

NANOTECHNOLOGIES FOR SECURE COMMUNICATIONS

The spectrum of threats and types of attackers targeting information systems are growing, creating security concerns for national security, businesses, and individuals. In this environment, attention to new measures that enhance security is growing at all levels. As a result, public and private standards relevant to information protection are becoming increasingly stringent. Quantum Cryptography (QC) is one emerging security technology that offers radically new protection measures. Quantum key distribution (QKD) encryption, the most advanced recently developed method of QC aimed to distribute a secret key, can be used in conjunction with existing virtual private network service offerings for businesses needing communication services for content requiring a higher degree of confidentiality and protection. Practical realisation of QKD technology relies on availability of systems providing production, propagation and detection of individual light particles - single photons. Single photon sources based on nano-structured materials such as quantum dots, carbon nanotubes and diamond nanowires that have enabled the development, and recent demonstration, of a small number of commercial products. The working distance of existing technologies is currently limited to around 100km; significant development in fibre optics is required to make further advances here. The costs involved in developing QKD-based products also make it impractical for mainstream applications and, for now, these applications are limited to use by major financial institutions, national security and other government agencies.



The need for secure communications

Information is the lifeblood of the modern global economy. Secure storage and transmission of sensitive information has become a growing risk for both business and private communications. Businesses that are the most at risk include financial institutions, insurance companies, national security departments, corporations' intellectual property units, trading institutions, and any storage area network that may hold such information. As a result, the number of governments placing high priority on security of information systems and networks has increased since 2008. In 2010 communication security took first position on the OECD list of top ten ICT policy priorities¹. With risks now fuelled by sophisticated and organized groups, information security requires novel technologies capable of providing ultimate protection for confidential data traffic.

Cryptography is a centuries old method of communicating sensitive information between two parties in such a way that a third party is restricted from obtaining it. The most advanced form currently, Public Key Cryptography (PKC), was ushered into existence by the computer age. With this method, different keys are used for encryption and decryption. The idea is that individuals looking to receive encrypted messages send out encryption keys publicly, while keeping private keys for themselves. The secrecy of the keys relies on computational

complexity of certain mathematical problems. However, computer power and mathematics are constantly advancing. Particularly, with expectations that quantum computing will become a practical technology very soon, inventing an algorithm that could break or solve the current mathematical problem is inevitable. In addition, eavesdropping on the key is not detectable with classical cryptography. That means that users do not know if someone is tampering with their keys. On the other hand, PKC uses identical keys for encryption and decryption and technologies for frequent and reliable key distribution are needed with this type of cryptography. Quantum Cryptography (QC) is an emerging security approach that offers radically new protection measures².

Nano-enabled technologies for secure exchange of information

QKD enhances the PKC approach by making the exercise of key sharing impossible to compromise. The principle of operation of an QKD system (the most advanced method of QC for now) is quite straightforward³: two communicators (in cryptography they are usually referred as Alice and Bob) are linked together with a quantum channel and a classical channel as depicted in *Figure 1*.

Alice generates and sends a random sequence of quantum bits that are sent over the quantum

SECURITY: NANOTECHNOLOGIES FOR SECURE COMMUNICATIONS

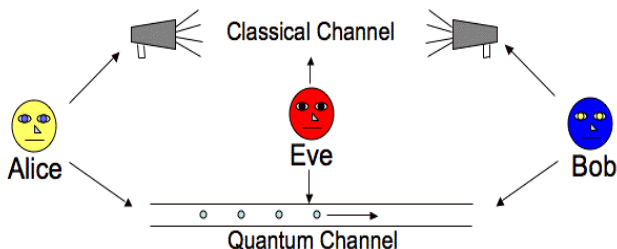


Figure 1: Diagram depicting the QKD principle.

channel. Upon reception of the data Bob contact Alice via the classical communication channel in order to check if an eavesdropper has tried to extract information from the quantum channel.

Based on quantum physics laws the presence of an eavesdropper is revealed by the imperfect correlation between the two lists of bits obtained after the transmission of quantum bits between the sender and the receiver. If the correlation is high enough, a perfectly secure key can be created from these two lists of data. Conversely, when an eavesdropper Eve has listened in on the quantum channel, the key generation process has to be aborted and started again.

To construct a practical QKD device one has to provide trustworthy generation, propagation and detection of single photons. Recent developments in nanomaterials and nanotechnology offer solutions for developing reliable systems. Fluorescent dye molecules, quantum dots (QD), carbon nanotubes, luminescent centres in diamond and diamond nanowires are among the materials currently being exploited for developing robust light sources that emits one photon at a time⁴. At present, single QD (**Figure 2**) are considered as one of the most promising materials to help creating viable solutions for quantum information processing. Their specific advantages include stability, compatibility with chip-technology, wide spectral range and high repetition rate.

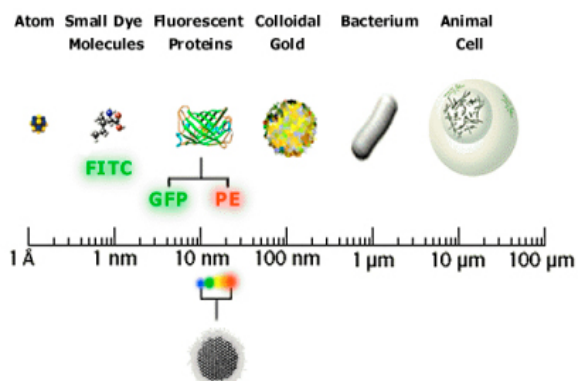


Figure 2: Size of QD relative to other objects (Source: Quantum Dot Corporation).

Impacts

Secure data transmission is a critical business need and the main driver for Quantum Key Distribution

based solutions. Extremely high levels of security are required in governmental organizations, armed forces, and national security departments, who can be classified as early adopters of QKD technology. As the market evolves and costs come down, the next groups to apply QKD technology will likely include financial institutions, foreign embassies, and online gambling companies. Anything damaging public confidence in the banking system would have serious implications. Within ten years, QKD could be applied extensively in all organizations which need to protect confidential customer information⁵. For EU citizens, the extensive implementation of QKD technology would give a peace of mind as their confidential information would be safe and secure. The competitive advantage of QKD over conventional cryptography is quite solid as it is based on the fundamental laws of quantum mechanics and if properly implemented, it guarantees absolute security for key distribution.

Commercial prospects

After Quantum Cryptography moved out of research laboratories to commercial markets, the business implications of this technology have been realized. Although some challenges still remain, Quantum Cryptography is addressing the shortcomings of conventional cryptography and rapidly developing into a large global market, reaching €583 million by 2015 according to a recent report⁶. The UK, Germany and France were mentioned to represent the most promising markets for quantum key distribution products in Europe.

Currently, commercial off-the-shelf QKD products are available from **ID Quantique** (Switzerland) and **MagiQ Technologies** (USA). QKD has reached a level of maturity such that it only takes a typical network engineer a few minutes to install a QKD system. However, all commercial products are based on optical fibre technology and are therefore limited in their technical capabilities and range. Other players in the market include Toshiba Research Europe, NEC Corporation, IBM, BBN Technologies, Mitsubishi, NTT and Bristol University. If the QKD technology leaders are small companies, it seems unlikely that financial institutions and other large organizations would trust their security to these small companies but rather to the trusted network providers that currently supply their network solutions. It can be assumed that technology producers such as ID Quantique are entering into technology relationships with network providers who have the reputation to distribute the technology further to reach customers like the aforementioned financial institutions.

Technological Challenges and Future Prospects

At present, practical implementation of basic quantum communication schemes at the lab scale

SECURITY: NANOTECHNOLOGIES FOR SECURE COMMUNICATIONS

is becoming routine. However, non-trivial technological challenges exist hampering progress in developing viable high speed systems and transmitting information for long distances required for real life applications⁷.

The issues of scale, range, reliability, speed and robustness cannot be resolved by incremental improvements of existing technologies. There is a strong need for breakthroughs in research and technology developments. In order to achieve this, both the underlying technologies for detectors, quantum memories and interfaces, and their integration for specific applications such as high rate (fibre or free space) quantum communication, quantum repeaters and satellite-based communication links must be targeted.

In the meantime, the successful achievement of these technological challenges will result in a variety of interesting complementary products such as, for example, quantum random number generators, single-photon sources, single-photon detectors and entangled photons pair sources in the visible and UV range of electromagnetic waves.

Also, current quantum cryptography techniques have an Achilles' heel - there are no reliable methods for authentication of communicators and their location - that delays opening up a new realm of ultra-secure applications for all forms of highly sensitive communications.

For many quantum communication applications it is important to operate in a larger dimension space. This can be obtained by preparing two photons entangled in more than one degree of freedom and increasing in this way the number of qubits (units of quantum information). There are too many technical challenges and fundamental limitations at the present time which limit their usage. However new protocols, based on encoding of information in several degrees of freedom were recently suggested⁸. These multi-parametric protocols allow in principle to reach maximal critical error of 50% and allow relatively simple implementations with current fibre based technologies.

EU Competitive Position

Europe has put considerable effort into research in the field of quantum information processing that resulted in developing a strong scientific background. The support at European level has been provided mainly by funding R&D activities in the quantum information processing field through three European Framework Programmes FP5 (total funding €31M in 1998-2002), FP6 (€25M in 2002-2006) and FP7 (ca. €30M from 2007 to current)⁹. Also, the IST Research Program had funded SECOQC project on "Development of a Global Net-

work for Secure Communication based on Quantum Cryptography" with €11.35M grant in FP6. The consortium of 40 top research groups in the field of applied quantum cryptography developed an open network for dependable and secure long-range quantum communication built upon the QKD technology. The functionality of the developed architecture has been successfully demonstrated in 2008. In addition the consortium published a White Paper¹⁰ on QKD and QC and started activities on standardisation of the developed technology.

Future competitiveness of the EU requires a significant effort both on the European and national level. The structure of the funding must account for the interdisciplinary character of the field. Therefore it must support a spectrum of activities across different disciplines from experimental to theoretical physics, computer sciences and mathematics. Links with industry must be developed, both on the level of possible commercial exploitation, and through joint research programs making new technologies available outside the capabilities and know-how of traditional basic-research oriented laboratories. In particular, links with micro- and nano-fabrication facilities and related technology centres must be strengthened, and spinning off new quantum technologies like quantum sensors and high precision measurement devices ought to be encouraged.

In **Figure 3** the 2008 funding figures in the quantum information processing area are shown for the US, Canada, Japan and Europe. Despite recent new initiatives (e.g. Chist-ERA¹¹) the current level of R&D support puts Europe below average in terms of worldwide funding support in the field of quantum information. With such a potential decrease in international competitiveness, there is considerable risk that European research in quantum information processing and the resulting technology developments will not be sustainable, leaving Europe reliant on importing such developed QC technologies from abroad⁷.

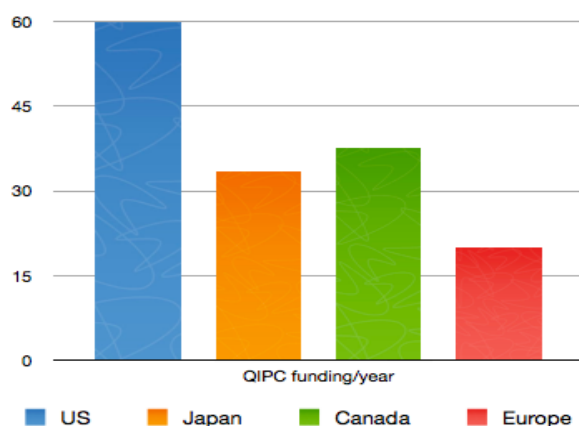


Figure 3: R&D Funding (in M€) in quantum information processing in 2008 (Source: QUIE2T report⁷).

SECURITY: NANOTECHNOLOGIES FOR SECURE COMMUNICATIONS

Challenges

Environment, Health & Safety Aspects

EHS aspects of nanotechnology-based applications for secure communications have been considered by ObservatoryNANO within the EHS review of the Security sector¹². Candidate nanomaterials for QC technology developments (such as quantum dots, carbon nanotubes or nanowires) will be included as substrate-bound materials, used in small amounts and be fully confined into the final products. Since nanomaterial release from these applications and potential exposure is very unlikely, those technologies are not expected to raise any specific risk for humans or the environment.

Ethical and Societal Aspects

Quantum cryptography raises both the traditional ethical questions of information technology and new specific issues related to cryptographic applications. Traditional questions include data privacy, personal autonomy and intellectual property rights. ObservatoryNANO published a review of these issues and current European norms and initiatives in the Annual Report on Ethical and Societal Aspects of Nanotechnology Enabled ICT and Security Technologies¹³. Specific questions relate to the marketing strategies of quantum cryptographic application. In the light of RSA security breach of SecureID technology in April 2011, quantum cryptography counts among the very few still secure alternatives. With the accrued attention to QC solutions, the theory-based promise of “100% security” needs to be critically and independently reviewed for the existing QC applications.

Summary

- Secure storage and transmission of sensitive information has become a growing risk for both business and private communications.
- Quantum Cryptography is an emerging security approach that may offer radically new protection measures for processing information. The competitive advantage of QKD over conventional cryptography is quite solid as it is based on the fundamental laws of quantum mechanics. However, the theory-based promise of “100% security” needs to be critically and independently reviewed for the existing QC applications.
- Europe has put a considerable effort into research in the field of quantum information processing that has resulted in the development of a strong scientific background and several commercial products.
- Nevertheless, with current levels of EU R&D funding below average in terms of worldwide funding support in the field of quantum informa-

tion processing, there is a considerable risk that European research, and the resulting commercial and defence technology developments, will not be sustainable.

- Future competitiveness of the EU requires a significant effort both on the European and national levels. The structure of the funding must account for the interdisciplinary character of the field.
- Governmental organizations, banks, armed forces, and national security departments are early adopters of QKD technology. As the market evolves and costs come down, the next group to apply QKD technology would be financial institutions, foreign embassies and online gambling companies.

Contact Information

Technical: Dr Sergey Gordeyev, Institute of Nanotechnology, sergey.gordeyev@nano.org.uk

Economic: Tom Crawley, Spinverse, tom.crawley@spinverse.com

References

- ¹ OECD (2010), *OECD Information Technology Outlook 2010*, OECD Publishing. http://dx.doi.org/10.1787/it_outlook-2010-en
- ² Quantum Cryptography and Secret-Key Distillation, Gilles Van Assche, Cambridge University Press, 2006.
- ³ Gisin, N., G. Ribordy, W. Tittel, and H. Zbinden. 2002. Quantum cryptography. *Review of Modern Physics* 74(1): 145-195 (<http://arxiv.org/abs/quant-ph/0101098>)
- ⁴ Beveratos, A. et al. Single photon quantum cryptography. *Phys. Rev. Lett.* 89, 187901 (2002).
- ⁵ Commercial Prospects for Quantum Information Processing, <http://www.qipirc.org/uploads/file/Commercial%20Prospects%20for%20QIP%20v1.pdf>
- ⁶ PRWeb news, <http://www.prweb.com/releases/quantum/cryptography/prweb2483574.htm>
- ⁷ Quantum Information Processing and Communication: Strategic report on current status, visions and goals for research in Europe, <http://qurope.eu>
- ⁸ On practical implementations of qudit-based quantum key distribution protocols. S. S. Straupe, S. P. Kulik, in *Quantum Cryptography and Computing*, Vol. 26, IOS Press, 2010. pp.83–98.
- ⁹ FP6 funded projects: SCALA, QAP, EuroSQIP; FP7 funded projects: AQUITE (5.3 M€), Q-ESSENCE (4.7 M€), SOLID(5.0 M€), COMPAS - (2.1 M€), COQUIT - (1.5 M€); CORNER - (2.7 M€); GEOMDISS - (2.1 M€); HIDEAS - (4.6 M€); HIP - (2.8 M€); MIDAS - (3.1 M€).
- ¹⁰ Development of a Global Network for Secure Communication based on Quantum Cryptography, <http://www.secoqc.net>
- ¹¹ European Coordinated Research on Long term Challenges in Information and Communication Sciences & Technologies E R A - N e t , <http://www.chistera.eu/call-2010>
- ¹² Marie-Claire Toufeksian, ObservatoryNano report on EHS Impacts. Technology Sector Evaluation: Security, 2010, <http://www.observatorynano.eu>
- ¹³ <http://www.observatorynano.eu/project/filesystem/files/Nanoelectronics%20ICT%20securityreportfinal.pdf>