Quantum Information Technology[1]

Timothy Spiller
Trusted E-Services Laboratory
HP Laboratories Bristol
HPL-2002-319
November 20th , 2002*

E-mail: ts@hplb.hpl.hp.com

quantum information, quantum computing, quantum cryptography, quantum teleportation

A new quantum information technology (QIT) could emerge in the future, based on current research in the fields of quantum information processing and communication (QIPC). In contrast to conventional IT, where quantum mechanics plays a support role in improving the building blocks, fundamental quantum phenomena play a central role for QIPC - information is stored, processed and communicated according to the laws of quantum physics. This additional freedom could enable future QIT to perform tasks we will never achieve with ordinary IT. This article provides an introduction to QIPC, some indication of the state of play today, and some comments on the future.

* Internal Accession Date Only
[1] Materials Today, 2002

Approved for External Publication

Quantum Information Technology

Timothy P. Spiller*
Hewlett-Packard Laboratories,
Filton Road, Stoke Gifford,
Bristol BS34 8QZ, UK.

Abstract
A new quantum information technology (QIT) could emerge in the future, based on current research in the fields of quantum information processing and communication[1-3] (QIPC). In contrast to conventional IT, where quantum mechanics plays a support role in improving the building blocks, fundamental quantum phenomena play a central role for QIPC – information is stored, processed and communicated according to the laws of quantum physics. This additional freedom could enable future QIT to perform tasks we will never achieve with ordinary IT. This article provides an introduction to QIPC, some indication of the state of play today, and some comments on the future.

1 Introduction – Moore's Law and beyond

Today many people are familiar with at least the consequences of Moore's Law – the fastest computer in the shops doubles in speed about every 18 months to two years. This is because electronic component devices are shrinking. The smaller they get, the faster they work, and the closer they can be packed on a silicon chip. This exponential progress, first noted[4] by Gordon Moore, a co-founder and former CEO of Intel, in 1965, has continued ever since. But it cannot go on forever. Hurdles exist, for example: silicon will hit problems, with oxide thinness, track width, or whatever;[5] new materials or even new paradigms, such as self-assembled nano-devices or molecular electronics, will be needed; lots of dollars will be needed, as Moore's second law tells us that fabrication costs are also growing exponentially. However, even if all the hurdles can be overcome, we will eventually run into Nature.

Very small things do not behave the same way as big ones – they begin to reveal their true quantum nature. Following Moore's Law, an extrapolation of the exponentially decaying number of electrons per elementary device on a chip gets to one electron per device around 2020. This is clearly too naïve, but it gives us a hint. Eventually we will get to scales where quantum phenomena rule, whether we like it or not. If we are unable to control these effects, then data bits in memory or processors will suffer errors from quantum fluctuations, and devices will fail. Clearly this alone makes a strong case for investment in research into quantum devices and quantum control. The results should enable us to push Moore's Law to the limit, evolving conventional information technology (IT) as far as it can go. However, such quantum research has already shown that the potential exists to do much more – revolution! Instead of playing support act to make better conventional devices, let quantum mechanics take centre stage in new technology that stores, processes and communicates information according to the laws of quantum mechanics. Great idea, but what is feasible and how far have we got?

2 The building blocks – quantum bits

Most information manipulation these days is done digitally, so data is processed, stored and communicated as bits. The two states of a conventional data bit (but written in suggestive quantum notation as) |0> and |1> take many forms – two different voltages across a transistor on a chip, two different orientations of a magnetic domain on a disc or tape, two different voltages propagating down

* ts@hplb.hpl.hp.com

a wire, two different light pulses travelling down an optical fibre, and so on – dependent upon what is being done with the data. At any time a bit is *always* in state |0> *or* state |1>, hence the name, although bits get flipped as data is processed or memory is rewritten. However, the quantum analogue of a conventional bit, a qubit, has rather more freedom. It can sit anywhere in a two-dimensional Hilbert space – picture it as the surface of a sphere – with a general state of the form

$$|\psi\rangle = \cos\alpha\,|0\rangle + \exp i\beta\,\sin\alpha\,|1\rangle \qquad (1)$$

parametrized by two angles. A conventional bit only has the choice of the poles, but a qubit can live anywhere on the surface of the sphere. States such as (1) are *superposition* states; they have amplitudes for and thus carry information about the states |0> and |1> *at the same time*. Similarly, a collection, or register, of *N* qubits can have exponentially many (2^N) amplitudes, whereas the analogous conventional data register can only hold one of these states at any given time. Clearly if it is possible to operate, or compute, simultaneously with all the amplitudes of a quantum register, there is the possibility of massively parallel computation based on quantum superpositions.[1,2]

We can read ordinary information without noticeably changing it – you can read a book without harming it and your telephone calls can be tapped without you knowing. The same is simply not so for quantum information. If a qubit in state (1) is measured to determine its bit value, it will always give the answer 0 or 1. This is a truly random and irreversible process, with respective probabilities of $\cos^2\alpha$ and $\sin^2\alpha$, and afterwards the qubit is left in the corresponding bit state |0> or |1> (if it isn't destroyed). It is thus impossible to read, or similarly copy or clone,[6,7] unknown quantum information without generally leaving evidence of the intrusion. This unavoidable disturbance through quantum measurement can be used to detect eavesdropping on quantum communications,[3] and provides the basis for guaranteed security.[8,9]

Many types of usable qubit exist, or in some cases reasonable approximations, where two orthogonal quantum states (used to represent |0> and |1>) are or can be separated from the rest of the space. Examples include: two adjacent energy eigenstates of atoms[10] or ions[11] (separated by a microwave or an optical transition); the vacuum or single photon state of a mode in a small optical or superconducting microwave cavity;[12] two orthogonal linear or circular polarizations of a travelling photon or weak light pulse;[3] the "which path" label of a photon[3] or atom in an interferometer; the energy eigenstates (up or down) of a spin-1/2 in a magnetic field;[13] two adjacent energy eigenstates of an electron or exciton in a quantum dot;[14] two charge states of a tiny superconducting island[15] or flux states of a superconducting ring;[16,17] and so on. This list is not at all exhaustive, and many more candidate qubits have been proposed and are under investigation. As with realisations of conventional data bits, the most appropriate choice is defined by the application.

3 Quantum information processing and communication (QIPC)[1-3]

The very features that make quantum mechanics so weird and wonderful, when compared to our everyday experience of the classical world, are those that also underpin its potentially revolutionary applications for information technology. A multi-qubit processor enables massively parallel *quantum computing* – interference between all the amplitudes in such a device could in theory be arranged to provide solutions to certain tasks that we will never be able to perform with even the best conventional supercomputers in the future. The irreversibility of quantum measurement enables two correspondents – Alice and Bob – to communicate with guaranteed security, using photon qubits and public communications. *Quantum cryptography* is secure against eavesdroppers, even if they have their own quantum technology. Then there is entanglement…

Two qubits (*A* and *B*) can exist in a state like

$$|\psi\rangle_{AB} = 2^{-1/2}(|0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B) \qquad (2)$$

that cannot be factored, so neither qubit has a state of its own, independent of its partner. As essentially all the (pure) quantum states of a multi-qubit register contain entanglement, it plays an important role in quantum processing. However, there is no reason for the two qubits in (2) to be in the same register or indeed physical location, and in such cases distributed entanglement provides for a remarkable form of communication – *quantum teleportation.* Coupled with conventional communication, entangled states can be used as a resource for teleporting quantum states, deconstructing them in one place and rebuilding them in another.

Essentially all aspects of QIPC can be reduced to three stages: prepare; evolve; measure. As we are big and clumsy and classical, and only relate to conventional information, we have to carefully prepare qubits in appropriate states, allow them to evolve, and then measure them to extract information in a form we can use. The middle stage could be the controlled evolution of many interacting qubits according to some prescribed quantum algorithm to effect a computation, or it could be the propagation of qubits from Alice to Bob for communication, perhaps also with processing at *A* or *B*. A detailed check-list for the implementation of QIPC has been laid out by David DiVincenzo.[18,19] In short:

(i) A collection of well-characterised qubits is needed. One at a time will do for cryptography; interactions and scalability in number are necessary for computing.
(ii) Preparation of known initial states for the qubits must be possible.
(iii) The quantum coherence of the system(s) must be maintained to a high degree during the evolution stage.
(iv) The unitary quantum evolution required by the algorithm or protocol must be realisable. As with conventional computing, the minimum of a universal set of elementary gates[20-22] must be possible.
(v) Quantum measurements on specific qubits must be possible.
(vi) The capability to interconvert stationary (processing or memory) qubits and flying (communication) qubits must exist.
(vii) It must be possible to transmit flying qubits coherently between specified locations.

Quantum computing requires (i)-(v), although distributing it between processors would add (vi) and (vii). Elementary quantum cryptography requires (i), (ii), (v) and (vii); ((iii) is effectively implicit in (vii)). Usable teleportation essentially requires the lot, although (vi) can be dropped for demonstrations and it should be noted that the processing demands (iv) are very simple compared to all-purpose computing. Qubit storage as needed in (iv) is implicit, although “long term” storage, so resources can be built up in advance for teleportation and other communication scenarios, would also be desirable.

The demands outlined above are very tough indeed. The construction of useful QIT will not be easy and the issue of quantum coherence (iii) is always lurking. With the additional freedom of Hilbert space that gives QIT its potential advantage comes the penalty that quantum states are very delicate. Qubits can entangle with things you don’t want them to entangle with, and over which you have no control. This decoherence is not too bad for individual photons propagating down standard optical fibres or even through free space, so usable quantum cryptosystems have already made it out of the laboratory. However, decoherence was thought to be a terminal problem for many interacting qubits, and so it was really the discovery of quantum error correction by Peter Shor[23,24] and Andrew Steane[25,26] that expanded quantum computing from an academic subject to one also having

technological promise. The techniques are subtle – you can't dive in and irreversibly measure everything – but share spirit with conventional error correction. The important quantum information can be encoded redundantly using extra qubits, and protected against or corrected for errors, perhaps indefinitely if the decoherence during an elementary quantum gate is small enough (with an error probability of order 10^{-4}) and there are plenty of qubits. However, these are still very challenging requirements.

4 Quantum computing

The seeds of quantum computing began with Richard Feynman[27] and others in the early 1980s and it was David Deutsch[28] who first considered in detail the implications of quantum physics for the theory of computation. In 1992 Deutsch and Richard Jozsa came up with an algorithm[29] that showed a clear quantum advantage and the subject really took off in the mid-1990s with the factoring algorithm of Peter Shor[30] and the searching algorithm of Lov Grover,[31] which give significant advantage over their classical counterparts. Much of the "secure" communications in the world today use public key cryptography, which is based on factoring a very large number into its two component primes (or related problems) being practically unbreakable. The construction of a many-thousand qubit quantum computer would thus trash the world's communications infrastructure – certainly dramatic, whether you approve or not. Quantum computers could clearly also do a much better job of simulating quantum systems[32] than conventional IT, and so would open up new research capabilities in many fields. The search is still on for more quantum algorithms – open problems exist because not everything is amenable to a naïve quantum speed-up. The quantum computational advantage arises because (in principle exponentially) many calculations can run in parallel during the evolution stage. However, quantum measurements have to be made to get answers, so simple number crunching doesn't get exponential advantage. Rather, it is problems that utilise the parallelism through interference that can gain. The factoring algorithm uses the exponential resources and a Fourier transform to find the (very large) periods of oscillatory functions, and the search algorithm offers a square root reduction in time by effectively searching "amplitudistically" rather than probabilistically.

Implementation research today has progressed to the few qubit and simple algorithm level. The first two-qubit gate was done with an ion trap[33] and work has now progressed to four-ion entanglement[34] and realisation of the Deutsch-Jozsa algorithm.[35] Atom-cavity interactions in the optical[36,37] and microwave[38] domains have got to three-qubit entanglement.[39] Use of nuclear spin qubits in a molecule in an ensemble nuclear magnetic resonance approach[40,41] has demonstrated a number of simple algorithms,[42-46] most recently the factoring of fifteen.[47] Single superconducting qubits based on charge or phase have been constructed[48-51] (see figure 1).

Many other approaches to quantum computing hardware have been proposed.[52,53] Examples include photons,[54] charge[14] or spin[13] in quantum dots, dopant nuclear (or electronic) spins in the solid state,[55,56] spins in fullerene cages,[57] trapped electrons[58] (see figure 2), quantum Hall systems,[59] magnetic molecules or nano-crystals[60] (see figure 3) and electrons on liquid helium.[61] From the perspective of scalability in qubit number, solid state approaches which build on the wealth of existing fabrication techniques have much appeal. It is certainly also the case that most qubit successes to date do not seem to be easily scalable. The flip side is that solid state systems generally suffer more decoherence, so it will be a very big challenge to reduce this to the level required for error correction and fault tolerant operation.

5 Quantum cryptography[3]

Around 1970 Stephen Wiesner[62] realised quantum mechanics could be useful for cryptography and in 1984 Charles Bennett and Gilles Brassard proposed the well known BB84 scheme[63] for quantum key distribution. Many developments and new protocols have followed.[64] The basic idea is for Alice and

Bob to share a secret key and to use this as a one-time-pad to communicate securely – quantum mechanics guarantees the security of the key. In BB84 Alice sends to Bob photons chosen randomly from the four states of two overlapping qubit bases (e.g. two orthogonal linear polarisations and right and left circular polarizations) and Bob measures in one of the two bases, chosen at random. After accumulating data, using public communication[65] and sacrificing some of the bits, they can then identify what to keep (the raw key – when Bob used the correct basis), locate and correct errors, and scramble and reduce their correct bits (privacy amplification) to distil a shared secret key. Like Bob, any eavesdropper (Eve) has to measure[66] the qubits – she has to play "guess the basis" and so cannot avoid introducing errors into the raw key. If Eve reads the lot, Alice and Bob know this and bin the raw key; if Eve reads only a fraction they can use the rest to distil some guaranteed secure bits.

The first prototype system[67] ran in 1989. Since then, many developments have taken quantum cryptography out of the laboratory and towards actual technology, using qubits embodied in weak laser pulses or photons, sent from Alice to Bob through standard telecommunications optical fibres or even free space. Fibre examples work over useful distances,[68-72] can operate alongside conventional communications through multiplexing,[73] can use multiple Bobs,[74] have used entangled photons[75-79] (see figure 4) and have shared a secret distributed between Bob and Charlie.[80] The working distance is now up to 67 km with a "plug & play" system[81] (see figure 5). Free space systems have also been developed,[82-87] with the aim of secure communications to and via satellites. The distance is currently up to 23.4 km at altitude in the Alps,[88] which makes quantum communication to near-Earth orbit satellites look feasible. Research continues to improve sources and detectors, which would enhance all forms of quantum cryptosystem – for example systems are now operating with "on-demand" single photons.[89]

On the theory and protocols side, research continues to see just what can and can't be done securely by quantum means. Clearly key distribution can, for example it is known that bit commitment can't,[90,91] and open problems in between remain.

6 Quantum teleportation

The theory for quantum teleportation was laid out[92] in 1993 by Charles Bennett, Gilles Brassard, Claude Crepeau, Richard Jozsa, Asher Peres and Bill Wootters. The basic idea is that if Alice and Bob share a pair of entangled qubits (as in (2)), they can use this as a resource to offer a teleportation service. Alice takes an unknown qubit from a customer, performs a two-qubit gate on this and qubit *A*, and then measures both. She transmits the results (two bits) to Bob by a conventional communication channel. The results uniquely identify one of four single-qubit operations to Bob, one of which is "do nothing"! Once he has performed the identified operation on qubit *B*, it is left in the state of the qubit supplied by the customer! There is no instantaneous signalling as the two bits have to be sent to Bob, so relativity is happy, and no quantum copy has been made as all record of the state is destroyed at Alice's end. Amusingly, and of course very much in principle, Alice doesn't have to know where Bob is provided that she broadcasts her bits! Also, if the customer supplies half of an entangled pair, the outcome is entanglement between two qubits who have never met!

From 1997 a number of experiments demonstrating the principles of teleportation have been performed.[93-98] The details differ, but their basis is to distribute entanglement using photon qubits (or light pulses), and to use this for the teleportation of a quantum state from *A* to *B*. Currently it is not possible to teleport the unknown state of a customer qubit (for example, another photon) with complete success because of the difficulty in realising the required two-qubit gate at *A* on demand. Research continues towards this goal. There is certainly an incentive because teleportation underpins the concept of a quantum repeater,[99] which could be used to extend the working distance of quantum cryptosystems. A recent step towards this has been the demonstration of teleportation through 2 km

of optical fibre[100] (see figure 6). It isn't "on demand", but it does show that teleportation is progressing beyond the confines of a single laboratory.

7 Prospects for QIT

Quantum cryptography works, around Ipswich (UK), under Lake Geneva and between mountains in the Alps (Europe), in the Los Alamos desert (USA), and in numerous other places worldwide. You can buy a working fibre system,[101] and secure satellite communications may well emerge over the next few years.

Few-qubit demonstration quantum computers exist. However, useful many-qubit machines are still a long way off and we don't yet know what form they might take. If QIT develops, it is unlikely to displace conventional IT and more likely to work with it, addressing specific tasks. In the future you are more likely to buy a PC with some quantum chips in it, rather than chucking your existing machine in the bin (or recycler) in favour of a new wholly quantum one!

Teleportation of a single qubit works down about 2 km of optical fibre. However, I very much doubt whether any of us will ever walk into a teleport and utter the immortal words: "Beam me up Scotty." That said, simpler teleportation could play a very important future role in distributing quantum information between processors, or effectively stringing out entanglement for long-distance quantum communications.

Present day IT companies measure their annual revenue in billions of dollars. If such mass-market scale or consumer QIT is to emerge in the future, new quantum applications, software and protocols will be needed. Hardware development is certainly necessary, but certainly also not sufficient. The development of large-scale quantum processors will likely be very expensive, so this investment will need the promise of a market. This means the quantum algorithms, theory and protocols folk cannot now put their feet up, and simply leave things to the hardware scientists and engineers. Much further research is needed in all aspects of the field if QIT is to become a reality.

8 Further information

Papers and preprints on all aspects of QIPC can be accessed electronically at:
http://xxx.lanl.gov/archive/quant-ph
http://www.vjquantuminfo.org/
Further information on the European Commission funded QIPC projects cited in this article can be found at:
http://www.cordis.lu/ist/fetqipc.htm
http://www.quiprocone.org

Acknowledgements

I thank my various QIPC colleagues for their kind provision of figures.

References

1. M. A. Neilsen and I. L. Chuang, *Quantum Computation and Information*, (Cambridge University Press, 2000), ISBN 0-521-63503-9.

2. H.-K. Lo, S. Popescu and T. P. Spiller (eds.), *Introduction to Quantum Computation and Information*, (World Scientific Publishing, 1998), ISBN 981-02-3399-X.

3. N. Gisin et al., *Rev. Mod. Phys.* **74**, 145 (2002).

4. The original paper is available at: http://www.intel.com/research/silicon/mooreslaw.htm

5. Pessimists have been predicting that the end of silicon is about five years away for more than five years now. If you want to make up your own mind, the International Technology Roadmap for Semiconductors is at: http://public.itrs.net/

6. W. K. Wootters and W. H. Zurek, *Nature* **299**, 802 (1982).

7. D. Dieks, *Phys. Lett. A* **92**, 271 (1982).

8. D. Mayers, "Unconditional security in Quantum Cryptography", quant-ph/9802025.

9. H.-K. Lo and H. F. Chau, *Science* **283**, 2050 (1999).

10. P. Domokos, et al., *Phys. Rev. A* **52**, 3554, (1995).

11. J. I. Cirac and P. Zoller, *Phys. Rev. Lett.* **74**, 4091 (1995).

12. X. Maître, et al., *Phys. Rev. Lett.* **79**, 769 (1997).

13. D. Loss and D. P. DiVincenzo, *Phys. Rev. A* **57**, 120 (1998).

14. A. K. Ekert, and R. Jozsa, *Rev. Mod. Phys.* **68**, 733 (1996).

15. A. Shnirman, et al., *Phys. Rev. Lett.* **79**, 2371 (1997).

16. M. F. Bocko, et al., *IEEE Trans. on Appl. Superconductivity* **7**, 3638 (1997).

17. J. E. Mooji, et al., *Science* **285**, 1036 (1999).

18. D. P. DiVincenzo, "Topics in Quantum Computers", in *Mesoscopic Electron Transport*, (ed. Kowenhoven, L., Schön, G. & Sohn, L.), NATO ASI Series E, (Kluwer Ac. Publ., Dordrecht, 1997); cond-mat/9612126.

19. D. P. DiVincenzo, *Fortschr. Phys.* **48**, 9 (2000).

20. D. P. DiVincenzo, *Phys. Rev. A* **51**, 1015 (1995).

21. S. Lloyd, *Phys. Rev. Lett.* **75**, 346 (1995).

22. A. Barenco, et al., *Phys. Rev. A* **52**, 3457 (1995).

23. P. W. Shor, *Phys. Rev. A* **52**, 2493 (1995).

24. P. W. Shor, "Fault-tolerant quantum computation", *Proc. 37th Annual Symposium on the Foundations of Computer Science*, 56 (IEEE Computer Society Press, Los Alamitos, CA, 1996); quant-ph/9605011.

25. A. M. Steane, *Phys. Rev. Lett.* **77**, 793 (1996).

26. A. M. Steane, *Phys. Rev. Lett.* **78**, 2252 (1997).

27. R. P. Feynman, *Int. J. Theor. Phys.* **21**, 467 (1982).

28. D. Deutsch, *Proc. R. Soc. Lond. A* **400**, 97 (1985).

29. D. Deutsch and R. Jozsa, *Proc. R. Soc. Lond. A* **439**, 553 (1992).

30. P. W. Shor, "Polynomial-Time Algorithm for Prime Factorization and Discrete Logarithms on a Quantum Computer", *Proc. 35th Annual Symposium on the Foundations of Computer*

Science, ed. S. Goldwasser, 124 (IEEE Computer Society Press, Los Alamitos, CA, 1994); *SIAM J. Computing* **26**, 1484 (1997); quant-ph/9508027.

31. L. K. Grover, "A fast quantum mechanical algorithm for database search", *Proc. 28th Annual ACM Symposium on the Theory of Computing (STOC)*, 212 (May 1996); quant-ph/9605043; *Phys. Rev. Lett.* **79**, 325 (1997); quant-ph/9706033.

32. See, for example, S. Lloyd, *Science* **273**, 1073 (1996).

33. C. Monroe, et al., *Phys. Rev. Lett.* **75**, 4714 (1995).

34. C. A. Sackett, et al., *Nature* **404**, 256 (2000).

35. S. Gulde, et al., (Quantum Optics and Spectroscopy Group, University of Innsbruck, (European Commission project QUBITS)), "Implementing the Deutsch-Josza algorithm on an ion-trap quantum computer", to be published.

36. H. J. Kimble, et al., *Phys. Rev. Lett.* **39**, 691 (1977).

37. A. B. Mundt, et al., *Phys. Rev. Lett.* **89**, 103001 (2002).

38. S. Haroche, et al., *Phil. Trans. R. Soc. Lond. A* **355**, 2367 (1997).

39. A. Rauschenbeutel, et al., *Science* **288**, 2024 (2000).

40. N. A. Gershenfeld and I. L. Chuang, *Science* **275**, 350 (1997).

41. D. Cory, et al., *Proc. Nat. Acad. Sci.* **94**, 1634 (1997).

42. I. L. Chuang, et al., Nature 393, 143 (1998).

43. J. A. Jones and M. Mosca, *J. Chem. Phys.* **109**, 1648 (1998).

44. J. A. Jones et al., Nature 393, 344 (1998).

45. I. L. Chuang, et al. *Phys. Rev. Lett.* **80**, 3408 (1998).

46. D. G. Cory, et al., *Phys. Rev. Lett.* **81**, 2152 (1998).

47. L. M. K. Vandersypen, et al., Nature 414, 883 (2001).

48. Y. Nakamura, et al., *Nature* **398**, 786 (1999).

49. D. Vion, et al., *Science* **296**, 886 (2002).

50. Y. Yu, et al., *Science* **296**, 889 (2002).

51. J. M. Martinis, et al., *Phys. Rev. Lett.* **89**, 117901 (2002).

52. *Fortschr. Phys.* **48**, Number 9-11, Special Focus Issue: "Experimental Proposals for Quantum Computers", eds. S. Braunstein and H.-K. Lo (2000).

53. R. G. Clark (ed.), *Experimental Implementation of Quantum Computation*, (Rinton Press, 2001), ISBN 1-58949-013-4.

54. E. Knill, et al., *Nature* **409**, 46 (2001).

55. B. E. Kane, *Nature* **393**, 133 (1998).

56. G. P. Berman, et al., *Superlattices and Microstructures* **27**, 89 (2000).

57. J. Twamley, (NUI Maynooth, (European Commission project QIPD-DF)), "Quantum cellular automata quantum computing with endohedral fullerenes", quant-ph/0210202.

58. G. Ciaramicoli, et al., *J. Mod. Opt.* **49**, 1307 (2002); *Phys. Rev. A* **63**, 052307 (2001); "A scalable quantum processor with trapped electrons", in preparation.

59. V. Privman, et al., *Phys. Letters A* **239**, 141 (1998).

60. J. Tejada, et al., *Nanotechnology* **12**, 181 (2001).

61. P. M. Platzman and M. I. Dykman, *Science* **284**, 1967 (1999).

62. S. Wiesner, *SIGACT News* **15**, 78 (1983) is where the ideas finally appeared in print.

63. C. H. Bennett and G. Brassard, “”Quantum cryptography: Public key distribution and coin tossing”, *Proc. IEEE International Conference on Computers, Systems and Signal Processing*, 175 (IEEE, New York, 1984).

64. For a recent review of the whole subject, see reference 3.

65. Technically, the public channel has to be unjammable, or failing that, authenticated, so in practice quantum systems realise secure key expansion.

66. As this destroys the qubits, the best she can do is to replace them in correspondence to her measured results.

67. C. H. Bennett, et al., *J. Cryptology* **5**, 3 (1992).

68. P. Townsend, et al., *Electron. Lett.* **29**, 634 (1993).

69. C. Marand and P. D. Townsend, *Opt. Lett.* **20**, 1695 (1995).

70. J. D. Franson and B. C. Jacobs, *Electron. Lett.* **31**, 232 (1995).

71. A. Muller, et al., *Europhys. Lett.* **33**, 335 (1996).

72. R. Hughes, et al., *J. Mod. Opt.* **47**, 553 (2000).

73. P. Townsend, *Electron. Lett.* **33**, 188 (1997).

74. P. Townsend, *Nature* **385**, 47 (1997).

75. A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1992).

76. T. Jennewein, et al., *Phys. Rev. Lett.* **84**, 4729 (2000).

77. D. Naik, et al., *Phys. Rev. Lett.* **84**, 4733 (2000).

78. W. Tittel, et al., *Phys. Rev. Lett.* **84**, 4737 (2000).

79. G. Ribordy, et al., *Phys. Rev. A* **63**, 012309 (2001).

80. W. Tittel, et al., *Phys. Rev. A* **63**, 042301 (2001).

81. D. Stucki, et al., *New J. Phys.* **4**, 41 (2002).

82. B. C. Jacobs and J. D. Franson, *Opt. Lett.* **21**, 1854 (1996).

83. W. T. Buttler, et al. *Phys. Rev. Lett.* **81**, 3283 (1998).

84. W. T. Buttler, et al. *Phys. Rev. Lett.* **84**, 5652 (2000).

85. P. M. Gorman, et al., J. Mod. Opt. 48, 1887 (2001).

86. J. G. Rarity, et al., *Electron. Lett.* **37**, 512 (2001).

87. R. J. Hughes, et al., *New J. Phys.* **4**, 43 (2002).

88. C. Kurtsiefer, et al., *Nature* **419**, 450 (2002).

89. A. Beveratos, et al., *Phys. Rev. Lett.* **89**, 187901 (2002).

90. D. Mayers, *Phys. Rev. Lett.* **78**, 3414 (1997).

91. H.-K. Lo and H. F. Chau, *Physica D* **120**, 177.

92. C. H. Bennett, et al., *Phys. Rev. Lett.* **70**, 1895 (1993).

93. D. Bouwmeester, et al., *Nature* **390**, 575 (1997).

94. D. Boschi, et al., *Phys. Rev. Lett.* **80**, 1121 (1998).

95. A. Furusawa, et al., *Science* **282**, 706 (1998).

96. M. A. Neilsen, et al., *Nature* **396**, 52 (1998).

97. Y.-H. Kim, et al., *Phys. Rev. Lett.* **86**, 1370 (2001).

98. E. Lombardi, et al., *Phys. Rev. Lett.* **88**, 070402 (2002).

99. H. J. Briegel, et al., *Phys. Rev. Lett.* **81**, 5932 (1998).

100. W. Tittel, et al., (Group of Applied Physics, University of Geneva, (European Commission project QUCOMM)), "Quantum teleportation of time-bin qubits over 2 km", to be published.

101. http://www.idquantique.com/

Figure captions

1. Scanning electron micrograph of the quantronium superconducting qubit.[49] The centerpiece is a small island linked to two Josephson junctions. By applying microwave pulses to the nearby lower gate electrode, the quantronium can be prepared in any coherent superposition of its two lowest energy eigenstates (the two qubit states). Reproduced by kind permission of the Quantronics Group, CEA-Saclay, France (European Commission project SQUBIT).
2. Schematic diagram of electrons (green) in a Penning trap.[58] The ring electrodes have alternating static voltages (red=positive, yellow=negative). Qubits can be encoded into the motional and spin degrees of freedom of each electron and they can be addressed with external microwave pulses. Reproduced by kind permission of Paolo Tombesi, University of Camerino, Italy (European Commission project QUELE).
3. Schematic diagram of coupled magnetic qubits.[60] The qubits are encoded into two magnetic states of magnetic molecules or nanocrystals (yellow) coupled to micro-SQUIDs (red) for measurement and to superconducting loops (blue) for mediation of qubit-qubit coupling. Reproduced by kind permission of Javier Tejada, University of Barcelona, Spain (European Commission projects MAGQIP, NANOMAGIQC) and IOP Publishing Ltd. (*Nanatechnology*).
4. An entangled photon source used to demonstrate quantum cryptography over 8 km.[79] Reproduced by kind permission of the Group of Applied Physics, University of Geneva, Switzerland (European Commission project QUCOMM).
5. A prototype "plug & play" quantum cryptosystem used to demonstrate quantum cryptography over 67 km.[81] Reproduced by kind permission of the Group of Applied Physics, University of Geneva, Switzerland (European Commission project QUCOMM) and IOP Publishing Ltd. (*New J. Phys.*).
6. A schematic diagram of the 2 km fibre quantum teleportation apparatus.[100] Femtosecond laser pulses are split in two parts using a variable beam-splitter (HWP+PBS). The reflected beam is sent to Alice who creates the qubits (encoded through "which time bin") to be teleported (at wavelength 1310 nm), which she then forwards to Charlie. The transmitted beam is used to produce entangled photon qubits. The 1310 nm photon is sent to Charlie, the 1550 nm photon to Bob who is situated in another lab, 55 m away from Charlie and connected by 2 km of optical fibre. Charlie effectively performs a gate and measures the two photons he has, using the 50/50 fibre coupler BS. When the outcome signals the action "do nothing" for Bob (1/4 of the time), he simply analyses his photon to prove that indeed the state encoded by Alice has been teleported. Reproduced by kind permission of the Group of Applied Physics, University of Geneva, Switzerland (European Commission project QUCOMM) and XX INSERT PUBLISHER XX.

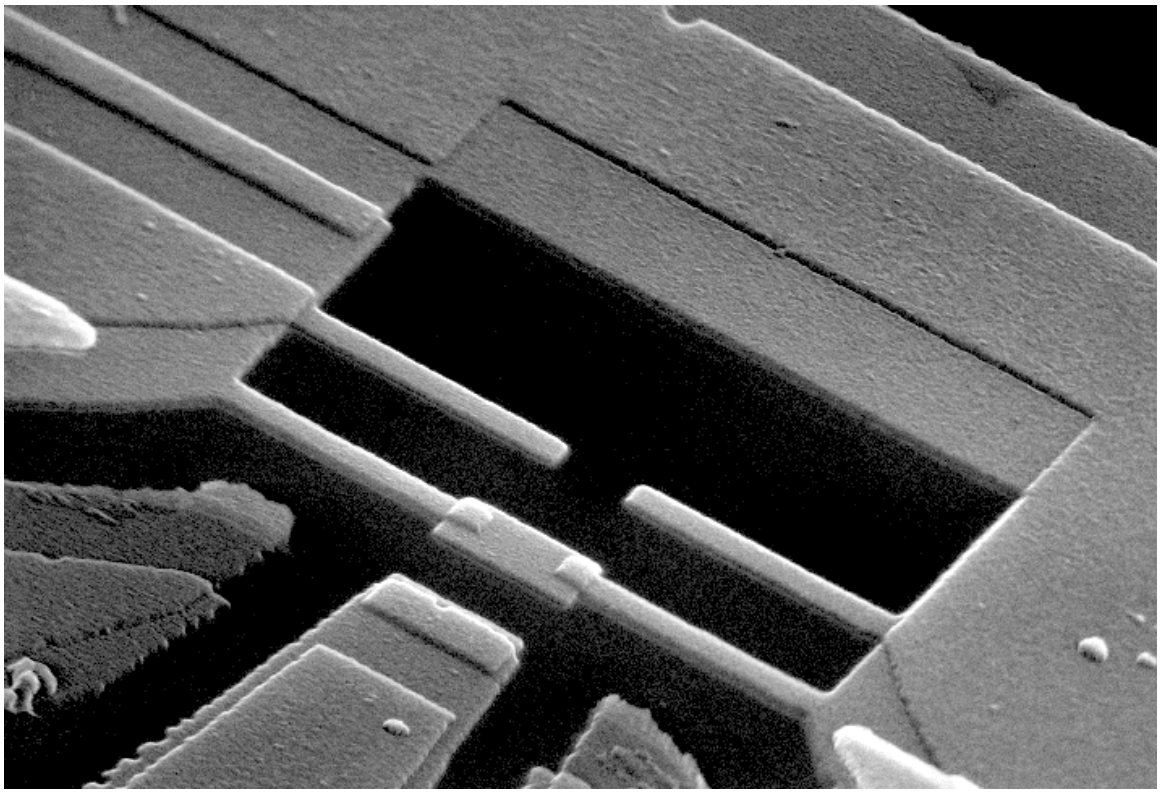

Figure 1

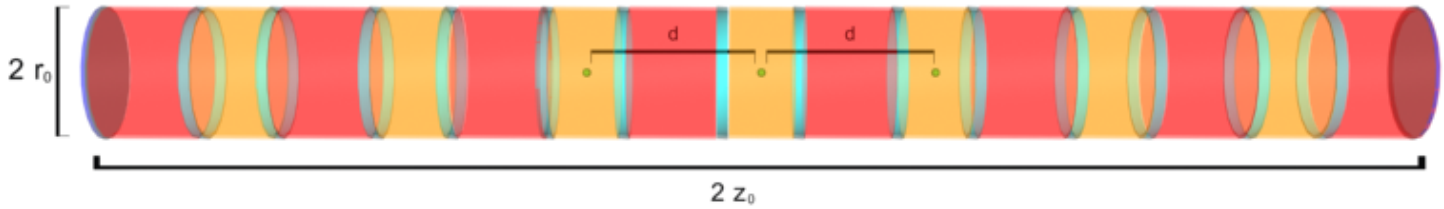

Figure 2

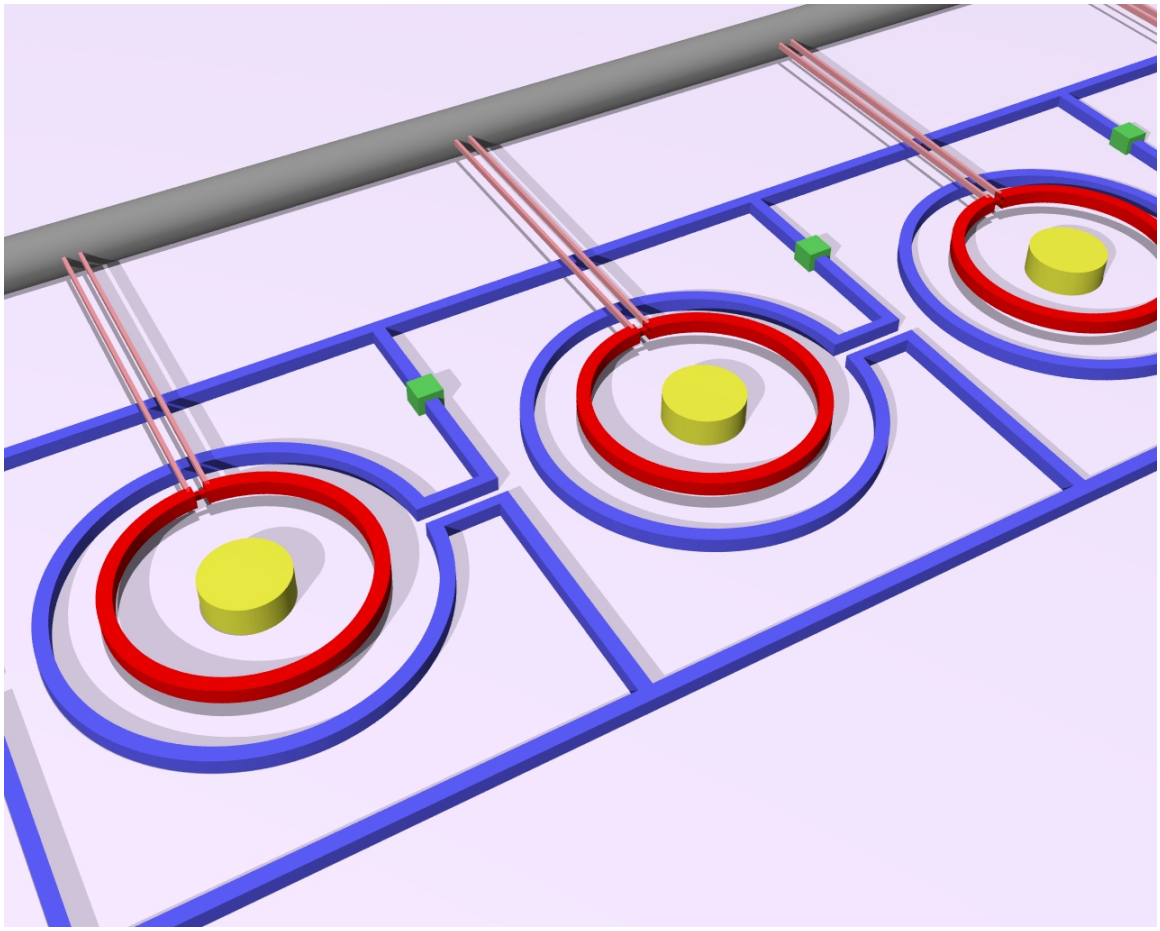

Figure 3

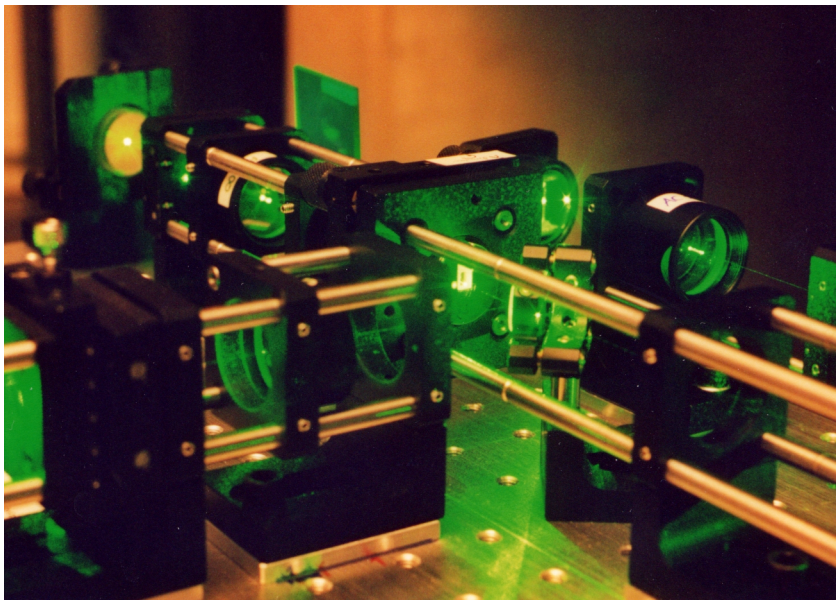

Figure 4

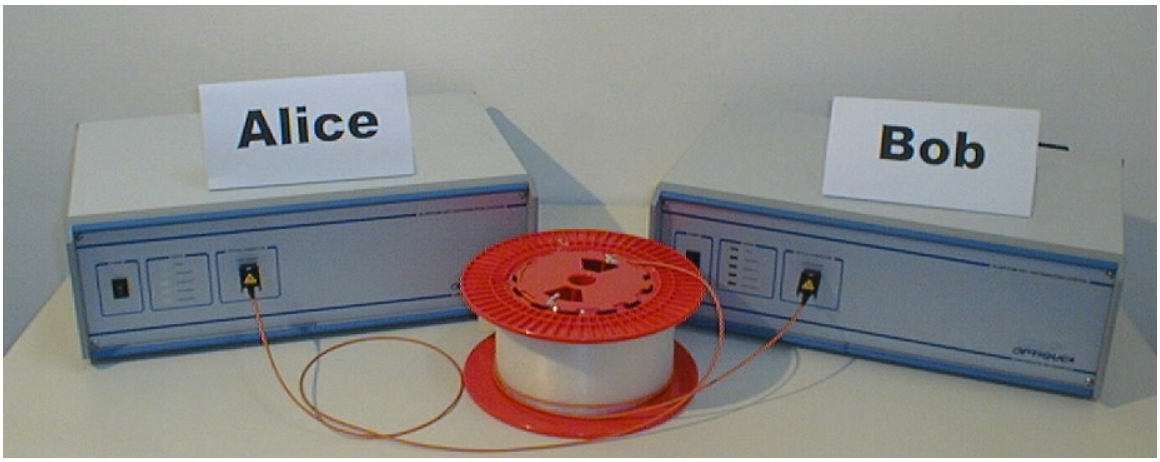

Figure 5

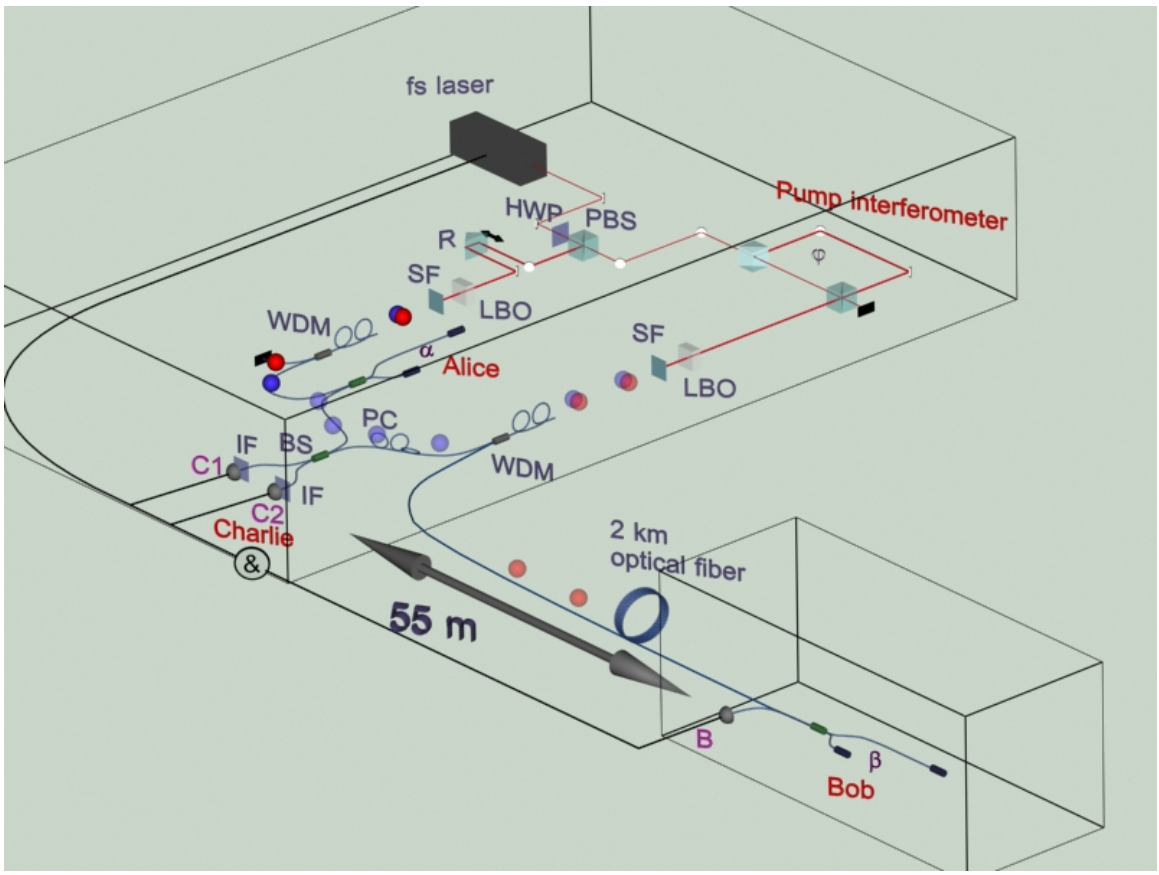
fs laser
HWP
PBS
Pump interferometer
R
SF
LBO
φ
WDM
α
Alice
SF
LBO
PC
IF
BS
C1
IF
WDM
C2
Charlie
&
2 km
optical fiber
55 m
B
β
Bob

Figure 6