing and quantum operations under constraints (for instance imposed by the physical system in which they are realised).

## *Special Week on Quantum Cryptography*

**Focus Week, 6–10 September 2004**

Organisers: A Kent, J Oppenheim and R Colbeck

Twenty leading theorists gave seminars during this Special Focus Week, which also featured some memorable informal discussions. Among the topics considered were novel security proofs for quantum key distribution, the problem of composability of elementary quantum cryptographic primitives, quantum protocols which attain cheat sensitivity (a novel form of security with no precise classical analogue), the phenomena of quantum locking and unlocking and their uses, and the striking discovery of quantum key distribution protocols which are provably secure even if quantum theory is incorrect (so long as superluminal signalling is impossible). Extensive informal discussions covered these topics and many others, including the subtleties which arise in abstractly modelling the properties of mistrustful quantum cryptographic tasks such as quantum bit commitment, and various types of security that might be attainable in tasks such as secure multi-party quantum computation. The workshop was generally agreed to be a great success, and the scope for informal discussion alongside formal presentations was much appreciated.

## *Entanglement and Transfer of Quantum Information*

**Workshop, 26–30 September 2004**

Organisers: DP DiVincenzo, M Plenio and A Briggs

Crucial to any implementation of quantum information processing are the controlled creation of entanglement between qubits and the controlled transfer of quantum information, in particular between stationary qubits and propagating qubits. Photons are the most natural candidates as propagating qubits for long-range communication, but for short-range communication other approaches may be taken such as moving matter qubits or excitations in systems of interacting particles. For static qubits there is a wide range of

possibilities, ranging from nuclear and electron spin to single and collective excitations. With many candidates being available, optimal choices have yet to be identified for both static and flying qubits. The workshop was organised by the Quantum Information Processing Interdisciplinary Research Collaboration (QIP IRC) together with the Isaac Newton Institute to provide a forum for discussions with the aims of reviewing leading experimental programmes within the theme of entanglement and transfer of qubits, relating these to theoretical developments in quantum information processing, and identifying promising roads towards the controlled entanglement and transfer of quantum information.

The workshop was very successful. It attracted a large enthusiastic participation, including many of the worldwide experts in the field. The interdisciplinary topics were carefully grouped. The following represent some (though by no means all) of the new results presented.

- Electron charge: Rabi oscillations can be demonstrated in a gated charge qubit in GaAs. Using the gate potentials, full manipulation over the Bloch sphere can be achieved. Phosphorous atoms can be deposited in subsurface sites in silicon to make a classical two-state charge system with potential as a qubit. Electron charge can be manipulated in nanotubes, and can demonstrate quantum spin-charge effects such as Kondo resonance and coulomb blockade.

- Electron spin: quantum information can be embodied in electron spins in compound semiconductors. The spins can propagate, and single electron spins in quantum dots can be measured through a nearby quantum point contact. Electron spins in molecular materials have long lifetimes, and can be manipulated with exquisite precision using pulse sequences derived from NMR such as BB1. Endohedral fullerenes give further quantum effects when placed inside nanotubes.

- Experimental and theoretical progress is being made in the use of atom chips to produce controlled and localised Bose–Einstein condensates with potential for quantum computing.

- Several matter-based qubits can be read out optically. Spin-qubits in N-V centres in diamond can be manipulated through ESR, and the result can be read out using a spin-dependent optical transition. A two-qubit operation has been performed with the nuclear spin of a $^{13}C$ atom in the vicinity.

- The interaction between photons and single ions is being exhibited in a range of systems. Entanglement of a photon and the qubit in a trapped ion has been demonstrated.

- Teleportation of quantum information in ion traps has been demonstrated in two laboratories, together with four-qubit algorithms. Scaleable schemes for ion trap computing have been developed, and simulations have been run. Distributed entanglement offers potential.

- Linear optical computing offers enormous challenges. Progress is being made in the conditional preparation of single photons, and there is both theoretical and experimental progress in reducing the considerable demands of efficient implementation.

- Superconducting qubits are perhaps the most mature solid-state implementation. There is now great control of flux qubits, with long ratios of coherence time to gate operation time, and potential for scaleable qubit–qubit interactions.

- New schemes have been developed for globally addressed quantum computing, which are now much more robust and versatile, and for quantum communication in rings of qubits with defined interactions.

- Quantum communication involving up to five qubits in optical fibres has been demonstrated, though without satisfactory photon-on-demand sources it is extremely slow.

Several of the delegates said that this had been the best QIP conference they had ever attended. They particularly commended the open structure of the conference, with plenty of discussion time both

inside and outside the formal sessions. The speakers were also commended on ensuring that their material was accessible to the whole of the multidisciplinary audience, while including many results announced for the first time. Where the invited 'big name' was unable to accept, we adopted a policy of encouraging them to nominate an active researcher in their group to come and give a presentation. In this way we achieved a good age distribution among the speakers, which further contributed to the lively debate and discussion. A number of new collaborations have arisen out of discussions at the workshop.

The original motive for the workshop was to foster dialogue with the mathematicians and theorists attending the Newton Institute programme. There were 122 delegates, including 22 programme participants. The organisers were deeply grateful to the Institute staff for superb organisation, and to DARPA and ONR for sponsorship. Many talks are available online at the Newton Institute website.

### *Quantum Statistics – Quantum Measurements, Estimation and Related Topics*

**Focus Week, 15–19 November 2004**

Organisers: VP Belavkin, RD Gill and A Winter

The three organisers of this event came, roughly speaking, from mathematical physics, mathematical statistics, and quantum information proper. The meeting served to bring together the subcommunity in quantum information science of people interested in quantum statistical estimation (estimation or tomography of states or operations or even measurements), and was perhaps the first ever of such meetings. This is a scattered subcommunity, so many researchers had here an opportunity to meet colleagues they had not seen before (and in quite a few cases not heard of before!), and the meeting served as a forum to establish the state of the art. It certainly has initiated several new scientific collaborations.

In particular there was a major contingent of researchers from Japan, where there is a long-established and advanced school in quantum state estimation but whose works (rather mathematical and using sophisticated geometrical methods) are almost unknown to the theoretical physicists in the field.

CH Bennett

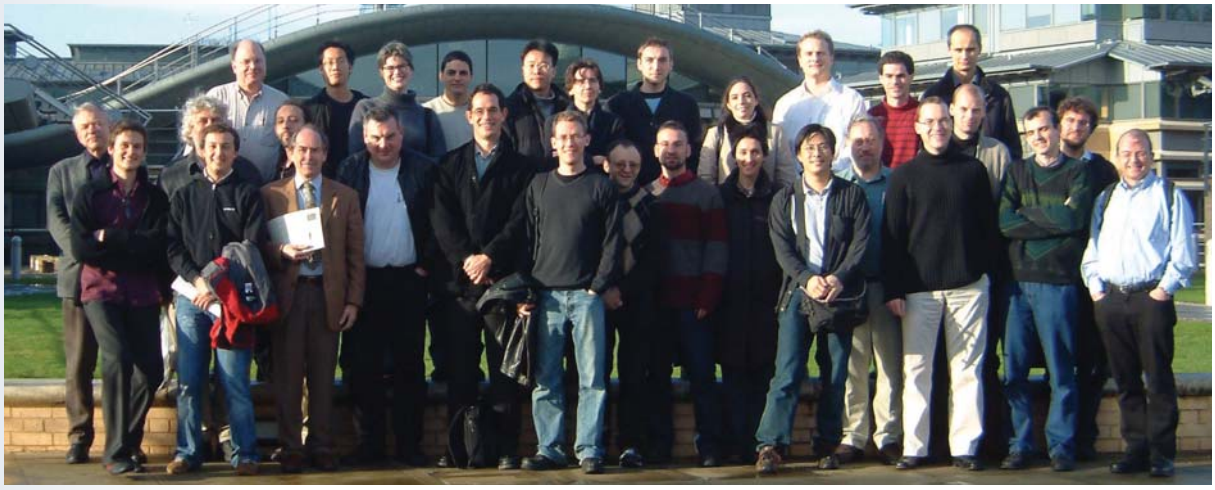
*SW Hawking and colleagues*

Particularly gratifying was the participation in the meeting of a number of mathematical statisticians, and among them several young people just starting doctoral or postdoctoral research without prior exposure to quantum information. We believe that the meeting has laid the seeds of important future cross-fertilisation between statistics and quantum information.

One of the scientific highpoints of the meeting was the presentation by Masahito Hayashi (Tokyo) of new results on Alexander Holevo's quantum Cramér–Rao bound, which was first published in 1980. This rather obscure (indeed, rather unappetising) bound has lain dormant for twenty-five years, no-one realising its significance. It now turns out to be *the* asymptotically sharp bound for the quality of the best possible reconstruction of a state based on collective (entangled) measurements. The connection goes via a quantum central limit theorem (approach to Gaussianity) and the fact that the bound is sharp for Gaussian states.

Further very exciting results were presented by Denes Petz on quantum sufficiency, and by Mauro D'Ariano on the tomography (calibration) of measurements. One particular unofficial topic of many discussions was the perspective for deriving a theory of distance between, and convergence of, quantum statistical models, which should generalise the classical statistical theory of L LeCam and give a framework that would organise the scattered results on asymptotic optimality. Another major unofficial topic was the question of $1/N^2$ rate estimation (for the fidelity or squared error) of an unknown unitary based on $N$ copies, a kind of quadratic speed-up in a quantum estimation problem, derived from entanglement.

S Wilkinson



*Participants at the workshop 'Quantum Gravity and Quantum Information'*

### *Quantum Gravity and Quantum Information*

**Focus Week, 14–17 December 2004**

Organiser: J Oppenheim

This meeting explored the interface between quantum gravity, quantum information and the foundations of quantum mechanics. Topics included black hole information, the measurement problem in a gravitational setting, quantum geometry, and big bang cosmology. Part of the objective was to provide a space where researchers in quantum gravity and quantum information could explore areas of common interest and identify worthwhile avenues of research.

There were some talks given by both well known and established researchers (Gerard t'Hooft, Roger Penrose, Seth Lloyd, Renate Loll, Neil Turok and Bill Unruh) and others given by up-and-coming researchers (Christophe Galfard, Daniel Gottesman, Fotini Markopoulou, Ralf Schützhold and Daniel Terno). Additionally, there were shorter, more informal talks (some at the public blackboards) designed to encourage interaction between researchers. These included talks by Florian Girelli, Ivette Fuentes Guridi, Louis H Kauffman, Viacheslav Belavkin, Jonathan Oppenheim, Martin Plenio, John Smolin and Charlie Bennett.

A number of the talks announced work being made public for the first time. Highlights included the talk of Christophe Galfard who presented his work with Stephen Hawking and Christiano Germani on the black hole information paradox. Since Hawking's public announcement and talk in Dublin at GR17, the work had generated considerable discussion, and this was the first time details were presented. Another highlight was the talk of Bill Unruh who presented a potential bound on determining the state of black hole radiation.

## *Outcome and Achievements*

The programme and its associated workshops were extremely productive, and it is very difficult to summarise the results: we do apologise to those participants whose work we haven't succeeded in representing appropriately. Some of the highlights follow.

The Newton Institute provided a special atmosphere facilitating the transfer of ideas between the usual narrow fields of specialisation. At the Institute, people can learn ideas outside their area by having them explained slowly and repeatedly by their authors. This allowed unexpected common themes to emerge, with different people applying the same idea in different domains. Some such major themes that emerged were locking of resources, general non-locality, additivity properties and fault-tolerant quantum computation.

### Locking

The Horodecki family, together with Jonathan Oppenheim, continued their investigation into the phenomenon of locking of entanglement measures that they discovered shortly before the start of the programme. Locking represents a paradigm shift in quantum information. Hitherto it was known that

different information resources can be traded one for another, but it was thought that in order to gain access to some resource one needs to pay a proportional amount of another resource. Unlocking means that one can gain access to arbitrarily large amounts of some resource by paying a very limited amount (say 1 bit) of another resource (the key).

Berry Groisman, Noah Linden, Sandu Popescu and Andreas Winter, together with the Horodecki family, investigated the implications of locking the entanglement of formation for multi-partite entanglement concentration. Multi-partite entanglement concentration is one of the most important open problems in quantum information. They analysed what is widely considered to be the simplest non-trivial problem in the field, a problem that defied solution for almost a decade. They showed that either entanglement of formation is lockable in a far simpler situation than the one suggested by Jonathan Oppenheim and the Horodecki family, or multi-particle reversible concentration is impossible, which then requires a drastic revisiting of the basic paradigm of quantum information, namely entanglement as a resource.

The very same problem, but from a completely different angle, was studied by John Smolin, Frank Verstraete and Andreas Winter. They derived the first general capacity theorems for multi-partite concentration and channels with classical assistance from the environment. Adrian Kent and Debbie Leung investigated the implication of locking in quantum cryptography. John Smolin considered the effect of locking of quantum information in quantum gravity, specifically on the black hole information paradox.

Finally, in related work right at the end of the programme, Michal Horodecki, Jonathan Oppenheim and Andreas Winter made their remarkable discovery that quantum information can be negative. The primitive they introduced, quantum state merging, also allowed them to solve several famous open problems in information theory, for example in distributed compression and quantum multiple access channels.

### Non-locality

From the very early days, entanglement and quantum non-locality have been recognised as the most important aspects of quantum mechanics as far as quantum information is concerned. This year, however, witnessed a new twist – the study of non-locality *per se*, i.e., all kinds of non-local correlations, not only those arising from quantum mechanics. Of course, non-locality that cannot arise from quantum mechanics doesn't exist in Nature, if Nature is quantum mechanical; nevertheless, the study of these hypothetical correlations turned out to be very useful since it offers a new perspective over what quantum non-locality actually is. The discovery of non-quantum non-local correlations, initiated by Popescu and Rohrlich, dates back about fifteen years, but it was only during the Newton Institute programme that their study really took off; and indeed it became a major theme of the programme.

Harry Buhrman, Richard Cleve, Noah Linden and Falk Unger considered the extremal case of non-local correlations, 'maximally non-local boxes'. They showed that in the presence of such non-local boxes any communication complexity function can be computed with just 1 bit of communication even if the non-local boxes have error around 5%, significantly improving van Dam's original proof that required perfect boxes. Based on this result, they went on to establish a new threshold for fault-tolerant classical computation. In discussions with Dan Gottesman, this result was then generalised to show that a (distributed) Clifford circuit quantum computation can be simulated with just one bit of communication and quantum entanglement, and used this result to derive the best known upper bounds on the quantum fault-tolerant threshold error probability.

Nicolas Gisin, Serge Massar, Sandu Popescu and Tony Short invented the idea of non-local 'couplers', the equivalent in the space of generalised non-locality of the quantum measurements with entangled eigenstates.

### Additivity Properties of Channels

Channel capacities and additivity properties have long been one of the core issues of quantum information. Charles Bennett and Andreas Winter characterised the tradeoff between sender–receiver shared randomness and classical forward communication required for simulating a classical channel. This long-neglected area of classical

S Wilkinson

*The Horodecki family. Left to right: P Horodecki, K Horodecki, R Horodecki, M Horodecki*

information theory has acquired new interest through its quantum generalisation, the problem of entanglement-assisted simulation of quantum channels. Further work at the Institute led to generalisation of the classical and quantum reverse Shannon theorem, especial to feedback channels in which the channel environment is returned to the sender in a manner called 'coherent classical communication' by Aram Harrow.

Mary Beth Ruskai considered questions about quantum channels, particularly capacity and related mathematical questions about $p$-norms and quantum entropy. She obtained a new additivity result; a simpler, alternative proof of the same result was then made by her together with Igor Devetak. Furthermore, Mary Beth Ruskai and Nilanjana Datta discovered and analysed a new class of channels in $d$ dimensions. Keiji Matsumoto studied the additivity problem from a $p$-norm based approach. Alexander Holevo's main interest was in the additivity properties of channels, in particular the classical capacity, the minimal output entropy and the entanglement of formation. All known results are consistent with the conjecture that these quantities are additive. A proof of this conjecture would have important consequences in quantum information.

### Fault-tolerant Quantum Computation

Since the presence of noise and faults in the functioning of gates is unavoidable, finding ways for performing fault-tolerant quantum computation is a most important issue. The basic principles were established about five years ago, but the results were very complicated and only a very small number of researchers actually understood them. This programme witnessed a renewed interest in the subject, with a large community becoming attracted to it. Many people were involved in almost daily discussions devoted simply to learning the subject. At the same time notable progress was made by John Preskill on a proof of the threshold theorem.

### Other Topics

Quantum cryptography was another of the major subjects discussed during the programme. Nicolas Gisin, Daniel Gottesman, Adrian Kent, Masato Koashi, Debbie Leung and Hoi-Kwong Lo worked on various new cryptographic protocols.

Interesting progress was made not only in the main themes of the programme but also in a wide variety of other topics in the field. For example, during the last couple of years, continuous variables have proved very useful tools for quantum information processing. Peter Knight has been working on how to enhance the non-classical properties of Gaussian states; discussions with Nicholas Cerf and Serge Massar led to a new approach to this problem by Knight and Myungshik Kim. Using NMR techniques for quantum computation was one of the earliest methods in the area; Tim Havel worked on experimental methods of quantum control in nuclear spin systems; and Raymond Laflamme has been interested in the amount of noise that would destroy entanglement in a higher dimension GHZ state in order to use this as a criterion for the performance of NMR experiments. Richard Jozsa studied quantum algorithms from a novel point of view. Most work to date on quantum algorithms has focussed on time complexity benefits. However, it is believed that no quantum process will be able to solve any NP-hard problem efficiently. Hence he realised that it is of much interest to identify further kinds of computational benefit such as parallelisability and efficient use of space; both these properties, which have been studied in classical computation theory, show unexpected behaviour in the quantum domain. Tony Sudbery worked on compatibility of subsystem states; results on the same subject were obtained by Matthias Christandel, Graeme Mitchison, Sumit Daftuar and Patrick Hayden.

CH Bennett

*Some of the key programme participants*

Quantum information is a very interdisciplinary subject, with close interaction between theoretical physicists, experimental physicists from very diverse areas, researchers in (classical) information, cryptographers and computer scientists. However, historically, most major advances in physics have opened, or at least significantly encouraged the development of, entire new areas of mathematics. It was our feeling that the time is now ripe for interaction between researchers in the quantum information community and pure mathematicians, and we made this one of the explicit aims of the programme. A number of pure mathematicians were invited and some of them spent extensive time on the programme. While it is yet early days, some notable results have been obtained. Louis Kauffman studied issues in quantum computation from the point of view of topology and knot theory. He accomplished a reformulation of the Freedman–Kitaev–Fibonacci model for quantum computing in terms of *q*-deformed spin networks and the coloured Jones polynomial. Furthermore, Lomonaco and Kauffman worked on braiding, spin networks and topological quantum computation, while Lomonaco also worked on vector fields of quantum entanglement. Roger Howe studied the issue of mutually unbiased bases.

A very positive outcome of the programme was the emergence of the connection of quantum information with mathematical statistics. Estimating quantum states is one of the central problems in quantum information. The problem is very different from classical statistical ones because of the fact that sampling some parameters characterising the quantum states necessarily precludes sampling of other parameters. A number of major results have been obtained during the last couple of years; they were obtained with very simple tools, starting effectively from scratch. Very recently however, as became apparent during the programme and its associated workshop on statistics, a number of statisticians have joined the effort, adapting to these new problems powerful statistical methods hitherto unknown in the quantum information community. Consequently many important new results have been obtained, as well as a systematisation of the old results.

## Conclusion

Overall, the programme has initiated many fruitful collaborations, and it is already clear that they are having lasting impact on the scientists involved. Work done during the programme has already resulted in many e-prints and manuscripts submitted for publication, and will likely be remembered as a high point in the development of the field. It will also be remembered for having given experts in related fields who were previously unfamiliar with quantum concepts the opportunity to familiarise themselves deeply with quantum concepts and begin contributing to this new field in their own right.