Towards a Quantum Information Technology Industry

Timothy P. Spiller, William J. Munro
Trusted Systems Laboratory
HP Laboratories Bristol
HPL-2005-207
November 28, 2005*

quantum technology, quantum computation, a quantum industry

The research fields of quantum information processing and communication are now well established, although still growing and developing. It was realised early on that there is significant potential for new technologies and applications, leading to the vision of a whole new quantum information technology industry. The vision is not yet reality, and there are many open questions with regard to how it might become so. This article raises some of these questions, and gives a viewpoint on how we might proceed, from where we are today towards a quantum information technology industry in the future.

* Internal Accession Date Only
Approved for External Publication

Towards a Quantum Information Technology Industry

T P Spiller and W J Munro

Hewlett-Packard Laboratories, Filton Road, Stoke Gifford Bristol, BS34 8QZ, UK

E-mail: tim.spiller@hp.com

E-mail: bill.munro@hp.com

Abstract. The research fields of quantum information processing and communication are now well established, although still growing and developing. It was realised early on that there is significant potential for new technologies and applications, leading to the vision of a whole new quantum information technology industry. The vision is not yet reality, and there are many open questions with regard to how it might become so. This article raises some of these questions, and gives a viewpoint on how we might proceed, from where we are today towards a quantum information technology industry in the future.

PACS numbers: 03.67.-a, 03.67.Dd, 03.67.Hk, 03.67.Lx

1. Motivation

The basic ideas behind quantum information processing began to appear about twenty years ago, and those behind quantum communication even earlier. About a decade ago various important theoretical results, in combination with experimental developments at the qubit level, launched the research "big time". Now although the fields are still relatively new and certainly still growing and developing, research results in quantum information processing and communication [1, 2, 3, 4] (QIPC) have already shown that a whole new quantum information technology (QIT) could emerge in the future.

With conventional information technology (IT), quantum mechanics effectively plays a "support role", in helping to improve the materials and device building blocks. In contrast, 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, things are radically different—here information is actually stored, processed and communicated according to the laws of quantum physics. Research has already shown that this additional quantum freedom could enable future QIT to perform tasks we will never practically achieve with ordinary IT. To date, though, there exists no significant QIT industry. If there is to be a substantial QIT industry in the future—utilising the promise of QIPC research—a great many questions and issues will have to be addressed. To begin with, a strategy for the development of a QIT industry from where we are today, would be helpful. Now this article certainly doesn't purport to present one. However, it raises some of the questions and issues, and provides some comments and suggestions. It gets the ball rolling, and gives people some food for thought.

The conventional IT industry has a vast and detailed Roadmap for its continuing development, the International Technology Roadmap for Semiconductors [5]. This identifies numerous key materials, engineering and technological problems and barriers, and routes for their solution or circumvention. It is too early to start drawing up a comparable roadmap for QIT industry. A strategy for the development of actual technologies for such an 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.. Now it should be noted that there exists already a very comprehensive Quantum Computing Roadmap [6], coordinated by ARDA in USA. In effect, for this Roadmap the goal is already clearly identified—that of realising many-qubit scalable quantum computing, to enable the construction of a factoring machine. However, as will be discussed later, it is certainly not clear that this goal should be one of the initial goals for a QIT *Industry* Roadmap. In parallel with the US effort, there is also a European Strategic Report on QIPC [7]. This summarises the current state of QIPC research, and discusses future prospects and research goals. For a QIT *Industry* Roadmap, the debate over the strategy for building an industry, and thus the goals and milestones, still needs to be had. Actual quantum technologies have to appear, so more specific materials, engineering and IT

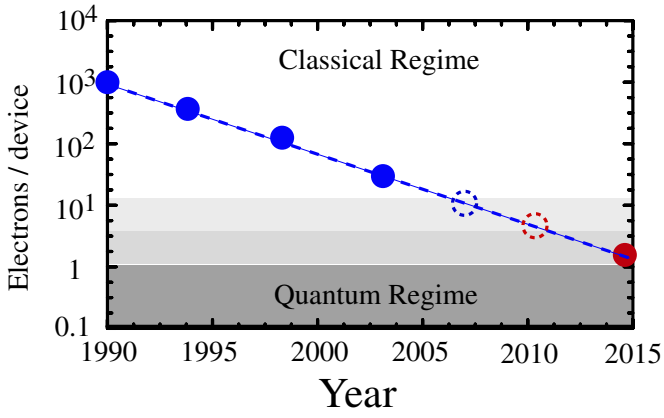

Figure 1. Moore's Law, illustrated through the number of electrons per operating device. This is decreasing exponentially as devices shrink in size. Quantum effects become increasingly important as the *Quantum Regime* is approached.

support (since it seems very likely that complex quantum technologies will require very complex conventional IT to function) demands can be identified. Only then can a detailed QIT Industry Roadmap begin to emerge.

2. Background

We know from Moore's Law 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 [8] 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.

Practical hurdles exist: for example, silicon will eventually hit problems, with insulating oxide layers becoming too thin, conducting tracks becoming too narrow, or whatever [5]. Mind you, 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 pretty effectively trampled upon its challengers. As so much has already been invested in this technology route, it makes sense to push it 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 for conventional IT, ultimately tending towards components at atomic scales. A further issue is that financial hurdles exist. Lots of dollars/euros/yen/etc. 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.

In a nutshell, 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, such as superposition, entanglement and irreversible disturbance upon measurement. Now, 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, especially if new paradigms for conventional IT components emerge, 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.

Then there is QIT... Over the last couple of decades quantum research has led to the new fields of QIPC, and it has already been shown that the potential exists to do much more than provide some valuable support to the existing IT industry. There is the possibility of revolutionary new quantum information technology, based on storing, processing and communicating information according to the laws of quantum physics, utilizing effects such as superposition, entanglement and quantum measurement. 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 and suggestions, in order to further stimulate the 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. It should certainly be kept in mind that just after the transistor and other IT components and devices emerged, folk didn't sit down, take stock of previous times of industrial revolution and then simply draw up a strategy that led to the IT industry we have today. It wasn't that easy.

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, equally important, 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 effects of quantum superposition could be eliminated by the deliberate introduction of decoherence, engineered, for example, to remove off-diagonal terms in the relevant representation. 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 beginnings 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 really 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 candidate 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. It should also be remembered that what we glibly refer to as the IT industry today had many separate beginnings, effectively as smaller and (at that time) distinct industries. These have coalesced over time, driven by the customer demands to provide simpler and cheaper integrated technologies, and complete solutions.

There are different routes through the industry 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 begin 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, (e.g. HP, IBM, Hitachi, Toshiba, NEC, a number of telecom companies, defence technology companies, etc.). 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 important 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 people (i.e. not those involved directly in QIPC research). 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 in the future may not have PhDs in quantum physics, and may think about QIT from a somewhat different perspective.

6. Drivers for QIT

Building a factoring machine, based on Shor's factoring algorithm [9] in order to break much of the world's current "secure" communications, is an excellent driver and current incentive (in terms of research dollars) 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 will constitute a major, as opposed to a specialist, 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.. Nevertheless, Shor's algorithm will always be a theoretical landmark for QIP, as it demonstrates the potential for large scale quantum computing. It continues to be an excellent research driver.

Of course all this would change if someone invents a "killer application" for QIT which requires scalable quantum computing—many qubits rather than a few—to be of use. Then the defence and security agencies' desire for a factoring machine would share the same long term goal—scalable quantum computing—as mainstream commercial interests, and in this case a single strategy and Roadmap would at least in part serve everyone. However, at present, from the commercial perspective it seems that quantum communications [3], quantum searching [10] (and all its related algorithms) or other applications of QIPC [11]-[23] have the potential for rather wider use and application, compared to factoring. We must also keep in mind that we are still at the beginnings 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 [24, 25] 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 a QIT industry.

It can be argued that quantum games [12, 13, 14, 15], auctions and the like 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 [16]-[23]. 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 an area where a QIT industry takes off. Examples are the improvement of phase measurement through non-classical interference [17, 18], more accurate frequency standards [19, 20], higher resolution lithography [21], enhanced gyroscopes [22] and improved sensing of weak forces and fields [23]. None of these seem likely to be "killer" consumer applications,

but their specialist markets could provide the start for QIT.

Quantum simulation [11] provides 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 large scale 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. Technology strategy: Optics, ion traps, solid state?

Having raised some of the candidate applications areas which could form the basis for starting a QIT industry, what about the candidate technologies? Consider first the following comments.

- States of light (single photons, weak coherent states, or some sort of quantum continuous variable states) are the best for propagating quantum information over significant distances.
- Interconversion between travelling optical qubits and static (presumably matter-based) qubits is still an open research problem, being addressed in many places and, for example, proving the scientific focus for the UK QIP IRC [26].
- Processing qubits (those capable of coherent interaction) are currently scarce—nobody has more than a handful talking to each other.
- Given the scarcity of qubits, initial few-qubit processing applications could well have to operate probabilistically and without error correction, even though methods for combatting decoherence and errors will almost certainly be needed for larger scale applications.
- There is currently no consensus on the best route to scalable quantum computing.
- Until a localised quantum processor gets to about 50 qubits or more, it doesn't really escape the regime of what might be simulatable (admittedly with vast effort) with conventional computing.

Given these, it's clear that the QIT application area at least in part determines the technology.

If quantum communication [3] is to be the initial application focus area then the technology focus is on quantum optics. Furthermore, if the focus is tightened to quantum key distribution (QKD), it is possible to define engineering goals such as improved sources and detectors, and to begin the construction of a technology roadmap for this area [27]. A next step from simple QKD is to consider few-qubit quantum processing, either for quantum repeaters to extend the operating distance of QKD, or for implementing distributed quantum communication protocols such as games, auctions, voting etc.. There is now some technology choice. Conversion from optical (communication) qubits to some sort of static matter-based qubits for processing, or doing everything all-optically. Given the open questions on qubit interconversion at this time, it is our view that the all-optical route should certainly be considered. With collaborators, we have proposed a very efficient (in terms of qubit resources) approach to distributed all-optical quantum processing [28, 29]. This relies on weak optical non-linearities in order to create, interact and detect photonic qubits. There are currently open research questions with regard to the realisation of appropriate non-linearities, but if these can be solved there is real technological potential in this approach.

For quantum metrology [16]-[23], the particular application influences the technology path. Phase measurement [17, 18], lithography [21] and weak force measurement [23] will likely use non-classical states of light (entangled, or maybe Schrödinger cat like superpositions). Improved frequency standards [19, 20] could come from clocks using entangled atomic states. Ultra-sensitive gyroscopes could be based on matter wave interferometry with entangled states [22].

If the application focus is quantum simulation, then something around 50 interacting qubits is the challenge, to realise something that could become an actual product. Again, there is some technology choice. The all-optical approach [28, 29] is possible, although it is likely that quantum memory (or at least buffering) would be needed, requiring a solution to the qubit interconversion problem. Solid state qubits form another possibility. The stated appeal of such systems is that fabrication expertise from existing IT may enable scaling—if you can build a few then you can build a lot. However, this has to be tempered by difficulties with coherence times and measurement. Superconducting qubits [30], one of the most promising solid state routes, have been around since 1999 [31], but are still only just at the two-qubit level [32, 33, 34]. There is clearly still a long way to go before solid state simulators become a viable proposition. Ion traps [35] are another possible technology route. Certainly they have shown impressive results with a few qubits [36, 37, 38, 39]. There are also proposals for scaling up the number of ions, connecting traps through quantum electromagnetic fields [40, 41], or using more complicated trap technologies [42, 43]. If the ion-trappers can get these proposals working, then, given what they've achieved to date, they could well have a genuine technology path to quantum simulators.

9. Towards QIT

We have presented a view on how a QIT industry might evolve, starting from the research base that exists today. It could bootstrap itself into existence, starting with one, or a few, relatively small scale and specialist applications. These could be based on quantum communication—not just quantum key exchange but including more sophisticated few-qubit/party protocols, requiring some modest quantum processing. Or they could be based on quantum-improved metrology and sensing. Or, if enough qubits can be mustered, there could be quantum simulators which can boldly go where classical computers haven't been before. In each of these cases there would seem to be viable markets, although clearly very small by current IT market standards. But there's potential for a start.

Although there are some choices, each of the suggested application areas have some clear technology routes. At this point it is therefore reasonable for a mini, application-specific and technology-focussed, roadmap to start emerging for each of the possible application areas. Certainly this is already happening, at least in part, for quantum communication [27]. However, in parallel with all this, it should not be forgotten that there is a real need for new application areas as well. New few-qubit applications would open up further bootstrapping opportunites, and new many-qubit applications with much wider commercial potential than factoring would provide an incentive for the current IT industry to look really long term, towards many-qubit scalable QIT.

These are very exciting times. The last decade or so has produced a great deal of stimulating and impressive QIPC research, with many important breakthroughs. More of this can be expected over the next decade. However, in addition, there is now a growing expectation for real quantum information technology. Certainly there are some promising avenues—applications, with an accompanying technology route—for seeding and growing a QIT industry. The next decade will show us which of these can turn promise into reality.

Acknowledgement

We thank Ray Beausoleil for numerous stimulating dicussions on this topic.

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, G. G. Ribordy, W. Tittel and H. Zbinden, Rev. Mod. Phys. 74, 145 (2002).
[4] T. P. Spiller, W. J. Munro, S. D. Barrett and P. Kok, "An introduction to quantum information processing: applications and realisations", to appear in Contemp. Phys..
[5] International Technology Roadmap for Semiconductors: http://public.itrs.net/
[6] ARDA Quantum Computing Roadmap: http://qist.lanl.gov/qcomp_map.shtml

[7] QIPC Strategic Report: http://qist.ect.it/Reports/reports.htm
[8] The original paper is available at: http://www.intel.com/technology/mooreslaw/index.htm
[9] 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.
[10] 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.
[11] See, for example, S. Lloyd, Science 273, 1073 (1996).
[12] J. Eisert, M. Wilkens and M. Lewenstein, Phys. Rev. Lett. 83, 3077 (1999).
[13] J. Eisert and M. Wilkens, J. Mod. Opt. 47, 2543 (2000).
[14] R. Kay, N. F. Johnson and S. Benjamin, J. Phys. A 34, l547 (2001).
[15] K.-Y. Chen, T. Hogg and R. G. Beausoleil, Quantum Information Processing 1, 449 (2002).
[16] A. V. Sergienko and G. S. Jaeger, Contemp. Phys. 44, 341 (2003).
[17] C. M. Caves, Phys. Rev. D 23, 1693 (1981).
[18] B. Yurke, S. L. McCall and J. R. Klauder, Phys. Rev. A 33, 4033 (1986).
[19] J. J. Bollinger, W. M. Itano, D. J. Wineland and D. J. Heinzen, Phys. Rev. A 54, R4649 (1996).
[20] S. F. Huelga, C. Macchiavello, T. Pellizzari, A. K. Ekert, M. B. Plenio, J. I. Cirac, Phys. Rev. Lett. 79, 3865 (1997).
[21] A. N. Boto, P. Kok, D. S. Abrams, S. L. Braunstein, C. P. Williams and J. P. Dowling, Phys. Rev. Lett. 85, 2733 (2000).
[22] J. P. Dowling, Phys. Rev. A 57, 4736 (1998).
[23] W. J. Munro, K. Nemoto, G. J. Milburn and S. L. Braunstein, Phys. Rev. A 66, 023819 (2002).
[24] http://www.idquantique.com/
[25] http://www.magiqtech.com/
[26] http://www.qipirc.org/
[27] ARDA Quantum Cryptography Roadmap: http://qist.lanl.gov/qcrypt_map.shtml
[28] W. J. Munro, K. Nemoto, T. P. Spiller, S. D. Barrett, P. Kok and R. G. Beausoleil, J. Opt. B: Quantum Semiclass. Opt. 7 S135 (2005).
[29] W. J. Munro, K. Nemoto and T. P. Spiller, New J. Phys. 7, 137 (2005).
[30] A. Shnirman, G. Schön, and Z. Hermon, Phys. Rev. Lett. 79, 2371 (1997).
[31] Y. Nakamura, Y. A. Pashkin, and J. S. Tsai, Nature (London) 398, 786 (1999).
[32] T. Yamamoto, Yu. A. Pashkin, O. Astafiev, Y. Nakamura, J. S. Tsai, Nature 425, 941 (2003).
[33] A. J. Berkley, H. Xu , R. C. Ramos, M. A. Gubrud, F. W. Strauch, P. R. Johnson, J. R. Anderson, A. J. Dragt, C. J. Lobb and F. C. Wellstood, Science 300, 1548 (2003).
[34] R. McDermott, R. W. Simmonds, M. Steffen, K. B. Cooper, K. Cicak, K. D. Osborn, S. Oh, D. P. Pappas and J. M. Martinis, Science 307, 1299 (2005).
[35] J. I. Cirac and P. Zoller, Phys. Rev. Lett. 74, 4091 (1995).
[36] C. A. Sackett, D. Kielpinski, B. E. King, C. Langer, V. Meyer, C. J. Myatt, M. Rowe, Q. A. Turchette, W. M. Itano, D. J. Wineland and C. Monroe, Nature 404, 256 (2000).
[37] S. Gulde, M. Riebe, G. P. T. Lancaster, C. Becher, J. Eschner, H. Haffner, F. Schmidt-Kaler, I. L. Chuang and R. Blatt, Nature 421, 48 (2003).
[38] M. Riebe, H. Haffner, C. F. Roos, W. Hansel, J. Benhelm, G. P. T. Lancaster, T. W. Korber, C. Becher, F. Schmidt-Kaler, D. F. V. James and R. Blatt, Nature 429, 734 (2004).
[39] M. D. Barrett, J. Chiaverini, T. Schaetz, J. Britton, W. M. Itano, J. D. Jost, E. Knill, C. Langer, D. Leibfried, R. Ozeri, D. J. Wineland, Nature 429, 737 (2004).
[40] J. I. Cirac, P. Zoller, H. J. Kimble and H. Mabuchi, Phys. Rev. Lett. 78, 3221 (1997).
[41] T. Pellizzari, Phys. Rev. Lett. 79, 5242 (1997).
[42] J. I. Cirac and P. Zoller, Nature 404, 579 (2000).
[43] D. Kielpinski, C. Monroe and D. J. Wineland, Nature 417, 709 (2002).