

Quantum Cryptography - Out of the Laboratory and Into the Market

25 and 27 April, 2005
and DTI

Bank of England

Introduction - Charles Hughes (QIP LLP)

These notes summarise a series of three events organised by Quantum Information Partners LLP, and hosted by Alastair Clark, Adviser to the Governor of the Bank of England, and Ray Browne, Deputy Director, Key Business Technologies, at the DTI. Their purpose was not to recommend or to promote Quantum Technology, but to provide a factual account of what is possible, what is being done and why. Secure Messaging is a critical part of today's business infrastructure, and business leaders need to understand the risks to which they could be exposed by future developments in technology, and the ways in which they can be mitigated. These events brought together academics, development teams, product suppliers and business leaders to share information on this fast developing field.

Context – New Situations, Solutions and Opportunities - Charles Ross (QIP LLP)

Why Quantum Cryptography?

Classical cryptographic systems all have weaknesses that can be attacked by software running on powerful computers. Systems that were considered secure 20 years ago can now be routinely broken – much sooner than their inventors anticipated – and there are concerns that today's systems could equally be broken at some time in the future as a result of advances in mathematics, computation or both. Moreover, there is active research world-wide aimed at developing a quantum computer, which, once realised, would be capable of breaking many existing codes. Quantum Cryptography uses intrinsic physical phenomena implemented in hardware to provide inherently secure communications, and has the potential to offer the only known antidote to quantum computers.

Secure Data Communication Today

Today's secure high-speed data transmission systems use symmetric encryption algorithms, which rely upon a secret cryptographic key, known to both sender and recipient. Anybody who can discover this secret key is potentially able to decode the data. In the most secure environments keys

are transported physically by courier. This is expensive, open to compromise, and not conducive to frequent changes of key, which would reduce the risk and scope of exposure. The alternative is to distribute the keys electronically using public key cryptography. This depends upon asymmetric encryption algorithms, which use pairs of keys, only one of which is secret. These algorithms rely upon one-way functions, which are used to generate the asymmetric key pairs, but make it computationally infeasible to deduce one key from the other. The concern is that future advances in mathematics or in computation could enable secret keys distributed in this way to be discovered, and that data transmitted today and recorded by an eavesdropper might be decoded at some time in the future to the potential embarrassment of both sender and receiver. Quantum Key Distribution (QKD) can provide protection against such an eventuality, as well as offering an automated process that is easier and cheaper to operate than either physical key distribution or public key infrastructure (PKI).

Quantum Cryptography Today and in the Future

Quantum Cryptography is based upon the encoding of data on individual photons of light, which can be transmitted through optical fibres or on a line of sight through free space. This allows the laws of physics to be invoked either to detect that a transmission has been intercepted, or to guarantee that it has not.

Products using these techniques are available now, and can demonstrate continuous, reliable operation. At present, there are limits on the speed and length of the quantum links, and current practice is to use these only for key distribution. Data can be transmitted over a conventional network, encrypted with the quantum keys.

QKD can operate on either a synchronous or asynchronous basis. In the former case, keys are transmitted continuously, and each is used only until the next is received. This allows very frequent changes of key. In the latter case keys are exchanged when the quantum channel is open, for use at some time in the future. This is appropriate in circumstances where the quantum channel uses, for example, low orbit satellites, which may be only intermittently accessible.

Today's equipment will distribute up to 100 independently generated random 256 bit keys per second, although higher speeds can be anticipated in future. If these are used as one-time pads, absolute security can be guaranteed, but each message can be no longer than the key used to encrypt it. For higher speeds, a conventional symmetric cryptographic algorithm can be used; the ability to change keys 100 times every second significantly reduces the risk of compromise.

Point-to-point fibre links of up to 120km are possible. For greater distances, links can be chained, but the relay points are a weakness and must be physically secured. Quantum repeaters which overcome this limitation are likely to be possible in future. Free space links are limited to line-of-sight

communication. This can be between tall buildings today – in the future via satellite, weather permitting.

Quantum communication currently operates only on a point-to-point basis. In the near future, hybrid networks are likely to be built which integrate quantum key distribution with conventional routers in a physically secure environment. Ultimately, optically switched networks combined with quantum repeaters might allow end to end quantum communication.

Current Views of Quantum Cryptography

General awareness of QC is extremely low, even within the Information Systems community. Among those who do have some familiarity with the topic, five shades of opinion have emerged.

1. Some still believe that current software-based cryptography will meet all needs for the foreseeable future.
2. There is a growing band of opinion, however, that QC offers enhanced security for the transmission of critical data over insecure networks such as the Internet.
3. In some contexts Quantum Key Distribution (QKD) is attractive in its own right for the simplified administration and enhanced security that it can offer.
4. In others, a specialised network, implemented entirely with quantum technology, would be more attractive.
5. And there is a growing realisation that once quantum computers are developed, quantum cryptography may be the only antidote.

Quantum Technologies and their Impact - Professor Andrew Briggs (QIPIRC)

Professor Briggs is Director of the Quantum Information Processing Interdisciplinary Research Collaboration (QIPIRC) , which forms the focus for UK research in Quantum Information Processing (QIP), encompassing both quantum computing and quantum cryptography. The development of QIP depends upon the ability to manipulate matter at the level of individual atoms, electrons and photons, and recent scientific publications demonstrate the rapid progress that is being made.

QIP exploits three phenomena that are intrinsic to the fundamental laws of quantum physics

- Superposition – a quantum bit (qubit) represented by a single photon or electron, can represent a '0' and a '1' simultaneously.
- Entanglement – measurements on related qubits can still be correlated when they are physically separated
- No Cloning – quantum information cannot be copied without introducing errors

The third of these is central to quantum cryptography(QC) in that it implies that quantum data cannot be intercepted without detection.

The UK has a leading position in QIP research, with many world firsts, but our history and culture has not proved conducive to commercial development and exploitation. There is an opportunity now for the UK to pioneer the business exploitation of Quantum Cryptography. Such inventions have often proved to have applications far beyond those anticipated by their inventors, and this could well be no exception. Already other financial centres, such as Singapore, are moving to build QC networks. We should not allow London to be left behind.

Business Implications - Professor Brian Collins (RMCS Cranfield University)

The controlled sharing of secrets is now a critical business need. Current mechanisms for doing this all depend upon computational infeasibility, and ultimately Quantum Computing will defeat them. Businesses need to be able to guarantee confidentiality, integrity, availability, authentication and non-repudiation of transmitted data. Quantum Key Distribution, combined with an appropriate method of link initiation, provides help with some of these, and further developments in QC will provide more help in the future. When quantum computing ultimately breaks conventional cryptography, QC may be the only game in town.

Implications for Banking - Stuart Brocklehurst (VISA International)

The UK economy is heavily dependent upon Banking – some 32% of GDP, and today's banking depends heavily upon cryptography. PKI-based key exchange is widely used, and this is subject to mathematical risk and will ultimately be compromised by quantum computers. Cryptography is needed both to guarantee the secrecy and integrity of customer information, and to protect against fraud. The banking system has always tolerated some level of fraud, and it has proved sufficient to provide protection at a level that makes a concerted attack by fraudsters uneconomic. However, the climate is changing, with attacks aimed primarily at disruption becoming increasingly likely. Anything which could damage public confidence in the banking system would have serious implications, and this could happen as a result of press hype relating to real or imagined vulnerabilities, as well as in response to actual disruption.

Recent banking practice has been to keep the level of threat under continual review, and to carry out major infrastructure upgrades when it reaches unacceptable levels. However, this process is expensive, and takes a great deal of management attention.

QC today provides nothing new in cryptography as such, but it does offer absolute security in key transmission. Currently it has its limitations in terms of distance and network topology, but these are gradually being overcome. In the meantime, there are applications for which it would be comparatively inexpensive and non-disruptive to deploy.

The Finance industry is not fast-moving, and major infrastructure upgrades can take many years to deploy. Whilst the level of security offered by QC might not be necessary today, it could well be justified by the saving in cost, management effort and disruption from avoidance of the need for future upgrades. Now is the time for the industry to undertake practical trials, which will enable it to understand at first hand the benefits and limitations of this technology.

The State of the Art Today

Dr Andrew Shields - Toshiba Research, Europe

Toshiba has developed a Quantum Key Server, which can generate and distribute up to a hundred 256 bit keys per second over an optical fibre in excess of 120km in length. It uses a 'one way' design, and its security has been rigorously proven. It is self-initialising and managing, and designed for continuous operation. In trials with MCI over a 20km link in Cambridge, four weeks of continuous hands-off operation were demonstrated.

As a future development, Toshiba envisage a combined router and quantum key server, which can use a common fibre for both data and key exchange. This will enable specialised secure networks to be built, provided that the nodes can be physically secured. In the longer term, the development of quantum repeaters based upon entanglement, combined with optical switches, could enable end-to-end quantum protection.

Dr Brian Lowans - QinetiQ Limited

QinetiQ has a long history in the field of QC, having been the first to demonstrate its feasibility over optical fibre in 1993. In 2002 it established a record of 23km for free space transmission, and in 2005 it delivered a free space QC system to BBN as part of the DARPA-funded Quantum Net initiative. This has been proven in continuous 24x7 operation.

Quantum Key Distribution and generation on a line of sight building-to-building basis is demonstrable now. It is easy to install and capable of continuous operation. A demonstration over 150km in the Canary Islands, funded by ESA is planned for later in the year, with the possibility of world-wide operation by satellite in the foreseeable future.

Grégoire Ribordy - id Quantique SA

Id Quantique has just launched its Vectis link encryptor. This uses a dedicated pair of optical fibres for key exchange, while data are transmitted over a conventional Ethernet connection using AES encryption. Full management capabilities are provided. One of the first commercial QC applications that they have demonstrated is for secure data replication between two computer centres.

Kevin B Latravers - MagiQ Inc.

MagiQ has been selling commercial quantum key distribution systems for 18 months. Their QPN security gateway provides QKD in a VPN environment, and allows encryption keys to be exchanged at least once per second over fibre links up to 120km in length.

Initial users have tended to be organisations that are concerned about the long term security of data transmitted today. The ease with which many of today's fibre links can be tapped has also been a cause of concern. Links to data centre back-up sites have been a popular application, particularly for organisations that are moving from passive back-up to active load-sharing operation.

High security environments that previously relied upon physical key distribution have also found that QKD can reduce costs as well as enhancing security through more frequent key change. Some Telcos are now looking at providing QKD as a value-added service.

The Way Forward - Mark Aldington (QIP LLP)

Quantum Computing is out of the laboratory now. Fourteen organisations around the world claim to have practical systems, and four of these have been demonstrated in London this week. Deployment is actively being planned in Austria, Singapore and the USA. Once the computational challenges of conventional cryptography have been overcome, either through realisation of a quantum computer, or from advances in mathematics and conventional computation, QC may be the only game in town.

In order to maintain the UK's leadership position in this important and fast-developing field, QIP LLP proposes the inauguration of a Quantum Knowledge Network encompassing:

- Monitoring Facility – a facility for the intelligent dissemination of information to interested parties
- Knowledge Transfer Network – for two way communication between developers and potential end users
- Participation in the US-initiated standards activity (Stuart Brocklehurst is already involved in this)
- Demonstration of the City of London's lead with a real quantum network
- Design of target applications – to facilitate the wider exploitation of QC potential

This subject is too important to ignore. The only question is whether we all move slowly forward individually, or more effectively with. QIP as the knowledgeable bridge between technology and business applications is ideally placed to co-ordinate this effort.

Dr. Alan Shepherd
May 2005-05-03

Questions and Answers

Q What level of expertise is required for the operational management of this technology?

A Today's products are easy to set up and manage and are designed for continuous unattended operation. There is less management overhead than with traditional technologies such as PKI.

Q Might this ultimately be applicable to the mass consumer market?

A Maybe in the long term, but the availability of optical fibre to the home will be a limiting factor?

Q Will there be government restrictions on the deployment of this technology?

A Maybe in some countries, but essentially the genie is already out of the bottle.

Q In the mesh network illustrated by Toshiba, aren't the nodes insecure?

A Yes, they would need to be secured by physical means. Work is being done on various techniques that might overcome this limitation in the future. Once quantum computers are developed, quantum repeaters could be realised with the same technology.

Q Does QC only handle key distribution?

A Current products are designed for QKD, but work is going on to develop more comprehensive products for the future.

Q The use of one key per message has been established for years in the context of credit card authorisation.

A Yes, but with QKD each key is generated independently.

Q QC does not overcome the link initialisation problem.

A Agreed

Q QKD protects only the keys from interception.

A Yes, but the messages can be protected with stronger encryption.

Q What is today's cost for a QKD system?

A Around £50 - 100,000 plus the cost of the link. Costs will come down as the market develops.

Q What is the size of the market?

A Tens of millions of pounds in the short term.

Q How will QC fit in with the current move to IP-based VLAN network structures?

A QKD products are designed to work alongside this technology. Next generation networks are expected to use optical switching, and may incorporate QC technology more directly.