On QKD Industrialization

J. Dávila, D. Lancho, J. Martinez, and V. Martin

Facultad de Informática, Univ. Politécnica de Madrid
Campus de Montegancedo, Boadilla del Monte
Madrid 28660, Spain
Vicente@fi.upm.es

Abstract. During the 25 years of existence of the first protocol for Quantum Key Distribution, much has been said and expected of what came to be termed as Quantum Cryptography. After all this time, much progress has been done but also the reality check and analysis that naturally comes with maturity is underway. A new panorama is emerging, and the way in which the challenges imposed by market requirements are tackled will determine the fate of Quantum Cryptography. The present paper attempts to frame a reasonable view on the issues of the security and market requirements that QKD should achieve to become a marketable technology.

Keywords: Quantum Key Distribution, Security assurance and standardization, Market requirements.

1 Introduction

Setting aside the historical paper of Wiesner about quantum money, the birth of Quantum Cryptography could be associated with the BB84 protocol, actually in 1983. Although Quantum Cryptography is a broader field, it was the Quantum Key Distribution (QKD) schemes, initiated by this protocol, which shaped the field as we know it today. At present, it is only QKD to which a reasonable degree of technological maturity and market relevance can be ascribed. QKD protocols serve the purpose of growing a preshared secret among two parties. The preshared secret serves to guarantee the integrity of the protocol in the first transaction, while the quantum properties of nature are used to guarantee, with any threshold we would like to pose, the privacy of the generated key. In the QKD implementation proposals to date, part of this new generated key is used to check the integrity of the next protocol round, a practice that should be carefully reconsidered from a practical perspective. From a security standpoint, integrity control and key generation are two basically different processes, hence they should be kept separated [2]. Concepts of separation and controlled information flow are a well acknowledged practice [3] that has made its way in modern high security architectures as exemplified by MILS (Multiple Independent Levels of Security/Safety [4]) and that could have prevented or, at least, alleviated the possible impact of recently discovered weaknesses in QKD [5]. Simple integrity

A. Sergienko, S. Pascazio, and P. Villoresi (Eds.): QuantumCom 2009, LNICST 36, pp. 297–302, 2010.

control techniques well regarded in practice, like seeding a pseudo random number generator with an initially shared secret, are robust and demand only a small secret to run for a long time. A simple XOR among the strings obtained by this method and the quantum key used for the same purpose would provide the best of both worlds.

Key management is the provisions made in a cryptography system design that are related to generation, exchange, storage, safeguarding, use, vetting, and replacement of keys. It includes cryptographic protocol design, key servers, user procedures, and other relevant protocols. Key management is essential for any security infrastructure and QKD can be certainly a very powerful primitive to strength many operations relevant to the security market. However, while QKD protocols can be proven theoretically secure under simple assumptions, these are not, and cannot be, backed by implementation under any known industrial process. The widely spread view that QKD could achieve perfect secrecy in real applications is clearly flawed, certainly from the point of view of the conventional cryptography community, as opposed to the quantum cryptography one, where many were pushing absolute security as the spear head of the new field. The history of cryptography is full of examples of good ideas that have claimed to offer higher levels of security, and then reality has put them in the curiosities corner [6]. These excessively triumphant views, together with the fact that shared secrets are a relatively small part of the whole security market and can be achieved by other means [7], led also to the early dismissal of QKD by many security practitioners. At most, it was relegated to an immature technology status that could be relevant to some niche markets in the future.

As QKD technology advanced and made its way out of the laboratory and began to be marketed and tested in competition with more traditional technologies, issues about its actual security level, market relevance, reliability, cost/benefit, etc. started to arise.

The first fact to realize in this commercial environment is that in general, and in one component in particular, absolute security is not really an interesting goal to pursue in itself. Security is a general property of the system that is build up over many components and strengthening one of them does not necessary makes the full system more secure. Application always dictates the security level requirements but usability, reliability, interoperability and cost are many times as relevant as security needs. Some are started to be addressed by the QKD community using rules akin to those applied to conventional systems. Certification is a case in point. To build trust on the final user, similar methods to those that have already proven its validity must be used. Intensive and detailed independent evaluation, strict quality control, good acceptance by the insurance companies and adequate information campaigns help to market a security product, but these do not cover all the bases. To base QKD devices certification on well known standards like FIPS 140, Common Criteria [8,9], etc. as is being done in the current work at the Quantum Industry Specification Group of the European Telecommunications Standards Institute [10,11] is a reasonable and necessary move, maybe the only one possible. These certifications are routinely applied to all kinds of electronic devices and their application to the corresponding part in QKD devices should be straightforward. Its use concerning the optical subsystem is an unexplored field in need of being addressed.

QKD modules will include microcontrollers, electronic memories, buses and many other elements common to the general microelectronics market. QKD modules cannot be safer than the software that runs inside them and controls all their functionalities. Everything in the software that can be reprogrammed, updated or maintained in any way inside a QKD module has to be specially protected because its integrity must be guaranteed all along the module service. Using general purpose hardware and software components (microprocessors, memories, operating systems, drivers,...) has many advantages, in particular those related to the final cost and maintenance, but can also introduce security breaches in the system.

QKD modules require specific purpose software that implements the protocols, controls the optoelectronic hardware and is responsible for the administrative and operational interfaces. If we accept the software security as an upper security bound in a QKD system, as it is with all embedded systems, then the software has to be secure by design and has to be evaluated, inspected and certified at a high level of security if we want to see the QKD technology in the high security market shelves.

Definitively, security and risk always go together; consequently, security has to be as multi-valuated as the risk is in real scenarios. In many infrastructures, different security levels are defined, and the products used inside them have to match the security level specified. Because of this, different certification levels could be adapted to different applications. QKD technology can provide different security levels at different costs using different technologies and settings. This flexibility must be made available in real QKD systems to exploit its commercial horizon because it could match many different scenarios. In principle, Common Criteria methodology profiles will help to discover and add some flexibility to QKD so as to meet the different demands of those various potential markets.

However, certification is not the security holy grail, and one must bear in mind that, for example, Common Criteria higher levels do not necessarily equate with higher security, but claims have been more thoroughly evaluated. For instance, Windows XP operating system is EAL4+ certified [12,13], despite the continuous patches needed due to the almost daily discovery of security failures. The sets of claims for QKD must be carefully crafted to be meaningful for the intended market. Certification, however, fulfills an important role for QKD since it translates QKD jargon and claims to the language used by its potential customers.

Usability and interoperability are also requirements that could prove essential for the QKD success. QKD must offer a set of characteristics compelling enough to be the technique of choice. For an extremely secure application with only a point to point link, usability and interoperability could be of secondary interest compared to the increase in security; however, for a company seeking to introduce QKD in an already deployed platform, these two could prove as essential as the perceived security increase.

QKD devices generate keys to be used outside the QKD device itself and, because of that, interoperability with other security systems is absolutely necessary. For example, in a high security environment, the QKD link would generate the same key at both ends on the quantum link but, probably, the key will be fed into an Electronic Key Management System (EKMS) or fill device [1] that will distribute it for its final use. In such case, QKD equipment has to be fully compatible with all key management systems it pretends to connect to and operate with.

Interoperability would be also of primary interest in the case of a network provider selling QKD services to its clients. For a customer, interoperability is a must. It allows for various QKD providers, meaning more market competition and thus lower price. It also means not to be locked with just one manufacturer. In fact, advanced security models advocate for increasing modularity to allow a better security scrutiny but this also means lower maintenance risks and costs if you have different providers for each module. QKD systems have to be interoperable with all the systems they will work with, and they also require full interoperability, standardization and security certification of all its internal modules and components (optic fibers, laser, diodes, phase shifters, delay lines, etc.).

Reliability comes hand in hand with low maintenance. One of the advantages of QKD is the possibility of low maintenance costs if the system is reliable. When using standard devices, a master key is needed to operate the system. At a given moment in time, there is no more entropy in the system than that originally in the master key. Hence, the need to balance the security level with the frequency of master key update. The procedures to change the master key in high security systems are rather involved and an acknowledged weakness. In a reliable QKD system, this weakness is confined to just the first installation. After a correct install, the system can work unattended as long as the device does not fail or the channel is interrupted. The system can even raise an alarm in case of attack, an example of an advantage of a QKD system over a conventional one. Potential low maintenance in QKD systems illustrates also how different the new markets for QKD can be from those expected at first sight. In fact, the use most commonly cited: as an extremely safe device producing keys to be used in a Vernam-Mauborgne cypher, would probably be one of the least used. Cyphering large amounts of data through a high speed link with a symmetric block cypher like AES would be much more likely. Even for a high speed channel, changing the key a few times per hour would suffice to keep a much higher security level than the attained nowadays. Hence, a low key generation rate but in a much more reliable and interoperable system would be the preferred choice, as opposed to the ever higher key generation rate philosophy pursued above all in current developments. High key rate would be useful in a scenario in which just one QKD link is used to feed keys to many data channels. On the contrary, low key rate systems able to withstand high optical losses would be much more suited for

[1] A fill device is an electronic module used to load cryptographic keys into electronic encryption machines. Fill devices are usually hand held and battery operated.

network integration in standard networks, the preferred scenario for a network operator.

Cost comes also with reliability, as it is also a product of physical integration in robust and compact devices. When considering the maximum cost of any security device, the first thing to mind is that investments in a security system should never cost more than the assets that is trying to protect. Then, the reliability and maintenance of the system have to be included.

When we compare the relative cost of a conventional device to a QKD system, several things must be taken into account. In conventional electronic security devices or systems, main budget expenses go to pay high quality design, manufacture, inspection, quality control and secure delivery. QKD systems will add to those charges the specific expenses related to its optical and optoelectronic subsystems. This is an additional cost because QKD modules also include electronic subsystems that are equivalent to those used in actual conventional security devices. At this respect, QKD systems have in their optical and quantum subsystems an additional handicap compared with the conventional devices in use for key generation and key distribution.

In general, we can conclude that other issues are more or equally important than extremely high security levels, and new QKD developments should take this into account.

In order to see a QKD industry pleasantly installed in the telecommunications market, many issues are to be addressed. Some of them are already being worked out, whereas others will take more time. Once all will be solved, there is certainly a range of applications in which QKD will fit nicely. Whether its use will be widespread or not, it will depend as much on technological advances with wisely chosen development targets as on a correct market approach.

Acknowledgment

This work was supported by CDTI, Ministry of Trade and Industry of Spain under project Segur@, CENIT-2007 2004 and UPM 178/Q06 1005-127.

References

1. Bennett, C.H., Brassard, G.: Quantum Cryptography: Public Key Distribution and Coin Tossing. In: Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore, India, December 1984, pp. 175–179 (1984)
2. Barker, E., Barker, W., Burr, W., Polk, W., Smid, M.: Recommendation for Key Management Part 1: General. NIST Special Publication 800-57 (March 2007), http://csrc.nist.gov/groups/ST/toolkit/documents/SP800-57Part1_3-8-07.pdf
3. Rushby, J.: Design and Verification of Secure Systems. In: Proc. 8th ACM Symposium on Operating System Principles, pp. 12–21 (1981)
4. Alves-Foss, J., Harrison, W.S., Oman, P., Taylor, C.: The MILS (Multiple Independent Levels of Security/Safety) Architecture for High Assurance Embedded Systems. International Journal of Embedded Systems (2007) (in press)

5. Cederloff, J., Larsson, J.: Security Aspects of the Authentication Used in Quantum Cryptography. IEEE Transactions on Information Theory 54, 1735 (2008)
6. Knudsen, L., Rijmen, V.: Two Rights Sometimes Make a Wrong. In: Proceedings of SAC 1997, Fourth Annual Workshop on Selected Areas in Cryptography, School of Computer Science, Carleton University, pp. 213–223 (1997)
7. Menezes, A.J., van Oorschot, P.C., Vanstone, S.A.: Handbook of Applied Cryptography. CRC Press, Boca Raton (2001)
8. FIPS PUB 140-2, Security Requirements For Cryptographic Modules. Federal Information Processing Standards Publication (2001)
9. ISO/IEC 15408, Common Criteria for Information Technology Security Evaluation and annex Common Methodology for Information Technology Security Evaluation, the technical basis for the international agreement known as Common Criteria Recognition Agreement
10. European Telecommunications Standards Institute, Quantum Industry Specification Group. *portal.etsi.org*
11. Länger, T., Lenhart, G.: Standardization of quantum key distribution and the ETSI standardization initiative ISG-QKD. New J. Phys. 11, 055051 (2009)
12. Woodie, A.: Windows Server 2003 Earns EAL 4 Certification from U.S. Government. The Windows Observer, January 11 (2006), `http://www.itjungle.com/two/two011106-story05.html`
13. `http://www.commoncriteriaportal.org/files/epfiles/20080303_st_vid10184-vr.pdf`