ANALYSIS OF QIST-RELATED GUIDELINES AND ROADMAPS OUTSIDE THE ERA

A COMPARISON OF THE US AND EU ROADMAPS

Version 1.0, December 2005

Authors: **D. Binosi** (Innsbruck)
T. Calarco (Harvard/Trento)

LIST OF ACRONYMS AND ABBREVIATIONS

QC	quantum computing
QCr	quantum cryptography
QIPC	quantum information processing and communication
QIST	quantum information sciences and technologies
QKD	quantum key distribution

The document "*QIPC – Strategic report on current status, visions and goals for research in Europe*" is a roadmap type document that expresses the visions and challenges for QIPC in Europe, addressing at the same time the current state-of-the-art of the field, an outlook on future efforts and a summary of long and medium term goals.

In such a rapidly evolving environment as the one characterizing the field of QIPC, with virtually any industrialized country running its own research programme, this is not the first example of such a document, for the US "*A Quantum Information Science and Technology Roadmap*" precedes the EU one by two years. Therefore, in an effort to examine QIST guidelines developed outside Europe, and their applicability to the European case, we present here a comparison between these two roadmaps. It should be clear from the outset that this comparison is not written with the objective in mind of establishing which of the two documents better serves the purpose of facilitating the progress of QIPC research towards the quantum computer science era; in contrast, its function is to highlight the differences that are to be found in them, explain why they are there and possibly point towards a way of integrating the two documents.

GENESIS OF THE ROADMAPS

The paths that have led to the creation of the US and EU roadmap on QIST are quite different (and, in a sense, opposite), something that is at the root of many, if not all, of the differences that characterize the two position documents.

In particular, as far as the US roadmaps are concerned,

The US roadmap genesis: the top-down approach

- the US government agency Advanced Research and Development Activity (ARDA) appointed a Technology Expert Panel (TEP) with the objective of writing a QC roadmap, to "*facilitate the progress of QC research towards the quantum computer-science era*". The panel work started with a two-day "Quantum Information Science and Technology Experts Panel Meeting" held in La Jolla, California, USA, in late January 2002, where the panel's members established the objectives that should be pursued by QC research (see next section) and consequently decided to write the roadmap with among its many intents the one of setting a "*path leading to the desired QC test-bed era by 2012 by providing some direction for the field with specific five- and ten-year technical goals*". A year later a second TEP was appointed with the objective of writing a QCr roadmap, to "*facilitate the progress of quantum-cryptography research towards a practical "quantum information-assurance era" in which quantum cryptography becomes more closely integrated with conventional, basic, and applied information-security and communications research*". Work on the roadmap started immediately afterwards, with a "Quantum Cryptography Technology Experts Panel Meeting" held in Warrenton, Virginia in June 2003, where once again a set of QCr objectives was established, and the writing of the roadmap [which focuses only on QKD topics] started with one of its aims focused on the setting of a *"path leading to the desired quantum information-assurance objective by 2014 by providing some direction for the field with specific high-level technical goals."*

In the EU case, on the other hand,

The EU roadmap genesis: the bottom-up approach

- the potential of QC and QCr was quickly recognized by FET, the Future and Emerging Technologies Unit of the Directorate General Information Society of the European Commission, whose pathfinder activity played a crucial role for the development of the field in Europe. At the 5th European QIPC Workshop (September 2004 in Rome) a special session was organized by FET, entitled "Perspectives for QIPC in the Seventh Framework Program". The main point was that input towards the European Commission would be needed on the part of the scientific community for the preparation of the Seventh Framework Program. There was a general discussion on the actions to be taken with the aim of promoting QIPC research in Europe, strengthening its image in a coherent way, unifying the research community by elaborating a common European strategy and goals, and, especially, providing the required input to the European Commission, reaching decision makers in an appropriate way. It was then decided (i) to write a strategic report including an assessment of current results and an outlook on future efforts, and (ii) to expand the strategic report with a detailed technical assessment, to draw up a summary of long and medium term goals, and to express visions and challenges for QIPC in Europe. A committee was nominated in charge of this, and work on the document started immediately afterwards.

This brief account of the document genesis clearly shows the top-down nature of the US approach to the QC and QCr roadmaps and the bottom-up nature of the EU one; this is far from being an anecdotal fact, and has, as we will see, an important impact on the scope, purpose, structure and content differences of the two documents.

THE DIFFERENT SCOPE AND PURPOSE OF THE US/EU ROADMAPS

The US and EU roadmap scope

Probably the most important difference in the two roadmaps under scrutiny is the purpose for which they have been written. As has been pointed out in the previous section, the US roadmap was written following a top-down approach, with the roadmap being commissioned from a government agency (ARDA) to a specially appointed TEP; the genesis of the EU roadmap has instead followed a bottom-up path, since it was the QIPC community that had identified the roadmap as an appropriate way of reaching decision makers, and therefore elected a committee in charge of writing it. This implies a broader scope in the case of the EU roadmap, as on top of the common purpose that the two documents should serve, it has the pivotal function of identifying specific measures (in the form of organizational, investment and infrastructure developments) that the EC should urgently take in order to maintain the EU research in QIST related subject at the forefront.

The top-down and bottom-up approaches as a result of different funding policies

These different approaches can be seen in fact as a by-product of the different policies that characterize the US and EU funding in QIST. The latter represents a priority research area in the US, with a total federal investment of nearly \$100M/yr. On the other hand, as the EU roadmap notice "*a [European] commission investment of €7M/yr will compete very poorly with the US*", and the roadmap has been taken as the first of a series of initiative for maintaining the European QIPC research at the forefront. This aspect has an evident impact on the structure and content of the EU roadmap which in contrast to the US one (i) presents an entire section dedicated to a detailed analysis of the funding of QIPC research at the national, European and worldwide level, and (ii) has in general a narrower focus on the QIPC research carried out in European labs (and therefore some topics have been stressed more than others).

Moreover, the antithetic top-down/bottom-up approaches are reflected throughout the documents, and in particular in the way objectives have been defined and identified. In the US case

- the TEP has identified very challenging objectives to meet, and in particular
  - for QC, to "*develop by 2012 a suite of viable emerging-QC technologies of sufficient complexity to function as quantum computer-science test-beds in which architectural and algorithmic issues can be explored*", which has been broken down into "*desired high level goals*", namely to "*encode a single qubit into the state of a logical qubit formed from several qubits, perform repetitive error correction on the logical qubit, and transfer the state of the logical qubit into the state of another set of physical qubits with high fidelity*" (year

The US goals for QC (2012)

2007 goals) and to "*implement a concatenated quantum error-correcting code*" (year 2012 goal);

The US goals for QCr (2014)

- for QCr, to "*develop by 2014 a suite of practical quantum cryptographic technologies of sufficient maturity, accessibility, and robustness that they can, either as stand-alone systems or when seamlessly integrated with conventional information assurance methods, provide new, secure communications tools, which can be evaluated as value-added ingredients of future secure communications solutions with consistent and demonstrable benefits*", which has also been broken down to some high level goals, namely to "*implement networked, secure communications testbeds over metro-area distances in optical fibers and over free-space optical communications paths using "first wave" QKD-enhanced key management*" (year 2007 goal), to "*implement networked, secure communications testbeds using ("second wave") advanced light source QKD encryption, in optical fibers over metro-area distances, and over few-kilometer free-space optical-communications paths*" (year 2010 goal), and to "*develop integrated QKD-based key management and encryption to support secure networks from intra-net scale to long-haul optical fiber and satellite optical communications*" (year 2014 goal);

- given the above goals, the TEP has then described in the roadmap what it considered to be the necessary steps to reach them starting from the state-of-the-art of the different QC and QCr implementations.

In contrast, in the EU case the roadmap committee has

- described the state-of-the-art of the different candidate QC and QCr implementations and assigned to each of them a different set of five and ten years goals;
- given the above, the committee has isolated a unique ten years goal, namely

The EU goals for QC (2015)

  - for QC to "*develop a few-qubit general-purpose quantum processor including error correction, as a model system to demonstrate quantum algorithms and various quantum computing architectures, and with emphasis on potential scalability*";

The EU goals for QCr (2015)

  - for QCr, to "*develop quantum cryptography towards becoming an established technology and a commercial product,* […] *to demonstrate long-distance quantum communication both in optical fiber and in free space, [and] on the 5-10 year time scale,* […] *to gain several orders of magnitude on the secret bit rate and to demonstrate quantum repeaters.*"

All the above mentioned aspects also influence the general prescriptive and descriptive purposes of the two roadmaps. In the US case:

The US roadmap prescriptive…

- the roadmap prescriptive role is the "*identification of what scientific, technology, skills, organizational, investment, and infrastructure developments will be necessary to achieve the desired goal, while providing options for how to get there*";

…and descriptive roles

- the descriptive function is of "*capturing the status and likely progress of the field while elucidating the role that each aspect of the field is expected to play toward achieving the desired goal*".

In the EU case however

The EU roadmap prescriptive…

- the roadmap prescriptive role is the identification of the organizational, investment and infrastructure developments (in particular the need of a dedicated QIPC ERA – European Research Area) that would be necessary in order to keep the European QIPC research at the forefront;

…and descriptive roles

- the descriptive function is of analyzing the state-of-the-art of different QC implementations and the likely progress (at five and ten years) that could be achieved in the latter.

The roadmaps common objectives

On the other hand both roadmaps: (i) are intended to be an aid to researchers and to those managing or observing the field by (ii) identifying strengths and weaknesses, as well as places where strategic investments would be beneficial; (iii) providing a framework for coordinating research activities and a venue for experts to provide advice; (iv) allowing informed decisions about future directions to be made, while tracking progress, and elucidating interrelationships between approaches to (v) assist researchers in developing synergistic solutions to obstacles within any one approach.

The need for a 'living document' policy

Clearly, the ambitious aim of describing such a rapidly evolving field, forces both roadmaps to be published as 'living documents', with scheduled (and possibly *ad hoc*) updates which allow the incorporation of new advances in the field, modify the roadmap structure to better capture new challenges that might arise, add sections on topics that could not be covered in previous versions and reflect on the purpose, impact, and scope of the roadmap, as well as its future role. In particular version 1.0 of the US QC roadmap was released in December 2002, and version 2.0 was released in April 2004; version 1.0 of the US QCr roadmap was released on July 2004. The EU roadmap is much younger: version 1.0 was released in May 2005 (with a description of the state-of-the-art of the different fields as per November 2004), and this version will continue to be updated regularly in the context of the European funded project ERA-Pilot QIST (in particular by its Workpackage 1). The next release, which will incorporate the new advances in the field until October 2005, is scheduled for December 2005/January 2006.

One step further: the ERA-Quantiki project

Also in line with the bottom-up approach that has characterised its genesis, the ERA-Pilot Workpackage 1 is running and maintaining a wiki version of the roadmap that *anyone* can edit, and which is used as a feedback channel that the entire QIPC community can use to suggest modifications and/or additions to the document (see http://cam.qubit.org/wiki/index.php/Category:ERA_Quantiki_Project).

STRUCTURE

The US roadmap four-level division

In the US case, both the QC and QCr roadmaps have been structured in a four level division, namely

- high level goals (the TEP suggested attainable technical objectives to be pursued),
- mid-level descriptions (which capture the breadth of QC approaches and QCr technologies with a graphical format),
- detailed level summaries (providing more information on the essential concept of each QC approach an QCr technology), and a
- general summary describing the TEP recommendations for optimizing the way forward.

The EU roadmap differences

In the EU case, the structure is rather similar, retaining the presence of some general QIPC research objectives in the coming five to ten years, detailed level summaries, and the roadmap committee recommendations. However

- the mid-level descriptions are absent, and
- there is an entire chapter addressing the different aspects of QIPC research in Europe (with a particular emphasis on a detailed view of QIPC funding at the national and European level).

The US promise criteria / attributes and development status metrics

While the presence of the QIPC funding chapter can be understood in the light of what has been described in the previous sections, the absence of the mid-level descriptions deserves few words of explanations. In the mid-level descriptions, the US TEP insists on the determination of a set of common criteria and metrics to use as a strict way to describe the state-of-the-art of a particular QC implementations and QCr technologies. Each of the latter has then two sets of metrics that characterize it

- one is represented by the "*promise criteria*" for QC (the DiVincenzo criteria) and the "*attributes*" for QCr: the former identifies the promises of that particular approach as a candidate QC technology, the latter how much a QCr approach is appealing in one or more respects;
- the second (the "*development status metrics*" in both cases, but with of course different parameters) captures the status of the QC/QCr approaches in terms of the technical advances "*along the way to achieving the high level goals*".

Promise criteria / attributes and development status metrics need to be considered simultaneously

However, when addressing a particular QC implementation, promise criteria and development status metrics need to be considered simultaneously. It can happen, for example, that a particular approach (e.g., solid state implementations) offers great potential for achieving scalable QC technology (good promise criteria) but is far from the high level goals in its development status metric; or, vice-versa, it may show that multiple steps have been achieved towards the high level goals, but does not offer good scalability potential (e.g., in the case of nuclear magnetic resonance implementations). For QCr approaches the same holds true, but in this case the attributes metric has been chosen in such a way that a particular score in one of its entries merely indicates that the approach is more suited or less suited in this one respect than in some other one.

Absence of these criteria in the EU roadmap

In the case of the EU roadmap, the development status metrics are not present, since we recall that no high level goals common to all QC implementations have been developed; on the other hand, the DiVincenzo criteria are there, and employed for the various QC implementations, even if their use is limited and not as systematic as it is in the US roadmap. Finally, attributes for QCr approaches are totally missing. On the other hand, the subtleties of interpretation, together with the variety of QC/QCr approaches and the number of parameters that have to be considered, tend to limit the usefulness of the graphic representations that the US roadmap proposes, this being the main reason as why an equivalent representation has not been adopted, for the moment, in the EU document.

CONTENT

The three topics division: QC-experiment, QC-theory and QCr

Both documents present the same division into the three major topics of QIPC: Quantum Computing, Quantum Cryptography and Quantum Information Sciences Theory (the latter being present starting from version 2.0 of the QC US roadmap). However, while the EU roadmap presents them all in a single document, the US one is divided in two parts, with Part 1 addressing Quantum Computation and Quantum Information Sciences Theory, and Part 2 Quantum Cryptography.

In table 1 we give the rough correspondence linking the subjects treated in the two documents regarding the approaches to QC and QCr are concerned.

QC-experiment content differences

As far as the former are concerned, the reason that there is such a large number of QC approaches in both documents, is due the fact that it is too early to single out the winning technology for the practical implementation of a QC device; it is even possible that the concrete technology has not yet been developed. One should notice, however, that the main difference between the two documents is the absence in the EU roadmap of the Nuclear Magnetic Resonance approach to QC. This is due to the fact that the EU roadmap committee has decided for a narrower focus on QC technologies which present (at least in principle) a high potential for scalability (as is clear from the declared QC ten year goal). Clearly this is not the case for NMR, since no viable approach is known to meet the first DiVincenzo criteria ("a scalable physical system with well characterized qubits") for such an approach. Other differences are

- the US 'Neutral Atoms' and 'Cavity QED' approaches to QC are condensed in the single EU 'Atoms and Cavity QED' section;
- the US 'Optical' approaches to QC section have a broader view than the corresponding EU section, since these approaches can include "*nonlinear*

elements as crucial elements provided those nonlinear elements are readily available or under development";

- the EU 'Impurity spins in solids' is only one of the possible technologies constituting the US 'Unique qubits' approaches to QC section, which presents therefore a broader view of potentially fruitful approaches to QC based on different quantum technologies.

QC-theory content differences

As far as the theory sections are concerned, the US document present sections on quantum algorithms and quantum computational complexity, quantum information theory, quantum computer architectures and the theory of decoherence. Each of these sections has its counterpart in the EU roadmap, which also presents a part on spin-offs of quantum information sciences, showing the impact that the theoretical work in this area is beginning to make on other scientific areas (e.g., quantum imaging, etc.).

QCr content differences

In the case of QCr, there are two main differences:

- the EU document identifies the two means by which QKD can be achieved, i.e., fiber and free-space systems, and accordingly describes various kinds of QKD implementation (weak laser pulses, single photon, entangled pairs, etc.); the US roadmap does the opposite: it identifies the QKD implementations and describe their realization in fiber and free space systems.
- the US document focuses exclusively on QKD protocols (with, however, a declared intention to "*extend the scope of the roadmap to non-QKD quantum cryptographic protocols in future versions*"), the EU roadmap presents a broader view on the subject, for it (briefly) describes research directions that go beyond QKD cryptographic protocols, and, in addition, develop in some details the problems of building interfaces between quantum information carriers and quantum information storage and processors, as well as quantum repeaters;

Quantum Computing approaches			
US roadmap (Part 1)		EU roadmap	
6.1	Nuclear Magnetic Resonance		
6.2	Trapped Ions	4.2.1	Quantum Computing with Trapped Ions
6.3	Neutral Atoms	4.2.2	Atoms and Cavity QED
6.4	Cavity QED	4.2.3	Atoms and Cavity QED
6.5	Optical	4.2.4	Linear Optics Quantum Computation
6.6	Solid State	4.2.5	Semiconductor Quantum Dots
6.7	Superconducting	4.2.6	Superconducting Circuits
6.8	'Unique' Qubits	4.2.7	Impurity Spins in Solids
6.9	Theory Component	4.3	Quantum Information Science Theory

Table 1: Comparison of the two roadmap content for the experimental QC approaches.

Quantum Cryptography			
US roadmap (Part 2)		EU roadmap	
6.1	Weak Laser Pulses over Fibers	4.1.1 4.1.2	Fiber based Systems Free Space Systems
6.2	Weak Laser Pulses through Free Space		
6.3	Single-Photon Light Sources		
6.4	Entangled Photon Pairs		
6.5	Continuous Variables		
		4.1.3	Quantum Interfaces and Memories

Table 2: Same as in Table 1 but for the QCr subject.

CONCLUSIONS

Clearly QIST has the potential to revolutionize almost all the areas of science and technology, providing us with unprecedented computational power, provably secure communications, etc. However, as for any other new paradigm, the advent of quantum computing technology will entail some level of risk.

The need for a broader view, beyond factoring and security issues

Much of the "secure" communications in the world today use public key cryptography (like the omnipresent RSA cryptographic scheme), which is based on the fact that no efficient classical algorithm for factorizing a large number is known. Therefore the construction of a many thousand qubits quantum computer has the potential to trash the world communication infrastructure. The US roadmap is particularly sensitive to the problem, and the TEP choice of the exclusive focus on QKD given in the QCr part is significant: quantum cryptographic systems are in fact the only ones that are safe against any attacks, including the ones coming from quantum computers. On the other hand, the building of a quantum repeater (an essential device if one wants to extend the working distance of quantum cryptosystems) will require a quantum device of a few tens of qubits (in contrast to the many thousands needed for efficient factoring), and consequently it is much more likely that we will have global provably secure communications before quantum code breaking. In this light, the absence in the US roadmap of a section/part dedicated to quantum repeaters is perplexing.

The importance of QC-theory should not be underestimated

Another point that is not sufficiently stressed in the US roadmap is that hardware development is certainly necessary, but certainly also not sufficient. Present day IT companies measure their annual revenue in billions of dollars/euros. If such mass-market scale or consumer QIST is to emerge in the future, new quantum applications, software and protocols (beyond the QKD so profusely described in both roadmaps) will be needed. Extrapolating from the current figures on annual investment in QIPC worldwide, the development of a scalable quantum computing device first, and then of a large scale quantum computer will be very expensive (in the order of several hundreds billions of dollars): these efforts therefore need the promise of a market, and the latter will be unavoidably linked to new ideas coming form the QIPC theory community.

The European flavor

The distinguishing feature of the European effort when one compares it with other international QIPC research programs in general, and the US one in particular, is (i) its broader scope, which goes beyond the focus on specific issues (e.g., security) or special applications (e.g., factoring), and (ii) its strong theoretical component and emphasis on fundamental physics. Particularly important is its effort to describe how related fields can benefit from the emergence of QIST and what are the spin-off technologies that one may expect (quantum based sensors, quantum metrology, quantum imaging, etc.)

Improvements of the EU roadmap are also needed

On the other hand the EU roadmap is not perfect: it would probably benefit from having a mid level review (similar to the US one, but simpler) that would catch the status of each QC/QCr implementation; the balance between scientific and funding issues should also be tuned to favor the former over the latter (but this will most likely happen if in the next Framework Program – FP7 – the creation of a European Research Area for the QIST field comes off).

Towards a common roadmap

Integration is the key: a joint international meeting between the US TEP and the EU roadmap committee, from which the emergence of a joint strategy leading to a common roadmap could be envisaged, would be very beneficial for the whole field.