New Journal of Physics
The open-access journal for physics

Standardization of quantum key distribution and the ETSI standardization initiative ISG-QKD

Thomas Länger[1] **and Gaby Lenhart**[2]

[1] Austrian Research Centers — ARC GmbH, Donau-City-Strasse 1, 1220 Vienna, Austria
[2] ETSI — European Telecommunications Standards Institute, 650, route des Lucioles 06921 Sophia-Antipolis Cedex, France
E-mail: thomas.laenger@arcs.ac.at and gaby.lenhart@etsi.org

New Journal of Physics **11** (2009) 055051 (16pp)
Received 26 January 2009
Published 27 May 2009
Online at http://www.njp.org/
doi:10.1088/1367-2630/11/5/055051

Abstract. In recent years, quantum key distribution (QKD) has been the object of intensive research activities and of rapid progress, and it is now developing into a competitive industry with commercial products. Once QKD systems are transferred from the controlled environment of physical laboratories into a real-world environment for practical use, a number of practical security, compatibility and connectivity issues need to be resolved. In particular, comprehensive security evaluation and watertight security proofs need to be addressed to increase trust in QKD. System interoperability with existing infrastructures and applications as well as conformance with specific user requirements have to be assured. Finding common solutions to these problems involving all actors can provide an advantage for the commercialization of QKD as well as for further technological development. The ETSI industry specification group for QKD (ISG-QKD) offers a forum for creating such universally accepted standards and will promote significant leverage effects on coordination, cooperation and convergence in research, technical development and business application of QKD.

Contents

1. Introduction

Since the first practical demonstration of quantum key distribution (QKD) over a distance of a few centimeters performed by Bennett *et al* (1992), research and experimental technology have experienced ample progress, so that significantly increased key rates and distances can be achieved with contemporary systems. Today, QKD is no longer confined to large optical tables in laboratories; systems are available for standard 19" racks, capable of automated continuous operation using readily available standard telecom fibers. In the SECOQC project of the 6th Framework Programme of the European Community (www.secoqc.net) six technologically different systems were operated under realistic assumptions in a QKD network in Vienna in autumn 2008 (Poppe 2008), feeding user level applications with cryptographic keys. Commercial products for point-to-point QKD are today available from at least three small start-up enterprises (id Quantique SA, Carouge Geneva, SmartQuantum Group SA, Lannion-Paris-Houston, MagiQ Technologies Inc., New York, NY) serving a market which is still primarily confined to businesses and research institutions buying the products for experimental evaluation.

Yet, although QKD systems today appear mature compared to the first experimental realizations, major technical improvements are required and to be expected; and additional requirements are imposed on these systems specifically when deployment in a commercial environment is considered.

For integration into existing information and communication technology (ICT) infrastructures, QKD systems need to be compatible with existing interfaces for handling cryptographic keys. They need to be compatible with the way systems and services are managed within ICT infrastructures. Also, prospective operators of QKD systems will have specific functional requirements that are only weakly related to the basic QKD technology. Applications within the banking sector will require system audit capabilities and defined quality of service. Most notably, qualified practical use of QKD requires that QKD systems are trusted by its users, which is usually achieved in a complex assurance procedure including security specification, evaluation and certification according to a standardized methodology like the ISO/EN 15408 Common Criteria standard[3]. Common Criteria evaluation results are recognized in 26 leading industrial countries worldwide. Especially required for the security certification of QKD systems is a framework for the underlying information theoretical security proofs, which again requires standardized properties of optical components, like photon sources and detectors. The business requirements, as well as the necessary technological development and original scientific research, shall be addressed in the ETSI industry specification group for QKD (ISG-QKD).

This paper has two main parts. In the first part (sections 2 and 3) we present the fundamentals of QKD and a classification of QKD as cryptographic key distribution primitive. We analyze key distribution primitives in general, as well as common encryption and authentication primitives regarding their foundation of security and determine which primitives can reasonably be combined for communication systems with highest security.

In the second part (sections 4, 5 and 6) we give an introduction to standardization of security techniques in general, and to the ISG mechanism of the ETSI in particular. We analyze the relevance of QKD standardization in the ICT work programme of the EU and mention when the ISG-QKD exactly started and which parties are currently participating. Section 6 lists the work items (WIs) of the ETSI ISG-QKD that have already been started or are scheduled to start in the near future.

2. QKD fundamentals

Quantum information theory is a relatively new scientific research discipline located at the intersection of quantum physics and information theory, two of the most notable scientific achievements of the 20th century. Quantum cryptography, or more precisely QKD, a new method for generating and distributing symmetrical cryptographic keys with information theoretical security, is based on quantum information theory. For an account of the historical development and a detailed technical description of QKD, see Gisin *et al* (2002), Dusek *et al* (2006) and the documents referenced therein.

[3] Common Criteria Part 1 *Introduction and general model (2006)*, Common Criteria Part 2 *Security functional requirements (2006)*, Common Criteria Part 3 *Security assurance requirements* (2007), Version 3.1, available at http://www.commoncriteriaportal.org (accessed 1 January 2009).

Information theoretically secure key distribution refers to the fact that the information, which an eavesdropper may have on the key, is always below an upper bound that can be made arbitrarily small. As such, QKD belongs to the class of information theoretically secure key distribution techniques that rely on a noisy channel as additional resource. For QKD this resource is the quantum channel. For a survey of these methods see Christandl *et al* (2007).

The power of QKD stems from the fact that it allows two parties to establish a secret key from a short pre-shared secret and a public exchange without any assumptions on the attack capabilities of an eavesdropper[4] or assumptions on the hardness of certain algebraic problems—something that was never shown to be possible with classical means.

QKD is the first marketable application exploiting quantum information and although there are still significant technical problems pending, it has great potential to obtain a fixed place among the technologies for securing communication confidentiality and privacy in the future information society and thus to become a driver for the success of a series of services in the fields of tomorrow's information society.

3. Classification of QKD as cryptographic primitive

QKD can be seen as atomic cryptographic primitive and as such it covers only one part of the cryptographic functionality, which is necessary to build a secure communication system (Menezes *et al* 1997, Schneier 1996). The common notion 'quantum cryptography' for QKD is unfortunately misleading and it shall be clearly noted that QKD is not a replacement for 'classical cryptography' as was claimed on multiple occasions in early publications on the subject. However, the primary keyword for publications in the field of QKD remains 'quantum cryptography' and for reasons of continuity there seems to be no practical way to change this in the future. Contrasting 'classical' and 'quantum' cryptography as a marketing instrument was also used to support the visibility of QKD as a technology and help generate the necessary interest and funding to develop the technology to the state of maturity it has today. On the other hand, these exaggerated claims have led to almost universal disregard of QKD in the cryptographic community preventing an unbiased evaluation of the possibilities that open up for security systems with QKD.

In the following the minimal set of cryptographic primitives for a secure communication system shall be evaluated with respect to the level of security that can be achieved. In order to secure the integrity and confidentiality of a message, as well as the authenticity of its origin, an encryption primitive and an authentication primitive must be combined with a key distribution primitive. As the overall security of a security system is at maximum as strong as its weakest link, or even weaker (Neumann 2003), encryption, authentication and key distribution primitives with a comparable level of security shall be identified (for a thorough discussion of cryptographic primitives and their relation to QKD see also Alléaume *et al* (2006) and Stebila *et al* (2009).

3.1. Encryption primitives

Encryption has been used from ancient times to protect the confidentiality of messages while they are transmitted. Today many kinds of ICT applications use a variety of encryption methods

[4] Here we refer to the security in the so-called 'uncalibrated device scenario' (Scarani *et al* 2009). It should however be noted that a number of practical implementations resort to the weaker 'calibrated device scenario'. This issue will be specifically addressed in the ISG-QKD work item 'Security Proofs' — see 6.8.

and algorithms for this goal. These include symmetric block and stream ciphers, where sender and receiver share two (identical or trivially related) keys and asymmetric key algorithms, where two keys are related in such a way that the private decryption key cannot easily be derived from the public encryption key. Examples for symmetric key algorithms are the Data Encryption Standard (DES), and its variant Triple DES, and the currently popular Advanced Encryption Standard (AES). Examples of contemporary asymmetric key algorithms are the Rivest, Shamir, and Adleman algorithm (RSA, Rivest *et al* 1978) and the family of elliptic curve algorithms.

These symmetric and asymmetric algorithms have in common that the security for maintaining the confidentiality of the encrypted message is computational, i.e. it is based on the assumption that an attacker is constrained in available computing power for the attack or the available time for carrying it out. For asymmetric cryptography the security additionally depends on the assumption that no efficient algebraic method exists to reverse the utilized cryptographic functions. These assumptions require constant attention (see the web site for cryptographic key length recommendations http://www.keylength.com) and have in some cases required costly migration to another algorithm when their security was challenged e.g. because of the rapid increase in computing power.

However, one symmetric cryptographic algorithm is different: the one time pad. If properly employed, it is the one and only information theoretically secure encryption method. Information theoretically secure refers to the fact that it can be formally proved that the amount of information an eavesdropper may have about the message is below an upper bound, which can be made arbitrarily small. The one time pad was invented in the early 1920s based on work of Gilbert Vernam and Joseph O Mauborgne and it took almost 30 years until its 'perfect secrecy' could be proved by Claude Shannon in 1949 (Shannon 1949). For applications with highest security requirements the one time pad is still in use today, despite its impractical prerequisites: it requires a truly random key with exactly the same length as the message to be encrypted.

3.2. Key distribution primitives

The generation of two identical streams of truly random bits at two distinct locations connected by a quantum channel is exactly what QKD can provide. As mentioned before, this can be achieved with information theoretically guaranteed security.

Other methods for distributing secret keys either make use of a given secure channel or rely on public key cryptography. Examples of a given secure channel are the trusted courier who carries a USB flash drive filled with a random bit sequence, or a digital channel that is secured with a previously distributed secret key. In the latter case the security level for the distribution process, and hence the security level of the subsequent encryption, is certainly lower than the security level of the secure channel.

An example of a key distribution method using public key cryptography is the Diffie–Hellmann key agreement (Diffie and Hellman 1976), which is e.g. used in the Secure Sockets Layer protocol (SSL/https) or in the Internet Key Exchange (IKE) protocol for setting up security associations in the IPSec protocol. In contrast to QKD, the security of both the secure channel and the public key agreement is again based on assumptions. The advantage of public key distribution lies in its ability to establish a secret key between two parties without prior mutual knowledge. But it is also clear that without prior mutual knowledge the identities of the parties cannot be authenticated and a man-in-the-middle attack cannot be ruled out. The

authentication of the communicating parties is usually solved with a public key infrastructure involving a trusted third party.

QKD, too, requires authentication of the parties to rule out man-in-the-middle attacks. The origin of the quantum channel and that of the classical channel that is used during the key distillation process following the quantum exchange are both authenticated when a common quantum error rate is computed. This is done by public discussion on the classical channel that uses a message authentication primitive to guarantee message integrity.

3.3. Message authentication primitives

For a secret communication system, message authentication, which means ensuring message integrity (i.e. that a message was not altered during transmission) and the identity of the sender are common goals. The QKD primitive itself requires message authentication for the messages its two peers exchange for the key distillation protocol.

Again, this goal can be accomplished using various technologies. A common approach is to apply digital signatures (Diffie and Hellman 1976) by condensing a given message to a block of data with fixed size using a cryptographic hash function and subsequently signing it using a private key. The receiver can apply the corresponding public key and is thus able to verify not only the integrity of the message, but also the authenticity of its origin. Another method for message authentication is using conventional message authentication code (MAC) algorithms. MAC algorithms can be constructed using a block cipher or be derived from cryptographic hash functions. They use the same key for computing and verifying the MAC value and require prior distribution of symmetrical keys.

The security of both digital signatures and MAC algorithms depends on computational assumptions and there has always been progress in developing new cryptanalytic attacks leading to significantly reduced effort for brute force attacks, as was the case for the widely used MD5 and RIPEMD in 2004 (Wang and Yu 2005) or SHA-1 in 2005 (Wang *et al* 2005).

Provably secure authentication can be achieved with hash functions, which are selected from a class of universal-2 hash functions according to a secret both parties share. This system was initially proposed by Wegman and Carter (1981).

In QKD, a small fraction of the continuously generated key can be used for information theoretically secure message authentication, but when a link is taken into operation, a pre-distributed initial secret is necessary to authenticate the public channel before the first quantum keys become available. This is comparable to digital signature schemes, where the public key (mostly in the form of an identity certificate) of the sender, or the public key of a trusted third party, when transitive trust relations are applied, must be pre-distributed (e.g. with a web browser). The necessity of a pre-distributed secret constitutes no principal disadvantage of information theoretically secure authentication schemes, as opposed to signature-based or MAC-based authentication systems, as is claimed e.g. in Paterson *et al* (2005).

3.4. Synopsis

The following table 1 lists the encryption, key distribution and message authentication primitives discussed above together with the principle on which their security is based on.

It is evident that QKD is ideally combined with one-time pad encryption and universal-2 hashing to form a secret and authentic communication system with an

Table 1. Security foundation of cryptographic primitives.

	Security based on
Encryption	
Symmetrical block or stream cipher (key shorter than message)	Assumption
Public key cryptography	Assumption
One time pad	Information theory
Key distribution	
Secure channel	Assumption
Public key cryptography	Assumption
QKD	(Quantum) information theory
Message authentication	
Public key cryptography	Assumption
MAC	Assumption
Universal-2 hash functions	Information theory

unprecedented level of theoretical security. The mere combination of QKD with universal-2 hashing for highly secure authentic and public communication systems is also imaginable. Example use cases of such systems are presented in the SECOQC Business White Paper (Ghernaouti-Hélie *et al* 2008).

The combination of the three listed information theoretically secure cryptographic building blocks in a network for highly secure communication was also one of the major achievements of the SECOQC project of the 6th Framework Programme of the European Community. The SECOQC network combines QKD with an efficient implementation of universal-2 hashing authentication (Shoup 1996) and, alternatively, one-time pad or AES with frequent key change for payload encryption.

4. Standardization of security techniques

Until the 1960s, cryptography was mostly used in the military and diplomatic corps. Almost without exception research results were classified and not published and therefore the need for standardization did not exist. It was only later when computer systems and computer networks were increasingly used in commercial applications outside the military that standardization of cryptographic techniques became an issue. This began in the early 1970s when the first packet switched data networks (like the X.25 network) were operated by telecom companies and banks. Today cryptographic standards have become an issue more than ever for the huge number of commercial and e-society applications of the Internet. The goal of standardizing cryptographic techniques was, and still is, to increase the security of applications, to advance technical development and to enable market growth through increased interoperability and competition.

Standards and specifications are published by recognized ICT standards bodies, such as ISO (International Organization for Standardization), IEC (International Electrotechnical Commission), IEEE (Institute of Electrical and Electronics Engineers), OMG (Object Management Group), operating worldwide; ISA (Instrument Society of America) and NIST (National Institute of Standards and Technology) in the United States and ETSI (European

Telecommunications Standards Institute), CEN (Comité Européen de Normalisation—European Committee for Standardization) and CENELEC (Comité Européen de Normalisation Electrotechnique—European Committee for Electrotechnical Standardization) in Europe. The standards give clear rules on how to properly use encryption methods and algorithms under certain conditions and in well-defined environments, thus promoting a high level of security on the different levels of ICT models under various circumstances.

In the USA, the Secretary of Commerce approves standards and guidelines that are developed by NIST for computer systems of government agencies. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS)[5].

ETSI's Security Algorithms Group of Experts (SAGE) provides cryptographic algorithms and protocols specific to fraud prevention, unauthorized access to public and private telecommunications networks and user data privacy. SAGE provides a service to all ETSI technical committees and organizations with whom ETSI has a formal relationship with e.g. other European standards bodies.

These are only two examples for standardization of security techniques. A comprehensive overview of standardization organizations, levels of standardization, evaluation criteria and codes of practice is given in Preneel (1991) and Affenzeller (2007).

5. The ETSI ISG-QKD

5.1. The ETSI ISG instrument

During the past couple of years, telecommunication has more and more developed towards ICT and so has the European Telecommunications Standards Institute. Currently, ETSI has more than 700 member companies, universities and research institutes. They all contribute to the standards development by direct participation. Their work is based on consensus; the standards are open and freely available on the Internet.

All ETSI members must adhere to the ETSI intellectual property rights policy, which encourages the use of IPR, and prescribes to all ETSI members that in case essential IPR is granted, it has to be granted to all ETSI members under fair, reasonable and non-discriminatory conditions.

In order to meet the very particular needs of the ICT business, i.e. rapid research and development in parallel with standardization, ETSI has created the concept of ISG. It needs a minimum of four ETSI members to found an ISG. Once the terms of reference are agreed and the ISG agreement is signed, the ISG can immediately start working.

An ISG is open to all ETSI members and non-members, who are willing to sign a specific ISG agreement bounding them to strict confidentiality regarding all kinds of draft work towards any organization outside the ISG as well as to the ETSI intellectual property rights rules.

ETSI provides the platform on which the actual technical work of standardization can be done. This means that ETSI provides all the necessary administration, such as meeting infrastructure and logistics, communication access, document handling on an internet portal, e-mail lists and publication of deliverables. The documents provided by an ISG are open standards called group specifications (GS) and freely downloadable from the download area on the ETSI portal http://www.etsi.org.

[5] *Federal Information Processing Standards Publications, FIPS Home Page*. Available at http://www.itl.nist.gov/fipspubs/ (accessed 1 January 2009).

5.2. Relevance of QKD and standardization in the ICT Work Programme of the EC

The 2008 ICT Standardization Work Programme (Standardisation 2008) lists EU legislation, policies and actions for which ICT standardization support is relevant. Data protection, privacy and security are the main issues mentioned by the European Commission. Measures shall be taken to prevent unauthorized access to communications in order to protect the confidentiality of communications, including both the contents and any data related to such communications, by means of public communications networks and publicly available electronic communications services (Directive 2002).

The Commission specially emphasizes security in the ICT Standardization Work Programme in Article 4: the provider of a publicly available electronic communications service must take appropriate technical and organizational measures to safeguard the security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

QKD with its strong long-term security perspective is an important building block for dependably secure communication networks. It has the potential to increase usability and acceptance for typical services of the Information Society of today and in the near and long-term future (Directive 2002).

The Commission believes that the extremely strong privacy properties of QKD can be used as privacy enhancing technology (PET) to enforce protection of personal data, as it is foreseen in the legal framework.

The ETSI ISG-QKD explicitly assesses the need for confidentiality and data protection of different user groups and works on the development of standards to address these needs with QKD systems. The international member structure of ETSI allows for bringing the ISG developments to a global level.

The ISG provides a framework for the dialogue between researchers, industry, policy makers, users and other representatives from communications society to share visions of future developments and to build the necessary technological standards that will allow manufacturers to create reliable, trustworthy and interoperable products while still maintaining diversity.

The Commission considers the need for respecting data protection rules to be taken into account in standardization activities and endeavors to take into account the input of the multi-stakeholder debate on PETs in preparing the corresponding Commission actions and the work of the European standardization bodies (Communication 2007).

The Commission prioritized the standardization of information technology and communications infrastructure for ICT in 2008, by supporting research and innovation brought to standardization as early as possible. In particular the Commission addressed standardization issues that may be identified in the Commission's research programs, relating to technologies and systems for the future internet, future spectrum management techniques, ad hoc networking, sensor and actuator networks, QKD and mobile payment systems and technologies (Standardisation 2008)

The Commission, however, supports the standardization of QKD not only from the technological point of view, but also from the business point of view. The lead market initiative aims to accelerate the emergence of innovative market areas through the close coordination of innovation policy instruments. Standardization is one of the key elements for the success of this initiative: a European lead in developing globally accepted standards and an anticipatory

approach would facilitate the growth of these markets both in Europe and abroad. To account for the crucial time dimension in these markets, a particularly focused effort should be made to accelerate standards setting to enable international acceptance (Communication 2008).

5.3. The ISG-QKD

The ETSI ISG-QKD is an interdisciplinary group uniting experts from various scientific fields, such as quantum physics, cryptology and information theory with ICT engineers. Delegates come from academia, research centers and industry from all over the world.

The initiative for the current ISG-QKD originated in the SECOQC project of the 6th Framework Programme of the European Community that ended in 8 October 2008 with the live demonstration of the SECOQ Quantum Back Bone network in Vienna. Results of SECOQC's certification and standardization sub-project suggested already during the project that transforming QKD into a marketable product requires not only comprehensive security evaluation, and detailed quantum security proofs, but also system compatibility with existing infrastructures and applications and conformance with specific user requirements (Ghernaouti-Hélie *et al* 2008). The practical implementation of a forum for addressing all these provisions clearly pushed the boundaries of the SECOQC project. So plans for creating such a forum beyond SECOQC, accessible by an audience of worldwide scope, were developed and contact with ETSI established.

The contract for ISG-QKD was signed by ETSI Director General Dr Walter Weigel on 28 July 2008 and the kick-off was held during the SECOQC conference in Vienna on 9 October 2008. Since then, another three-day meeting was held in December 2008 and the next ISG meeting is scheduled for February 2009. At the time of writing this paper (January 2009), the following 16 organizations are represented in the ISG (in alphabetical order): Austrian Research Centers GmbH, Facultad de Informatica, Universidad Politecnica de Madrid, Hewlett-Packard, Centre de Compétences France, id Quantique SA, Institut Telecom, Istituto Nazionale di Ricerca Metrologica (INRIM), MIMOS Berhad, QinetiQ Group plc, Quantum Works, SmartQuantum SA, Swisscom SA, Telcordia Technologies, Inc., Telefónica SA, Thales Group, Toshiba Research Europe Ltd and University of Lausanne.

The group committed itself to a preliminary timeframe of 2 years to carry out their basic plans. In order to achieve this ambitious goal, additional work will be carried out in specialist task forces, which are financed by the European Commission. Those specialist task forces unite very small groups of experts of a very closely defined field, who cater to the ISG, in order to allow the ISG to create well-designed specifications.

6. WIs of the ISG-QKD

Several candidates for WIs were already identified in the SECOQC project and have been included in the initial plans for the ISG-QKD. Other WIs were identified during the recent ISG meetings, and additional ones have already been announced for the upcoming meeting.

Some of the active WIs have a scientific and technical focus to be addressed by the scientists developing the theoretical and experimental basis for QKD systems, while others are addressed by system integrators who transform the basic research into marketable products and by prospective users of QKD, including providers who want to offer QKD as a service to customers, and end customers of QKD.

Table 2. WIs of the ISG-QKD.

Application
WI: user requirements
WI: application interface
QKD-Networks (planned)
QKD-Link
WI: components and internal interfaces
WI: QKD devices integration within standard optical networks
WI: QKD security specification
WI: Security assurance requirements
Accompanying WIs
WI: security proofs
WI: ontology, vocabulary and terms of reference (planned)
Impact of QKD
WI: promoters and inhibitors for QKD
WI: prospects of QKD in Europe

Table 2 lists the WIs that have already been started, or are scheduled to start in the near future.

In the following paragraphs the scope of the work for the single WIs is listed as defined in the work plans for the ISG-QKD and the associated specialist task force.

6.1. User requirements

Scope of the work to be carried out: there are different groups of prospective users of QKD systems, having different security requirements and other functional requirements on these systems. Security requirements (for example regarding cryptographic strength or specific audit capabilities) are in most cases imposed by organizational security policies reflecting specific security needs of a user group. Additional functional requirements are related to system availability and interconnectivity constraints, or to system management compatibility. In this WI a catalogue of security and other functional requirements shall be compiled that lists security and other functional requirements for different user groups and different fields of application. The catalogue shall serve as a basis for implementation-independent specifications of QKD systems (ISG-QKD WI definition).

6.2. Application interface

Scope of the work to be carried out: the WI is concerned with the interface over which a QKD system shall be attached to existing ICT systems. Classical (i.e. non-quantum) key exchange systems are available on the market and are widely used to exchange keys for securing data transfer. These systems, in general, employ Diffie–Hellman style asymmetrical key exchange. QKD systems replacing such asymmetrical key exchange subsystems shall be compatible with these interfaces. In the course of this task, a collection of interfaces relevant for QKD systems shall be compiled, and the feasibility of adapting interfaces to specific characteristics of quantum key exchange shall be analyzed (ISG-QKD WI definition).

6.3. QKD networks

A specific WI for QKD networks is at the time of writing this paper (January 2009) still being discussed. Today, when quantum repeaters, as they are e.g. discussed in Briegel *et al* (1998), are not readily available, QKD links can be assembled to form trusted repeater networks, as was demonstrated with the network of the SECOQC project (Salvail *et al* 2009).

6.4. Components and internal interfaces

Scope of the work to be carried out: this WI is a preparatory action for the definition of the properties of components and internal interfaces of QKD systems. Irrespective of the underlying technologies, there are certain devices that appear in most QKD systems. These are e.g. quantum physical devices like photon sources and detectors or classical equipment like protocol processing computer hardware and operating systems. For these components, relevant properties shall be identified that are to be subsequently subject to standardization. Furthermore, a catalog of relevant requirements for interfaces between components shall be established, to support the upcoming definition of internal interfaces (ISG-QKD WI definition).

Sources and detectors play an especially important role in quantum information theoretical security proofs, which are ultimately based on assumptions on particular properties of these components. The characteristics of quantum optical components are generally of greatest importance for security analysis on the quantum optical level. This refers not only to the characteristics for which they are intended in the QKD system, but also to secondary, 'unused' characteristics of these components that can lead to unintentional leakage of confidential information through side channels, as shown by Vakhitov *et al* (2001). The identification of relevant properties and their standardized description, together with standardized testing and validation procedures, enables the efficient specification of security proofs and of generic security requirements of QKD systems.

Standards on this level can also have a substantial influence on the availability of high-quality components for the development of QKD systems as conformance to a standard represents a unique selling proposition. The increased availability of such components will again significantly reduce the necessary effort for designing and developing new QKD systems with a guaranteed security level.

Of equal importance are standards for common interfaces between components to ensure compatibility between components of different vendors.

6.5. QKD devices integration within standard optical networks

Scope of the work to be carried out: preparatory work to define hardware and software requisites for the integration of QKD devices within a shared standard optical network infrastructure. In order to maximize the amount of hardware and software shared by the quantum and conventional parts within specified requirements, some functionalities and limits must be established: in particular, optical power limits in a shared fiber, mechanism for its control, time slot reservation, quality of service requisites, etc. The functions and interface needed to accomplish this task must be defined in order that manufacturers of conventional and quantum equipment could guarantee their compatibility. Note that this does not refer to the interface of the application that would use the keys, but to protocols and requisites to use resources by both the quantum and conventional components of an optical network (ISG-QKD WI definition).

6.6. QKD security specification

Scope of the work to be carried out: in this task, technical security specifications of quantum cryptographic systems will be written. They will contain a threat and risk analysis of the assets that are to be protected in the system. These are e.g. the produced keys. Based upon this analysis, a number of security objectives shall be derived, which again are to be maintained during operation of the quantum cryptographic system. Consequently, specific functional requirements for actual implementations of quantum cryptographic systems shall be developed and listed. These specifications will provide guidance for developers and manufacturers of quantum cryptographic systems (STF QKD WI definition).

A security specification describes the security properties of an ICT system and is a prerequisite for security evaluation and certification, which again is the prerequisite for taking such a system into operation for a responsible cryptographic task. The goal of this WI is to develop a generic security specification for typical QKD systems according to the paradigm of the Common Criteria ISO/EN 15409 standard for security evaluation. Such a generic 'Protection Profile' can subsequently be used by QKD system developers and manufacturers to produce security specifications with standardized level of detail for their implementations.

6.7. Security assurance requirements

Scope of the work to be carried out: this is a preparatory WI for the security certification of quantum cryptographic equipment. The predefined assurance packages of the ISO/EN 15408 'Common Criteria' standard shall be evaluated with respect to applicability and sufficiency for the qualified development and production of QKD systems. Necessary augmentations for the specific nature of QKD systems shall be identified and added to form re-usable assurance packages for different security levels (ISG-QKD WI definition).

The 'Common Criteria' standard predefines seven evaluation assurance levels (EAL1–EAL7) that can be applied to the evaluation of a security system (in our case a QKD system). The EALs are sets of assurance requirements with increasing severity, which, once met, shall support trust that the system is as secure as intended and specified. Assurance requirements determine how QKD systems are securely developed and manufactured, which developer and manufacturer actions and tests are obligatory, and which documentation must be provided.

6.8. Security proofs

Scope of the work to be carried out: the goal of this WI is the study and systematization of existing security proofs, including the very recent state of the art and the presentation of such work in an accessible monograph. The monograph shall serve as a reference textbook for assessing the capabilities of different QKD systems and constructing respective requirements and evaluation criteria for practical security evaluation of QKD systems. This task will require some amount of original research of scientists who are not members of the ISG (ISG-QKD WI definition).

The existence of systematic security proofs, based upon standardized system implementation and attacker models, is a prerequisite for the definition of security levels for QKD. Standardized security proofs, based on standardized system implementation and attacker models, are also necessary to make QKD systems comparable.

6.9. Ontology, vocabulary and terms of reference

A specific WI is at the time of this writing (January 2009) being planned, but not officially instantiated. The ontology shall cover the domain of QKD systems providing a glossary of terms and relations among them to outline an exact and definite framework of reference for the communication of facts and issues in publications, specifications and discussions among researchers, system integrators and customers. It also shall include implementation-independent models for QKD links and networks, a description and nomenclature of common components and their relationship, as well as a research map of involved scientific disciplines and research topics.

6.10. Promoters and inhibitors of QKD

First attempts have been made to put innovative QKD products on the market. The potential for such products is high. A lot of e-services are theoretically available but are not yet frequently used (e.g. digital signature, e-health monitoring and data transfer, e-learning and accreditation). Some reluctance to deployment of these technologies stems from the lack of trust in the security of electronic communication. QKD has the potential to make such communication secure and trustworthy.

The WI covers the assessment of fields of applications, user needs and expectations as well as potential risks. This includes the identification of present and future promoters and inhibitors of QKD diffusion, applications, requirements and the framework constituting the notion of trust in this technology.

The result will be an overview paper on promoters and inhibitors of QKD in general as it is reflected by recent studies and experts in the field. The paper will be introduced to the ISG for critical discussion. It will provide a valuable input for the scenario workshop that is planned for the next WI, and for other WIs of the ISG-QKD.

6.11. WI: prospects for QKD in Europe

This WI is a major building block to assess the future challenges of QKD. The first step will be to identify valid criteria in order to evaluate what qualifies as a preferable technology to be reliable and trustworthy for the user. The next step contains the organization of a scenario workshop at the European level.

A scenario is a systemic, explicit vision of a possible future. In the context of science and technology, scenario workshops provide a framework for a dialogue between researchers, industry, policy makers, users and other representatives from society. They contain a prospective facet, looking beyond the immediate horizon—possibly into the next decade. Scenario building seeks wider inputs of knowledge for the development of an analysis and an action plan thereby making use of broader participation. Such a participation helps to build networks and mobilizes actors around shared visions of future developments. All these features will be addressed in this scenario building approach.

For the scenario workshop, selected experts representing stakeholder groups such as scientific and technical experts, industry, politics and administration, user groups and other societal non-profit organizations will meet to discuss the applications and user needs that QKD must meet. Further to that, the possible impacts of trustworthy communication technologies on the communication behavior of users will be evaluated. Participants will be people who are

familiar with the discourse on QKD. The workshop participants will be invited from various European countries and possibly from other regions.

7. Conclusion

In this paper, we analyzed QKD as a cryptographic primitive and how it can be combined with one-time-pad encryption and universal-2 hashing into confidential and authentic communication systems with an unprecedented level of theoretical security.

We stated that the practical application of QKD in a real-world scenario requires trusted QKD systems with clearly defined and evaluated security properties and security proofs. In addition, for practical use, QKD systems need to be compatible with existing ICT infrastructures. These issues can be resolved in a standardization process, where producers, developers and scientists, as well as prospective customers and users work together on common specifications. The ETSI ISG-QKD was founded with this goal in 2008 and currently 16 universities, research centers and companies are providing their expertise for nine different topics.

The ISG-QKD is open for participation by research institutions and companies from all over the world, with especially affordable membership fees for non-profit research institutions and universities. The specifications produced by the ISG-QKD are open standards and downloadable from the ETSI portal at no cost.

Thus the ISG-QKD provides an excellent basis to provide globally accepted standards for QKD, able to fit and protect various underlying systems. It will be one of the major challenges for the members of this group to translate the latest scientific results into a technically feasible implementation in a timely manner.

References

Affenzeller J *et al* 2007 Strategic Agenda for Standardisation in support of the Artemis Strategic Research Agenda *ARTEMIS—European Platform on Intelligent Embedded Systems* https://www.artemisia-association.org/downloads/standardisation.pdf (accessed 5 May 2009)

Alléaume R, Rarity J, Renner R, Ribordy G, Riguidel M, Salvail L, Shields A, Weinfurter H and Zeilinge A 2006 SECOQC White Paper on Quantum Key Distribution and Cryptography arXiv:quant-ph/0701168

Bennett Ch, Bessette F, Brassard G, Salvail L and Smolin J 1992 Experimental quantum cryptography *J. Cryptol* **5** 3–28

Briegel H-J, Dür W, Cirac J and Zoller P 1998 Quantum repeaters: the role of imperfect local operations in quantum communication *Phys. Rev. Lett* **81** 5932–5

Christandl M, Ekert A, Horodecki M, Horodecki P, Oppenheim J and Renner R 2007 Unifying classical and quantum key distillation *Proc. 4th Theory of Cryptography Conf.* (*Lecture Notes in Computer Science* vol 4392) pp 456–78

Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs) 2007 *Off. J. Eur. Union* D Celex number 52007DC0228

Communication from the Commission to the Council, the European Parliament and the European Economic and Social Committee—Towards an increased contribution from standardisation to innovation in Europe 2008 *Off. J. Eur. Union* D Celex number 52008DC0133

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) 2002 *Off. J. Eur. Union* L Celex number 02002L0058–20060503

Diffie W and Hellman M E 1976 New directions in cryptography *IEEE Trans. Inf. Theory* **22** 644–54

Dusek M, Lütkenhaus N and Hendrych M 2006 *Quantum Cryptography Progress in Optics* vol 49 ed E Wolf (Amsterdom: Elsevier) pp 381–454

Ghernaouti-Hélie S, Tashi I, Länger T and Monyk C 2009 SECOQC Business White Paper arXiv:0904.4073 [quant-ph]

Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum cryptography *Rev. Mod. Phys* **74** 145–95

Menezes A J, van Oorschot P C and Vanstone S A 1997 *Handbook of Applied Cryptography* (Boca Raton, FL: CRC Press)

Neumann P G 2003 *Principled Assuredly Trustworthy Composable Architectures* (Menlo Park: Computer Science Laboratory, SRI International)

Paterson K G, Piper F and Schack R 2005 Why quantum cryptography? arXiv:quant-ph/0406147

Poppe A, Peev M and Maurhart O 2008 Outline of the SECOQC quantum-key-distribution network in Vienna *Int. J. Quantum Inf.* **6** 209–18

Preneel B 1991 *Standardization of Cryptographic Techniques Computer Security and Industrial Cryptography* (*Lect. Not. Comput. Sci.* vol 741) (Berlin: Springer) pp 162–73

Rivest R L, Shamir A and Adleman L M 1978 A method for obtaining digital signatures and public-key cryptosystems *Commun. ACM* **21** 120–6

Salvail L, Peev M, Diamanti E, Alléaume R, Lütkenhaus N and Länger Th 2009 Security of trusted repearter QKD networks *J. Comput. Secur.* at press (arXiv:0904.4072 [quant-ph])

Scarani V, Bechmann-Pasquanucci H, Cerf N, Dusek M, Lütkenhaus N and Peev M 2009 A framework for practical quantum cryptography *Rev. Mod. Phys.* at press (arXiv:quant-ph/0802.4155)

Schneier B 1996 *Applied Cryptography* (New York: Wiley)

Shannon C E 1949 Communication theory of secrecy systems *Bell Syst. Tech. J.* **28** 656–715

Shoup V 1996 On fast and provably secure message authentication based on universal hashing *Proc. Crypto '96, Lect. Not. Comput. Sci.* **1109** 313–28

Standardisation 2008 *ICT Standardisation Work Programme 2008* http://portal.etsi.org/

Stebila D, Mosca M and Lütkenhaus N 2009 The case for quantum key distribution arXiv:0902.2839v1 [quant-ph]

Vakhitov A, Makarov V and Hjelme D R 2001 Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography *J. Mod. Opt.* **48** 2023–38

Wang X and Yu H 2005 How to break MD5 and other hash functions *Proc. EUROCRYPT 2005* (*Lect. Not. Comput. Sci.* vol 3494) pp 19–35

Wang X, Yin Y L and Yu H 2005 Finding collisions in the full SHA-1 *Lect. Not. Comput. Sci.* **3621** 17–36

Wegman M N and Carter J L 1981 New hash functions and their use in authentication and set equality *J. Comput. Syst. Sci.* **22** 265–79