European Foresight Platform
supporting forward looking decision making
www.foresight-platform.eu

Prospects of Quantum Key Distribution: Making Data Communication Secure for the Future

EFP Brief No. 183

Authors: Susanne Giesecke Susanne.Giesecke@ait.ac.at
Thomas Länger Thomas.Laenger@ait.ac.at
Sponsors: European Commission, DG Infso, ETSI (European Telecommunications Standards Institute)
Type: Single issue
Organizer: Austrian Institute of Technology, ETSI
Duration: 2008-2010 **Budget:** 250,000€ **Time Horizon:** 10 years **Date of Brief:** May 2011

Purpose

The application of the highest information-theoretically secure cryptographic primitives for securing data transmission was long considered unfeasible because of a missing primitive for the distribution of the necessary cryptographic keys between sender and receiver ensuring a comparable level of security. With quantum key distribution (QKD), a technology has been invented that enables the generation and distribution of appropriate cryptographic. ETSI started a standardisation initiative including foresight elements looking into the next ten years of QKD applications.

"Theoretically Perfectly Secret"

Participation in the information society means becoming more and more dependent on data exchange via electronic communication networks; relying on their proper guarding of communication confidentiality, integrity, and property of origin and destination. Quantum key distribution (QKD) with its strong long-term security perspective is an important building block of reliably secure communication networks. It has the potential to increase the usability and acceptance of the typical services that mark the information society of today and tomorrow. Experts expect that QKD will allow ultra-secure encryption of sensitive data sent by banks, hospitals and government organisations and enable the everyday use of "one-time pad" encryption, the only known method that is theoretically perfectly secret.

While QKD now seems to be on the verge of commercialisation, there is still a lot of hype and misunderstanding around the technology and its potential use. The QKD initiative at ETSI was used to analyse the technology behind QKD and how it relates to other security technologies, on the one hand, and display developments and recent milestones towards practical application, on the other.

Reaching out to the Prospective User

Economic success is especially important for the future development of QKD. To get it out of its role as a niche technology for military and intelligence services only, a commercially successful use for a broader user group is necessary. Obvious application scenarios exist within the banking sector and in information and communication technology systems in large urban areas.

One challenge for the successful commercialisation of quantum cryptography is the gap between the developers of the technology and the prospective users. Developers are usually experimental physicists, and development is driven by scientific interest rather than by consumer demand turning on issues of practical use. At the same time, prospective users are hardly able to recognize what benefits quantum cryptography can yield for them.

Hence, one important goal of this activity was to bring the developing scientists and prospective commercial users together to allow them to learn from each other what the technology is able to deliver and what is needed for practical application. Standardisation of a reference model for business application will be essential for the market uptake of QKD because perfectly secure communication, to the extent that it can be achieved with quantum cryptography, is clearly at odds with today's trend towards all-embracing surveillance.

The EFP is financed by the European Commission DG Research. It is part of a series of initiatives intended to provide a 'Knowledge Sharing Platform' for policy makers in the European Union. More information on the EFP and on the Knowledge Sharing Platform is provided at www.foresight-platform.eu

Working with the Standardisation Group

The work was mainly anchored in the cooperation of the Industry Specification (ISG)-QKD ETSI group on standardisation, which comprised an impressive representation of top ranking universities and other research organisations, security and telecom corporations from Europe, North America and Asia as well as start-ups. The prospects of QKD and its applications were discussed in consecutive group settings every six months over a two-year period as well as in single and group interviews with these and additional QKD experts. This approach was complemented by desk research of scientific literature, by bibliometric research and by a world-café-like setting with participants from the standardisation group and additional stakeholders to assess future prospects and the drivers and inhibitors for their realisation.

Recent Milestones

Of all quantum technologies quantum cryptography – or more precisely quantum key distribution – is nearest to market application, say market analysts. Some companies already offer off-the-shelf market products, which have proven their reliability in several demonstration projects and field tests.

In the fall of 2007, the Geneva government used the technology provided by the Geneva-based start-up *Id Quantique* to secure the network processing voting results.

Within the SwissQuantum project, a quantum key distribution network connecting the *European Organization for Nuclear Research (CERN)*, *University of Geneva (UNIGE)* and the *Engineering School of Geneva (HEPIA)* has been designed and deployed to demonstrate the reliability and robustness of QKD technology for encryption over metropolitan area networks (MAN; http://www.swissquantum.com/).

The first QKD network in Japan was launched in October 2010 as a live demonstration of an operational quantum key distribution network in the Tokyo metropolitan area.

Non-Technical Drivers and Inhibitors

Although more and more businesses see the need to increase the security and reliability of their networks and have to prove this to their customers, quantum key distribution currently seems to be perceived more as a solution looking for a problem. Insiders see a chance for QKD systems today where very ***sensitive to confidential information*** is handled and conventional cryptography is not enough. But the majority of the corporate world cares more about compliance than being at the forefront of IT security. The QKD community has not been able to make potential customers aware that QKD is a more differentiated product than conventional security systems.

Among experts, there is quite some debate about the prospects of a ***breakthrough in asymmetrical cryptosystems***. A wildcard, i.e. a short-cut innovation, might be used for factoring large numbers using either conventional computing or some kind of quantum computers. Such a development would favour the implementation of QKD-based systems for which, contrary to asymmetrical cryptosystems, there exist theoretical security proofs.

Another non-technical driver is the need for the ***long-term security of data*** communicated today. Many organisations must rely on the confidentiality of data once transmitted over a long period of time. QKD-based systems have an advantage over conventional cryptography systems in achieving perfect forward security in the long run, which means that QKD is the only available technology where future security can be guaranteed already today.

As in the case of classical cryptography in its beginnings, one of the most important drivers of QKD in the civil sector is definitely the ***telecom industry***. One inhibitor is the ***cost of the products and infrastructure***, which exceeds that of conventional security systems by several times. Yet, for the network of a bank connecting to its sites, the cost factor might not be the most prevalent one. Thus, until QKD is widely deployed in networks of carriers, there is at least a very specialized low volume market for ***point-to-point*** QKD links for data centres and for distributed clustered computing environments. These systems are deployed by institutions like banks, ministries or various kinds of security agencies.

The commercial development of QKD can be expected to resemble the market uptake of classical cryptography. Note that the markets in question are not necessarily “free markets” since they are highly regulated in some institutional contexts. Accordingly, the first target market for classical cryptography was the ***government market***, primarily armed forces and some research organisations. Consecutive phases are indicated in Figure 1.

QKD is presently in the first phase. Experts believe that sooner or later the costs will decline. To overcome the inhibitors described, the QKD community has to convince their sceptics of the benefits of QKD and that there are specific areas of application in conventional cryptographic systems. In the commercial sector, for instance banking, most systems have yet to be protected even by conventional cryptography, so it will be even more of a challenge to convince chief executives and other professionals to take a step beyond the systems commonly available today and embrace the advantages of QKD for cryptographic key exchange.

Market actors most likely to adapt the technology	
Phase 1	Government, armed forces & research institutes, early adopters
Phase 2	Large financial institutions & foreign embassies.
Phase 3	Medium-sized financial institutions, airport control, police & gaming houses.
Phase 4	Public utilities & local council/state offices.
Phase 5	Large organisations using sophisticated databases, such as data miners and data warehouses. Companies that need to protect confidential customer information, e.g. large accountancy or law firms.

Figure 1: Market uptake of QKD

Technical Drivers and Inhibitors

One additional driver of costs is the limited ***bit rate***. The secure key bit rate today ranges between a few kilobits to one megabit per second. But not only the bit rate has to be extended to make QKD more attractive, so has the ***distance***. For most systems in operation today, 50 to 100 kilometres is about the maximum viable distance. At longer distances, random noise continuously degrades the photon stream, which at about 200 kilometres reduces the bit rate to an impractical level of a few bits of secret key per second. Here technical advances in the typical components used in QKD systems are in order to increase rate and distance in specific Metropolitan Area Network (MAN) applications to more competitive levels: efficient photon sources and detectors as well as less lossy fibres.

Another practical limitation of QKD is the fact that QKD today only works between terminals directly connected to each other. The only way to achieve a key distribution system with the highest security level typical of QKD in a networking environment and at greater distances is to add ***quantum repeaters*** to regenerate the quantum bits. This is where innovation on the technology side is needed. Such repeaters that can be considered technically absolutely secure are still under development, for instance, at Geneva University.

Compatibility with existing security system is a crucial factor for the commercial prospects of QKD products. More compatibility and thus a broader range of options for implementation could be achieved by further ***miniaturisation***. Small size and optimised functionality in optical fibre or through free space can be expected to improve market opportunities. Compatibility is key because one thing is for sure: existing markets have to be conquered that recognise QKD as a valuable add on. QKD has to be integrated as a system, not in parts or components.

User discontent could become an additional driver of QKD: end users complain that much of the software and hardware currently available from conventional cryptography is not very ***user-friendly*** and frequently not compatible with corporate IT systems. The large number of providers on the market right now also reduces profitability. Those factors could be beneficial to QKD developers and sellers because IT support personnel may show less resistance towards adopting new technologies.

Two information issues, however, need to be solved before a new technology like QKD can be adopted, for example, by large corporations. First, QKD sellers have to be aware of the ***decision making hierarchy*** in such organisations. Even if CEOs support new IT solutions, internal IT support might not simply embrace such decisions (and vice versa). The second issue is that in most organisations, even in big financial or insurance companies, there most likely will not be a cryptographer among the staff. An average size bank has an information security officer who reads information on the Internet but is not capable of judging whether QKD is secure or is even better than other key distribution systems. They follow best practices.

Use Cases

The main QKD application is the sharing of very long keys between two remote parties, where the objective is to secure confidentiality and authenticity in subsequent communications. In the near to mid-term future, specifc applications of QKD will most likely depend on at what point in the network it will come into play. In its work on increasing trust in IT networks through QKD, the ETSI ISG-QKD documents a number of use cases for future application.

Offsite Backup/Business Continuity: To assure business continuity, a company or organisation has decided to add a backup site to their network and regularly perform a remote backup of the primary site. In case of data loss at the primary site, data is recovered from the secondary site. For protection against major disaster, the secondary site can be equipped and configured to assume control and fully take over operations. As strict confidentiality of data is required, an encryption system is mandatory. In this case, a QKD link encryptor can be used: the cryptographic keys are generated and exchanged between the primary and secondary site, using a QKD link, and fed into a link encryptor, which uses a symmetrical block or steam cipher to encrypt traffic on an Ethernet or Fibre Channel link.

Enterprise Metropolitan Area Network (MAN): The enterprise or government agency requires a high level of confidentiality, integrity and authenticity of its communication system. Therefore a dedicated security system is mandatory. The single network connections between the sites are secured with QKD link encryptors. The cryptographic keys, which are continuously generated by the QKD links, are fed into link encryptors using a symmetrical block or steam cipher for transparent traffic encryption on an Ethernet or Fibre Channel link. The entire traffic

between the sites is encrypted and authenticated on the OSI (open system interconnection) data link layer.

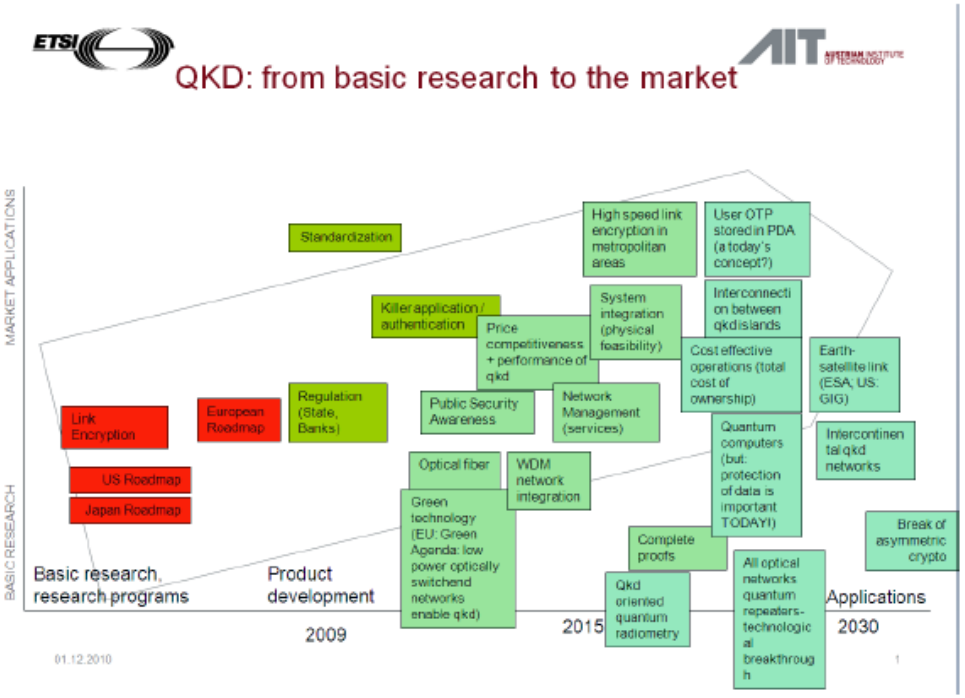
High Security Access Network: A QKD system is used to distribute cryptographic keys to end users attached to a passive optical network (PON), as they are common in fibre-to-the-home access network architectures. The same path that is usually used to relay the classical information from the terminal to the end users' units can be used to exchange quantum information, which can further be converted to a cryptographic key. QKD systems involved in this use case may consist of a highly asymmetrical setup where one central unit at the terminal serves many end units.

Long-Haul Service: A long-haul connection is established between remote sites that are served, one after the other, via a free-space QKD link by an aircraft or by a low orbiting space satellite. Different types of suitable aircraft include planes and possibly also high altitude platforms (HAPs), which are basically stationary aircraft or aircraft with limited cruising radius operating at heights of about 20 kilometres. The HAPs can supply a metropolitan area region with secret information from above, covering a potentially larger area than what can be achieved in the direct line of sight, especially in a metropolitan area.

Becoming an Indispensible Part of the Communication System

Quantum key distribution can never be more than a part of a larger system for the secure transfer of data, but as such a very important part. In the near to mid-term future, our society will have to deal with increasing security breaches and information leaks in all societal subsystems. The future vision for QKD is the implementation of quantum communication as the technology to exchange data at every level where (sensitive) information is exchanged.

The figure on the right was generated in a workshop with participants of the ETSI standardisation group ISG-QKD. The researchers were asked to identify prospective areas for developing basic research into marketable applications by 2030. They mentioned not only products and developments but also determinants of a scientific and societal nature. One such societal precondition was perceived to be an increased public awareness of security issues, another one a rising demand for green technology where QKD can contribute to energy saving. On the technical side, the provision of optical fibre and WDM network integration were mentioned for the near future. Experts see the emergence of the quantum computer and the breakthrough of asymmetric cryptography as lying further ahead, just as the overall implementation of optical network technology and quantum repeater optics.



References & Links

Giesecke, S. and Länger, T. (2011): Quantum Key Distribution: Promoters and Inhibitors of QKD. ETSI. Available for download at
https://www.isg-qkd.org/viewtopic.php?f=25&t=79&sid=546f865fffbe3e393f28a341d974d39c
http://www.etsi.org/deliver/etsi_gs/QKD/001_099/002/01.01.01_60/gs_QKD002v010101p.pdf
http://www.etsi.org/WebSite/Technologies/QKD.aspx