INFORMATION SOCIETIES TECHNOLOGY (IST) PROGRAMME

QIT Strategy Document

Project acronym: QUIPROCONE
Project full title: Quantum Information Processing & Communications Network of Excellence
Contract no.: *IST-1999-29064 (Thematic Network)*

Operative commencement date of contract: *1 August 2000*

Table of Contents

1 Introduction

Although the fields are new and very much still growing and developing, research results in the fields of quantum information processing and communication[1-3] (QIPC) have already shown that a whole new quantum information technology (QIT) could emerge in the future. In conventional IT, quantum mechanics effectively plays a “support role”, in helping to improve the materials and device building blocks. However, fundamental quantum phenomena play “centre stage” for QIPC. Although the detailed behaviour of conventional IT devices is ultimately determined by quantum mechanics, these devices actually manipulate data according to the familiar laws of classical physics. With QIPC, this is radically different – here information is actually stored, processed and communicated according to the laws of quantum physics. Research has already shown that this additional freedom could enable future QIT to perform tasks we will never achieve with ordinary IT. As yet, there is no significant QIT industry to speak of. If there is to be a substantial QIT industry in the future – utilising the promise of QIPC research – many questions and issues will have to be addressed. In effect, a strategy for the development of a QIT industry has to be developed. This article certainly doesn’t do this. However, it raises some of the questions and issues, and provides some comments. It makes a start.

In order to have a Roadmap for the QIT industry, analogous to the International Technology Roadmap for Semiconductors[4] for the conventional IT industry, the strategy for the development of the QIT industry has to be identified. Then the goals to be addressed by the Roadmap can be set, routes can be drawn up, milestones identified, etc.. It should be noted that there exists already a very comprehensive Quantum Computing Roadmap,[5] coordinated by ARDA in USA. In effect, for this Roadmap the goal is already clearly identified – that of realising scalable quantum computing to enable the construction of a factoring machine. It is certainly not clear that this goal should be one of the (initial) goals for a QIT Industry Roadmap – more on this later in Sections 6-8. For a QIT Industry Roadmap, the debate over the strategy and thus the goals still needs to be had. Only then can this industry Roadmap begin to materialise.

2 Background

Moore’s Law tells us that the fastest processor computer in the shops doubles in speed about every 18 months, and typical memory capability in electronic equipment shows a similar exponential growth. 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, which decreases communication times between components. This exponential progress, first noted[6] by Gordon Moore (a co-founder and former CEO of Intel) in 1965, has continued ever since, and is illustrated in figure 1. However, this progress cannot go on forever.

Firstly, practical hurdles exist: for example, silicon will eventually hit problems, with oxide thinness, track width, or whatever.[4] However, even this shouldn’t be taken lightly. For example, for a number of years now (certainly more than five!), pessimists have been predicting that the development of silicon-based technology will hit problems in about five years time. Despite these predictions, silicon technology has to date effectively trampled upon its challengers. Basically, so much has been invested already in this technology route that it really will get pushed as far as it can go. Nevertheless, it seems reasonable to assume that at some point new materials or even new paradigms (such as self-assembled nano-devices or molecular electronics) will take over from silicon to maintain Moore's Law, ultimately tending towards components at atomic scales. Secondly, financial hurdles exist. Lots of dollars/euros/yen… will be needed to maintain exponential progress with conventional IT, as Moore's Second Law tells us that fabrication costs are also growing exponentially. However, even if all these practical and financial hurdles can be overcome, we will eventually run into physical barriers due to Nature.

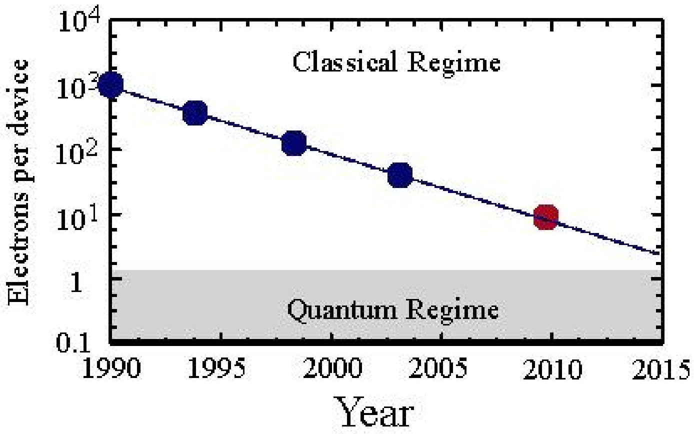

Figure 1. Moore's Law, illustrated through the number of electrons per operating device. This is decreasing exponentially as devices shrink in size. Quantum effects become increasingly important as the "Quantum Regime" is approached.

Quite simply, the fundamental building blocks of matter do not behave the same way as (almost all) macroscopic or even microscopic pieces of matter – they exhibit explicit effects of quantum mechanics. Following Moore's Law, a naïve extrapolation of the exponentially decaying number of electrons per elementary device on a chip gets to one electron per device around 2020, as shown in figure 1. The date should not be taken too seriously, but the point is clear. Eventually we will get to scales where quantum phenomena rule, whether we like it or not. Conventional data bits in nanoscale memory or processors will suffer errors from quantum fluctuations, and so unless we can control these effects, nanoscale conventional IT devices will fail to work as we expect them to. Controlling or suppressing quantum effects gets increasingly more difficult as the devices get smaller. Clearly this issue alone makes a strong case for investment in research into quantum devices and quantum control, and this is an important driver for the conventional IT industry. The results should enable us to push Moore's Law to the limit, evolving conventional IT as far as it can go.

However, over the last decade or so, quantum research has led to the new fields of QIPC, and has already shown that the potential exists to do much more than provide some valuable support to the existing IT industry. There is certainly the possibility of revolutionary new quantum information technology, based on storing, processing and communicating information according to the laws of quantum physics. Numerous ideas already exist for QIT, but at present there is essentially no QIT industry. So the big question is how to start one. Clearly this is a very involved question, and doesn't have a short answer – the complete answer would be a comprehensive and coherent strategy. Many things need to be considered and debated. This article raises some issues and makes some comments, to stimulate that debate.

3 The advantage and the disadvantage of history

The would-be inventors of new QIT have a big advantage over the inventors of conventional IT. Over fifty years of history on the invention, development and evolution of conventional IT exists, from its humble beginnings in a few simple applications right through to its ubiquitous role in present day life. A great deal can be learnt from this history. We can see how things started, from the transistor, through the first integrated circuits, to the systems-on-a-chip of today. Ideas can be borrowed and mistakes can hopefully be avoided second time around.

The would-be inventors of new QIT also have a big disadvantage over the inventors of conventional IT. Over fifty years of history on the invention, development and evolution of conventional IT exists! Given the ubiquitous role of IT today, it is very hard to actually ignore this history. Once ideas, models and pictures are inside your head, it becomes very hard to simply put them aside and think in a wholly new direction, “out of the box”… It is therefore very tempting to just look at the complete range of things we do today with conventional IT, and to try and do these things better with QIT. Or to look at things we’d like to do with current IT but can’t, and to try and do these with QIT.

Although these conflicting points can be raised on the use of the history of conventional IT, it is probably worth making some effort to draw what we can from this history, but keeping in mind that as we do so we may well be somewhat blinkered in our view of the way forward with QIT.

4 QIPC research linking to IT companies

It has already been mentioned that quantum research effectively provides a support role in helping to evolve conventional IT, since quantum mechanics is needed to properly understand, for example, the materials and the electronic behaviour of IT device components. This will become increasingly important as Moore’s Law progresses and devices get closer to the quantum limit. So although the technological aims (there are of course others, such as the advancement of fundamental understanding in physics and computer science) of QIPC research are the development of QIT, significant industrial impact could result from the applications of QIPC research to conventional IT. For example, a thorough understanding of decoherence and control mechanisms in a nanoscale quantum device could enable that device to be engineered for better performance as a classical IT component. Unwanted quantum fluctuations could be eliminated by the deliberate introduction of decoherence.

Whilst not being a primary thrust for QIPC research, this sort of application could significantly strengthen the links between QIPC and conventional IT companies, which could in turn help progress towards a new QIT industry. It is also worth noting that QIT is not going to displace or kill off conventional IT. We are big and clumsy and classical, and so it is hard to imagine any way that we might interface directly with QIT. Much more likely we will always have a conventional IT bridge to QIT. Therefore QIT should emerge alongside conventional IT, and it is thus a reasonable assumption that some of the existing conventional IT companies will move to include QIT when there is a business case. Indeed, for anything other than very simple (few-qubit based) QIT it seems likely that the actual technology will be hybrid IT-QIT, the IT being required for control and operation of the QIT, as well as interfacing and input/output. So QIT will need the expertise and underpinning of conventional IT.

5 The start of a QIT industry

There are a number of issues to consider with regard to the start of a QIT industry. Perhaps the most obvious and also the most important is that there won't be a QIT industry unless there is a market for QIT. More precisely, since QIT is something new and not an incremental step from existing IT (with its existing markets), there has to be a prediction of a market to get industry engaged in the development stage. So applications and products are needed for which there are identifiable markets. Attempting to take advantage of the history of IT, there are a number of factors to consider.

There is no good reason for assuming the "killer applications" – those with big markets, that will eventually dominate QIT revenue – will emerge early on in the life of QIT. This certainly didn't happen in the IT industry, which started small and with, relatively speaking, very crude technology, before expanding and evolving to where it is today. The first suggested application for the transistor was hearing aids. Then came various specialist military and defence applications. All the consumer stuff we are familiar with today came much later on. After being invented, the laser was basically a research tool for many years. The inventors of the laser didn't immediately predict DVD players and laser surgery. So there is no harm in trying to think big about QIT at this very early stage, but we should be prepared for the fact that we may be totally off the mark.

On this basis, it could be argued that something – a quantum hearing aid(!) – is needed to kick-start the QIT industry. The market can be small, by present day IT standards, but it has to be sufficient for things to start. This could then enable the QIT industry to bootstrap itself into existence, starting to grow and evolve as the IT industry did in its infancy. There are different routes through the bootstrapping phase (which could be explored in parallel), and all of them face barriers and problems. At the one end of the spectrum, the QIT industry could start through start-up companies. The advantages of this route are that start-ups are small and flexible, and they don't have to aim for big markets initially. The disadvantages are that any QIT may well require more R&D investment than any start-up can muster, and even after this they may not possess the manufacturing investment needed to get the price down (or the ability to run at little or no return to get the market up and running) – in effect they may end up producing expensive QIT hand-built by researchers. At the other end of the spectrum, the QIT industry could start through existing IT players developing products. The advantages of this route are that many big IT companies have extensive R&D facilities to provide for their conventional IT products, the experience of starting up new areas from scratch, the ability to invest in new manufacturing, and potentially the "support" conventional IT that will be needed alongside QIT to produce "self-contained" products. Probably the biggest disadvantage of this route is that big IT companies have much bigger revenues and profits than start-ups, so they will have to be convinced of the long term potential of QIT to provide a significant impact on these figures, in order to justify investment in this new area. At least until Moore's law begins to run out of steam…

For the latter route, a QIT industry growing inside the existing IT companies, it will basically need these companies to move on up two levels from where they are now. A good number of big IT companies today have significant QIPC research activities going on in their corporate research laboratories or R&D sections, (HP, IBM, Hitachi, Toshiba, NEC, a number of telecom companies, defence technology companies…). From here, there needs to be a step up to QIT R&D and prototyping, and then another step up to gearing up for manufacturing (each maybe requiring a factor of 10 in investment over what has gone before). So this isn't going to happen without the promise of payback from profits. It is therefore possible that the "spin-out" (from large IT companies) approach would provide a compromise route forward…

Another reason for wanting to try and get even a small QIT industry up and running is that it is necessary to get quantum widgets and simple QIT into the hands of other (not those involved directly in QIPC research) people. This is because there is no good reason to assume that the "killer applications" for QIT will be thought up by QIPC researchers. The inventors of the major applications of conventional IT today are generally not the people who researched and developed the basic building blocks. So the QIPC research community should at least be prepared for the prospect that the inventors of major QIT applications may not have PhDs in quantum physics, and may think about QIT from a somewhat different perspective.

6 The drivers for QIT

Building a factoring machine, based on Shor's factoring algorithm,[7] in order to break much of the world's current "secure" communications, is an excellent driver and current incentive (in terms of research $$$s!) for research progress in scalable quantum computing. Witness, for example, the very substantial investment being made in US, through ARDA, DARPA and the like, towards this goal. However, it is not at all clear that factoring is a commercial driver for QIT. It hardly seems likely that factoring machines have a large market – just one, or at least a select few, customer(s)! Furthermore, if the threat of a factoring machine looms large, even commercial secure communications would migrate towards other schemes (such as those based on NP-complete problems), once the security risk outweighs the potential added inconvenience over RSA etc..

Of course all this would change if someone invented a "killer application" for QIT which requires scalable quantum computing, many qubits rather than a few, to be of use. Then the defence/security agencies' desire for a factoring machine would share the same long term goal – scalable quantum computing – as commercial interests, and in this case a single Roadmap would at least in part serve everyone.

However, at present, from the commercial perspective it seems that quantum communications,[3] quantum searching[8] (and all its related algorithms) or other applications of QIPC[9-22] have the potential for rather wider use and application, compared to factoring. We must also keep in mind that we are still at the beginning of QIPC and QIT, so we are trying to guess and speculate about an iceberg (and hopefully not an ice cube) based on what is sticking out of the water.

7 Strategy: Bootstrapping a QIT industry?

So if the QIT industry has to start small and bootstrap itself into existence, what candidate starting points are there?

Quantum communication (key exchange, cryptography and other applications) is one area with potential. There is certainly a market for secure communication technology. What is not so clear is just how much folk are prepared to pay for such QIT technology, and so whether this area has the ability to induce the R&D investment from where things stand today, to kick-start a QIT industry. There are certainly a couple of start-up companies[23,24] giving it a go; it is now possible to buy quantum cryptography products. It is also worth noting that in terms of their research funding model the European Commission have pushed some quantum cryptography work away from Future and Emerging Technology, and into wider competition for research funding with other communications technology. So there are various pointers that quantum communication could seed the QIT industry.

It can be argued that quantum games[10-13] come under a very general heading of quantum communication. However, whereas simple quantum key exchange involves just two parties and can be done without any entanglement, it could be possible that quantum communications will have to go to more than two parties and/or to scenarios which necessarily require entanglement in order to start a QIT industry. It might be that only by addressing applications which have more complex goals (and thus protocols) than key exchange can QIT offer solutions that conventional IT cannot, or sufficient advantage to generate a market.

Another possible area is quantum(-improved) sensing and detecting – quantum metrology.[14-22] A great many applications currently exist for state-of-the-art measurement, sensing or detection technology. If QIT can offer a significant step forward compared to this technology, and not cost the earth, then this could be the area where a QIT industry takes off.

Quantum simulation[9] is yet another possibility. Certainly quantum simulators containing merely 50-100 qubits should be able to simulate quantum systems we will never be able to model (without theoretical corner-cutting) with conventional computers. If such simulators can be built, they could be a real stimulus for the QIT industry. Firstly, if they can be produced at a competitive (e.g. supercomputer scale) cost, then there ought to be a very lucrative specialist market for them as research tools. All universities and research institutes and laboratories would be in the market for one. Secondly, if this were to happen then it could also provide a real opportunity for new ideas and further development of QIT. Engineers, modellers, computer geeks and the like would all get to play with some serious QIT. The probability of some “killer applications” for QIT appearing would increase significantly at this point.

Of course, all of the possibilities above have been raised from the blinkered view of what we have on offer from QIPC research today. It could also be the case that new few-qubit or small scale QIPC applications, on the basis that this technology will be available well before scalable quantum computing, will provide the vehicle for starting off a QIT industry. Given this, it is clearly vital that research into new QIPC applications continues.

8 Towards a QIT industry Roadmap

If the QIT industry is to start through the bootstrapping strategy, then at this point in time an embryonic industry Roadmap could begin development. It is not possible at this point to have the focus and technological detail of the International Technology Roadmap for Semiconductors.[4] With quantum communication alone it should be possible to go part way there, because at least the physical realisation for communication – photons, or at least some quantum states of light – is agreed, and prototype technology exists. Therefore roadblocks can be identified (such as the limitations of current sources and detectors, and the absence of quantum repeaters) and technological goals and milestones can be set to get past them. However, with other QIT possibilities, such as those raised in Section 7, things are much less clear.

There is not any clear consensus yet on the best routes forward for quantum processing hardware. It is certainly likely that there will be more than one route – with conventional IT information is embodied differently in processors, memory, interconnects and interfaces with communication links, etc., and it seems very likely that quantum information will have a corresponding range of embodiments. So at present any form of quantum processing Roadmap has to be very open in terms of hardware possibilities. This is certainly the case, for example, in the Quantum Computing Roadmap,[5] which considers many possibilities for scalable quantum computing.

At the present time, in terms of quantum processing hardware, the US Quantum Computing Roadmap[5] covers all the ground extremely well, and the short term (few year) goals and milestones identified are pretty generic, independent of the ultimate longer term goals. However, it is very important to note that as time goes on and research progresses, the longer term goals will have increasing effect on the milestones. Then the hardware sections of a scalable quantum computing Roadmap and a commercially focussed QIT Roadmap would begin to differ significantly. For example, if certain few-qubit (or few tens of qubit) applications are identified as the QIT industry goal, the best routes to realising these (with acceptable error margins) may not be the best candidates for big scalable quantum computers. Probably the most important distinction between a scalable quantum computing Roadmap (aimed at the construction of a factoring machine) and a commercially focussed QIT Roadmap is the area of applications. From the QIT industry perspective, one of the main issues at present is the quest for new applications, presumably few-qubit (or few tens of qubit) as this hardware will become available first, to expand the range of possible starting points for a new industry. Of course, identifying the issue – the need for more applications – and incorporating this into a detailed Roadmap are two different things. It seems to be rather harder to define milestones for new application ideas than it is for hardware, once the embodiment is identified.

Given the commercial need for new applications, and the potential for divergence in hardware milestones, the time is probably now approaching when it makes sense to start a QIT industry Roadmap, distinct from that focussed on scalable quantum computing.

9 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. International Technology Roadmap for Semiconductors: http://public.itrs.net/

5. ARDA Quantum Computing Roadmap: http://qist.lanl.gov

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

7. 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.

8. 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.

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

10. J. Eisert, M. Wilkens and M. Lewenstein, Phys. Rev. Lett. 83, 3077 (1999).

11. J. Eisert and M. Wilkens, J. Mod. Opt. 47, 2543 (2000).

12. R. Kay, N. F. Johnson and S. Benjamin, J. Phys. A 34, l547 (2001).

13. K.-Y. Chen, T. Hogg and R. G. Beausoleil, Quantum Information Processing 1, 449 (2002), quant-ph/0301013.

14. J. J. Bollinger, et al., Phys. Rev. A 54, R4649 (1996).

15. S. F. Huelga, et al., Phys. Rev. Lett. 79, 3865 (1997).

16. H. Lee, P. Kok and J. P. Dowling, J. Mod. Opt. 49, 2325 (2002).

17. H. Lee, P. Kok and J. P. Dowling, “Quantum Imaging and Metrology”, Proceedings of the Sixth International Conference on Quantum Communication, Measurement and Computing, edited by J. H. Shapiro and O. Hirota (Rinton Press, 2002), quant-ph/0306113.

18. J. P. Dowling, Phys. Rev. A 57, 4736 (1998).

19. A. N. Boto, et al., Phys. Rev. Lett. 85, 2733 (2000).

20. P. Kok, et al., Phys. Rev. A 63, 063407 (2001).

21. W. J. Munro, et al., Phys. Rev. A 66, 023819 (2002).

22. K. Nemoto, et al., “Quantum Metrology: Detection of weak forces using Schrodinger Cat resources”, Proceedings of the Sixth International Conference on Quantum Communication, Measurement and Computing, 333, ed by J H Shapiro and O Hirota, Rinton Press (2003), quant-ph/0312063.

23. http://www.idquantique.com/

24. http://www.magiqtech.com/