ETSI GS QKD 005 V1.1.1 (2010-12)

Group Specification

Quantum Key Distribution (QKD); Security Proofs

Disclaimer

This document has been produced and approved by the Quantum Key Distribution (QKD) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG. It does not necessarily represent the views of the entire ETSI membership.

Reference
DGS/QKD-0005_SecProofs

Keywords
protocol, Quantum Key Distribution, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification (ISG) Group Quantum Key Distribution (QKD).

Introduction

The present document shall define the generic requirements for quantum information theoretic security proofs of quantum cryptography. It shall serve as a reference for the construction of requirements and evaluation criteria for practical security evaluation of quantum key distribution (QKD) systems.

In contrast to conventional cryptography which is often based on computational assumptions, quantum cryptography, notably QKD, offers "unconditional security" based on the laws of physics. To deliver such promise, demonstrating security by means of a security proof is an important aspect of quantum cryptography. Security proofs of quantum cryptography and their applicability have to be addressed with extreme care and precision primarily for two reasons. First, the security definition of a quantum cryptographic *protocol* is rather subtle. Second, it is often challenging to enforce assumptions in a security proof of a quantum cryptographic protocol in a practical quantum cryptographic *system*. Notice that any seemingly minor or innocent violation of an assumption in a security proof might be exploited by an adversary with disastrous consequences on the security of a practical QKD system.

The above two points:

i) the subtlety in security definitions; and

ii) the challenges to enforce assumptions in a practical QKD system,

shall be the two main themes of the present document.

1 Scope

Quantum key distribution (QKD) comprises technologies that use quantum mechanical effects to distribute private keys to distant partners. The goals of the present document are as follows:

- to make precise the nature of the security claim, including its statistical component;
- to list meaningful restrictions of adversarial action;
- to clarify the difference between security claim of a protocol (based on models) and the security claim of its implementation;
- to carefully list all the usual components of a QKD protocol with their critical characterizations.

The present document is developed by the QKD ISG group in which participate experts of QKD theory and practice. With the goals identified above, the present document shall help to:

- clarify the role QKD devices can play in a security infrastructure given the exact nature of their security claim;
- classify QKD devices regarding the security level they can achieve;
- clarify which parameters need to be monitored continuously or periodically to assure the generation of a secret key for the different security levels.

On the other hand, the present document will not try to do the following:

- to give specific parameters for successful QKD as these numbers change with time;
- to endorse particular security proofs.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

[1] ETSI GS QKD 008: "Quantum Key Distribution (QKD); QKD Module Security Specification".

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, M. Peev: " The security of practical quantum key distribution", Reviews of Modern Physics, Vol. 81, July-September 2009, pages 1301-1350. And references therein.

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and defintions apply:

advantage distillation: advantage distillation is a preprocessing of partially compromised data that involves two-way communications between two users, Alice and Bob

adversary: malicious entity in cryptography whose aim is to prevent the users of the cryptosystem from achieving their goals

Alice: legitimate entity who sends the data

ancilla: auxiliary (quantum mechanical) system

attacks: any action that aims at compromising the security of information

attenuation: reduction in intensity of the light beam (or signal)

authentication: used as short term for message authentication: Act of establishing or confirming that some message indeed originated from the entity it is claimed to come from and was not modified during transmission

bit commitment: scenario where Alice commits some message to Bob without being able to change it at a later stage, while Bob cannot read the message until authorized by Alice

bit error rate: percentage of bits with errors divided by the total number of bits that have been transmitted, received or processed over a given time period

Bob: legitimate entity who wishes to communicate securely with Alice and receives data from her

classical public channel: insecure communication channel, for example broadcast radio or internet, where all messages sent over this channel become available to all parties, including adversaries

clock rate: number of repetition events per time unit, e.g. number of signals sent per time unit

collective attack: attack where an adversary lets each individual signal interact with an ancilla each, but can perform joint operation on all the ancillas to extract information

composability: property that the output of one cryptographic protocol can be used by another cryptographic protocol in such a way that the security proof can be done for each protocol independently

conjugate variables: term in quantum mechanics characterizing mutually exclusive sets of properties, where the perfect knowledge of one blurs completely the other set of properties

cryptography: art and science of keeping data or messages secure

cryptographic primitives: fundamental protocols from which cryptographic applications can be composed

dark count: false alarm of a detector

NOTE: A detector may falsely give a detection event when the input state contains no photon.

dead time: duration after a detection event when a detector is inactive

decoding: process by which a receiver extracts the secret message from the publicly transmitted data

decoy state: legitimate user intentionally and randomly replaces the usual protocol signals by different signals to test the channel action

depolarization channel: quantum channel which has the same probability for each of the three types (X, Y and Z) of errors

detection efficiency: probability that an incident light photon produces a detection event

detection time: time at which a corresponding detector detects a photon

detector saturation: limit of detection frequency at which a detector can detect photons

device model: physical model of a device to capture the essential behaviour

distillation: distillation of a key which means the extraction of a secure key from some partially compromised data

eavesdropping: act of attempting to listen to the private conversation of others without their consent

encoding: process of mapping a secret message into a publicly accessible set of data from which the rightful user can decode the secret message again

entanglement: property of quantum mechanical systems that shows correlations between two physical systems that cannot be explained by classical physics

error correction: process of correcting errors in data that may have been corrupted due to errors during transmission or in storage

entropy: measure of uncertainty regarding information

eve: adversarial entity who eavesdrops the data in a quantum or classical link

gating mode: operation mode of photodetectors in which the detector can be triggered by a signal only during a specified time interval

homodyne detection: method of detecting a weak frequency-modulated signal through mixing with a strong reference frequency-modulated signal (so-called local oscillator)

individual attack: attack where Eve lets each signal interact separately with its own ancilla, and keeps the ancillas apart at later times

NOTE: A slightly different definition is used in Scaranie et al [i.1].

key establishment: procedure, conducted by two or more participants, which culminates in the derivation of keying material by all participants

NOTE: Key establishment can be based on pre-shared keys or on public key schemes.

key generation: process of generating secret keys for cryptography

key rate: rate of shared secret key generation resulting from a Quantum Key Distribution process

measurement: quantum mechanical process of reading out information from a quantum system

NOTE: The outcome of a measurement is always a classical event chosen from a set of mutually exclusive events.

multi-photon signal: optical signal containing more than one photon

permutation: change in the order of elements of a sequence of data

phase encoding: method of encoding qubits using optical phase differences between optical pulses

photon number: number of photons in a pulse

photon number resolution: ability of a photo-detection process to distinguish not only between 'no photon' and 'one or more photons', but being able to distinguish between 0,1,2,3,… photons

polarization: property of electromagnetic waves that describes the orientation of the oscillating electric field vector

privacy amplification: process of distilling secret keys from partially compromised data

private keys: keys known only to the rightful users

private states: quantum mechanical states from which private keys can be generated

protocol: list of steps to be performed by the participating entities to reach their goal

public announcement: messages sent over the public channel during a protocol

quantum channel: communication channel which can transmit quantum information, that is, it can transmit signal that needs to be described by quantum mechanics

quantum error correction codes: coding procedures for quantum states to protect them against errors during transmission or storage

quantum key distribution: procedure or method for generating and distributing symmetrical cryptographic keys with information theoretical security based on quantum information theory

quantum mechanics: physical theory that describes natural phenomena

quantum mechanical state: complete description of a physical system in quantum mechanics

quantum memories: device that can store and retrieve quantum mechanical states

quantum signal: signal described by a quantum mechanical state

quantum storage: See quantum memories.

qubit: unit of quantum information, described by a state vector in a two-level quantum mechanical system, which is formally equivalent to a two-dimensional vector space over the complex numbers

receiver: entity that receives signals

reconciliation: process of generating a set of data on which sender and receiver agree from a set of data which contains differences

NOTE: The result of reconciliation is not necessarily either the sender's or receiver's version of the data.

secret keys: private keys

security claim: precise formulation in which sense a cryptographic protocol is secure

security infrastructure: hierarchy of devices and protocols that manage key, user privileges and controls the cryptographic protocols

security level: level of protection against adversaries

security model: modeling of devices and protocols, and also of adversarial power

security parameters: parameters in a protocol that regulate the level of protection again adversaries

sender: entity sending signals

Shannon theory/information: Shannon's theory of communication defines the field of communication theory, including for example the throughput of information through noisy channels

NOTE: The central notion of that theory is the Shannon information, which is a measure of information content for signals based on entropy.

side channel: channels that are not included in the modeling of devices

security analysis: analysis of a cryptographic protocol to relate the security parameters with the exact security claim of the protocol

threshold detector: photon detector that can tell the difference between i) having no photon and ii) having one or more photons, but cannot tell the number of photons

time shift attack: specific attack aimed at a deviation between devices and their models, here the gating intervals of the various photo-detectors

trojan horse attack: any attack that aims at intruding Alice's or Bob's device to read out internal settings

X-type error: bit-flip error

Y-type error: phase error

Z-type error: combination of bit-flip and phase error

3.2 Symbols

For the purposes of the present document, the following symbol applies:

Epsilon ε	Security parameter, worst case probability that the adversary obtains a complete key produced in one run of the QKD system

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

QKD	Quantum Key distribution

4 Security Definition

4.1 What QKD delivers

Security Statement: The security statement of a QKD protocol is of a probabilistic nature. The final key can be claimed to be completely random and completely private, except with a probability ε. With that probability ε, one pessimistically assumes that an adversary might know the complete key. Any QKD device therefore shall have to quote not only the length of key that it creates in a given time over specified distances, but also the parameter ε associated with this key.

Origin of Security Parameter ε: There are several sources of this probabilistic nature of the secret key. The most obvious one comes from parameter estimation of the device and also the data, for example, the estimation of the error rate. However, as one can see from a simple example, there are additional effects that are not connected to parameter estimation.

EXAMPLE 1: Intercept/Resend attack: Consider a generic QKD protocol where an adversary intercepts all signals and resends new signals to the receiver, where the choice of the signals is based on the best guess from his measurement result. It is clear that with some (small) probability this attack succeeds without leaving any detectable trace, namely whenever all resent signals are identical to the original ones.

Reducing Security Parameter ε: A security proof shall specify for which systems parameters (loss, error rate) a secret key can be obtained, and what the security parameter ε is. Whenever a positive secret key rate is achieved with a given ε, then the value of ε can be decreased by increasing the number of exchanged quantum signals while maintaining the same system parameters. To achieve this goal, the security proof shall specify the exact protocol parameters (amount of privacy amplification) that achieve the target goal.

Interpretation: The security parameter ε has a clear interpretation, so that from a specific use case one can deduce the value of ε one should aim for, as it has a clear probability of failure interpretation which can be combined with a risk analysis.

EXAMPLE 2: One might imagine that a futuristic insurance company is wiling to ensure against a (highly unlikely) failure event.

Aborting Protocols: In setting the value of ε, note that QKD protocols can abort, for example whenever the observed error rate is too high. In these cases the output of the QKD protocol is a key of length zero, but the attempt to create a key has to be taken into account in choosing ε.

EXAMPLE 3: Eve can simply cut a quantum channel and perform a denial-of-service attack. Note that the same type of attack can also happen to a classical communication channel. So, this is not a particular short-coming of QKD.

Composability: In this property, a QKD protocol with a failure probability ε can be combined with any other protocol with a failure probability ε' in which the key is used. The failure probability ε" of the combined protocol is then bounded by the sum of ε and ε'. This property of composability of failure probabilities is essential, as the secret key is naturally to be used by other applications.

EXAMPLE 4: If during the lifetime of a QKD system, a QKD protocol with a failure probability ε is run N times, then the total failure probability for the combined N runs shall be given by N ε. So, it is not enough that ε is small. One needs to ensure that this total failure probability N ε remains small.

4.2 Structure of QKD protocols

This clause outlines the general structure of QKD protocols together with its components.

QKD protocols utilize different resources:

- **Quantum Channel:** this is a channel that preserves quantum mechanical features.

EXAMPLE: Standard telecom fibers and free-space optics transmission.

- **Authenticated Classical Channel:** this is a public channel which is authenticated, meaning that all messages on the channel are authenticated to come from the corresponding party. Information theoretically secure methods of authentication do exist. To implement a meaningful authentication structure is one of the main tasks in building up a QKD infrastructure.

- **Source of Randomness:** a physical random number generator (not a pseudo-random number generator).

A typical /QKD protocol runs in two phases:

1) **Quantum Phase:** In this phase quantum mechanical signals are exchanged via the quantum channel and measured by sender and receiver. At the end of this phase, both parties have a record of classical data. The assumptions on the quantum mechanical devices used in this step shall be discussed in depth in clause 4.4. Two distinct types of protocols exist:

   - **Prepare and Measure Protocols:** in this type of protocol one party (the sender) prepares signals chosen at random from a pre-defined set. The other party (the receiver) measures the signals in measurements of quantum mechanical nature, e.g. by choosing at random between a predefined set of quantum mechanically non-commuting measurements (active choice), or by having a single larger measurement containing non-commuting elements (passive choice).

   - **Entanglement based protocols:** in this type of protocols a third party provides bi-partite systems to both parties. Each party measures them by active or passive choice (see before). No trust needs to be put into the third party.

2) **Classical Communication Phase:** The quantum phase provides a record of classical data to both QKD parties. In the classical communication phase they use the authenticated classical channel to run through classical communication protocols (sifting, error correction, privacy amplification) to obtain a final secret key. These protocols shall be discussed in more detail in clause 4.6.

4.3 Framework for Security Statements of QKD Implementations

In this clause we clarify the interplay between scientific security proofs and tests performed on implementations in order to obtain accepted levels of security. It is important to become clear about this interplay as we develop procedures that will allow the certification of QKD implementations.

The security statement of a QKD implementation has two major contributions:

a) Scientific Security Proof:

A Scientific Security Proof takes:

1) a model of the physical devices;

2) a protocol executed with these model devices.

And proves conclusively the security of the protocol executed on the model devices. This proof gives the relevant parameters of the protocol and results in the precise security statement. For example, in the composable security definition, it gives the exact form of the security parameter ε as a function of protocol parameters.

The Scientfic Security Proof follows established accepted rules of scientific proofs and does not need further specification.

b) Implementation Verification:

To complete the security statement on a QKD implementation, we need to verify:

1) that the actual implementation corresponds to the model assumed in the security proof;

2) that the protocol executed in the device has been properly implemented.

The verification of both steps will have to be done according to the best available engineering standards, employing our best knowledge and understanding of devices.

It is important to realize the difference between the Scientific Security Proof and the Implementation Verification: the first one is a commonly accepted notion, the second one is based on best practices. Best practices can change over time, as they are based on the best available knowledge and experience. Therefore, it needs to be formulated in standards what these practices are. Testing can in principle be never exhaustive, and by definition a real device will always differ from the model. However, not all deviations are security relevant.

The result of verifications is either a pass/fail (e.g. by verifiying that certain required elements have been implemented, or some tests that have simple pass/fail outcomes) or by performing quantitative tests which give rise to security parameters that can be entered into the security proof.

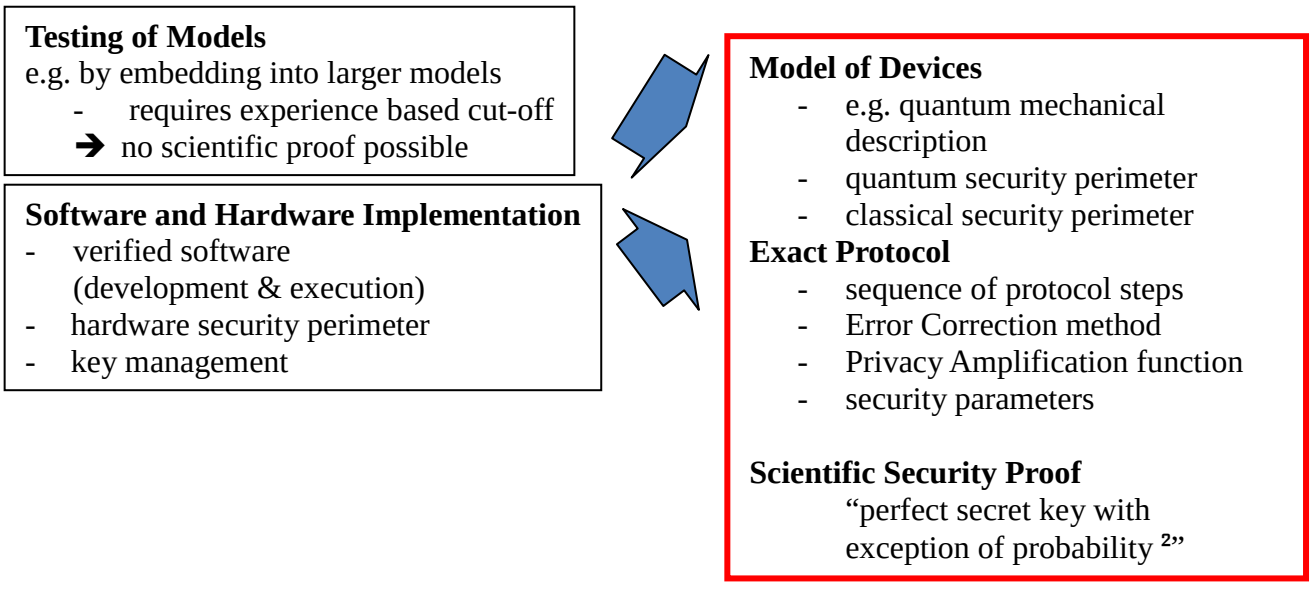

Figure 1: Illustration of interplay between scientific proof (red box) and verification based on best practices

4.4 Scientific Security proof framework

This clause explains the general features of security proofs, as they pertain to QKD protocols, and need to be linked to particular implementations by verifying the assumptions made in the protocol.

It is the task of a security proof to show which protocol parameters to choose so that for given observed parameters a secret key with security parameter ε can be generated. Any such proof is aimed at a protocol which makes assumptions about its implementation.

4.4.1 Security Assumptions on Devices

a) **Secure Perimeter:** One set of assumptions concerns the security of the QKD devices of the two legitimate parties, as it must be assumed that no adversary has access to the interior of these devices. Otherwise, they could read off the secret key as it is being generated. So a secure perimeter is assumed.

b) **Classical Interfaces:** All interfaces with the devices that pass through the secure perimeter have some underlying assumption about their performance to assure that they do not allow penetration (directly, or indirectly) of the secure perimeter. A simple example is that the classical data interfaces can be modelled by digital signals, such that no side-channel exists that permits reading off internal processes of the devices.

c) **Quantum Interfaces:** In addition to these classical channels, also the quantum channel needs to satisfy assumptions, as it leads directly to the heart of the QKD devices. No side-channels should exist that allow an eavesdropper to use the quantum channel for probing internal settings and data from outside of the device.

d) **Quantum Devices:** At the heart of the Quantum Phase of the QKD protocol are quantum mechanical devices, such as sources, detection set-ups, that generate the classical data. Typical security proofs rely on the quantum mechanical models of these devices in order to derive security statements of the QKD protocol.

e) **Deviations between Model and Device:** As a rule, there are always deviations between models and the behaviour of the actual system. For this reason, any model assumption should be made plausible, and any deviation from the actual system quantified. A security proof should be structured so as to include the quantification of the deviations, in order to take them into account during privacy amplification.

f) **Device Independent Security Proofs:** As an alternative to the quantification of deviations, there is a recent approach to the problem of correct modelling which can actually complete the QKD protocol without any physical models of the devices. In these instances, the QKD protocol must be an entanglement based protocol with an active choice of measurement. Note that all the other assumptions about the perimeter and the interfaces remain. Note also that these protocols cannot cope with more than 3 dB combined channel and detection loss in current implementations. For that reason we concentrate in the formulation of the present document on the approach that models the quantum mechanical devices.

g) **Assumptions on an adversary:** While QKD itself can be realized without imposing any technological restrictions on an adversary, it might be justified to make assumption on an adversary's power, as long as these are clearly stated and fully consistent assumptions. An example of such a set of assumptions is the noisy and bounded storage model for quantum cryptography tasks.

4.4.2 Assumptions on Adversary

This clause lists some possible assumption one might make on the capabilities of an adversary. Note that these restrictions cannot be verified but are assumed to hold. It remains to reconsider whether these assumptions are reasonable at any given time.

NOTE 1: In contrast to classical cryptography, technological restrictions as listed above need to hold only during the key establishment. If an adversary acquires later capabilities going beyond these restrictions then this does not endanger the security of the generated key.

The restrictions on the quantum storage ability are as follows:

No quantum memory: This version is often investigated in connection with individual attacks. Eve is forced to measure out her ancilla quantum state directly after the interaction.

Short term quantum memory: This shall allow an adversary to store her ancilla system until public announcements have been made, but after that time a measurement has to be made, usually combined with individual attacks.

Bounded memory: In this model at some later stage of the protocol the amount of quantum memory available to an eavesdropper is limited to some amount, so that it becomes a bound on the amount of long-term memory, while short-term memory in the first parts of the protocol can be unlimited.

Noisy memory: In this model it is assumed that any storage of quantum memory comes with an associated costs of noise within that memory.

NOTE 2: The idea of bounded memory and noisy memory can be combined together into some overall restriction on the capability of an eavesdropper in quantum storage.

The assumption of no quantum memory may result in a slightly higher key rate, explainable by the difference between the Holevo bound on Eve's information and the accessible information.

The bounded memory/noisy memory models are more recent developments which have the additional benefit to be able to achieve cryptographic primitives that go beyond QKD namely oblivious transfer, bit commitment etc. And, it is known that oblivious transfer can be used to implement a general secure two-party computation.

EXAMPLE: An example of a useful application would be secure identification with an untrusted ATM machine.

Specific attacks: In the literature one can quite often find some claims on secure key rates against some specific attacks.

NOTE 3: The analysis of specific attacks can be a good tool to investigate the limitations of a protocol, but it will not result in meaningful security statements.

Security statements should always be formulated pertaining to certain tool boxes that are available to an eavesdropper. That means, an eavesdropper can not only use each tool by itself, but also any combination of tools. QKD protocols that are secure against specific attacks often fail against eavesdroppers that use elements of that same attack but in different combinations.

4.5 Modelling, Assumptions and Side Channels

This clause discusses in detail the assumptions made in QKD protocol with respect to the quantum mechanical components of QKD devices and how verification should be done. It will also focus on the device modelling approach to security proofs of QKD mentioned in clause 4.4.1. The general philosophy is that a manufacturer shall comply with the items below:

i) specify clearly a detailed physical model of a practical QKD system;

ii) prove/verify to the user that the correspondence between the model and the physical system is indeed valid.

It is very important to have a correct model of a practical QKD system. One may well have a rigorous security proof of a QKD protocol. But, if one's model of a practical QKD system is incorrect, then there is no guarantee that the QKD system is secure. Moreover, implementation loopholes may exist in the system that may allow an eavesdropper to break/hack it.

Despite significant progress in the field, currently there is still a big gap between the theory and practice of QKD. In what follows, some general principles for modelling QKD systems are listed.

i) **List all assumptions:** It is very important to list all assumptions in a security model of a practical QKD system as explicitly as possible. This is because security is a very subtle subject and implicit assumptions or indeed any seemingly innocent shortcuts in the design of a QKD system could prove fatal from a security standpoint. A full QKD system consists of not only the optical layer, but also the electronics and classical post-processing layer. It is often rather challenging to list all assumptions explicitly. (At the time of writing, the issues of security in the calibration phase and the software layer remain largely unexplored.)

ii) **Verify** all assumptions.

iii) **Quantify deviations** from the idealized model: Practical systems are never perfect. Quite often, through testing, one will find that the characteristics or performance of our components deviate from those of our original idealized model.

NOTE: Ideally, what needs to be done is to characterize and quantify those deviations one by one and take them into account in privacy amplification. Some deviations (e.g. the fluctuations of laser intensities) are indeed easy to quantify and can be taken care of by privacy amplification. So, the above ideal procedure should be applied.

Realistically, for some deviations, however, a full characterization and quantification may be challenging at the current state of art. So, there might be situations in which one has to settle with the best effort at the moment. In these cases, one should at a minimum list all known specific attacks exploiting a particular deviation and perform those specific attacks and measure their power. Such realistic testing ensures that a practical QKD system does not suffer from obvious known attacks.

iv) **Security proof with non-idealized model:** A security proof for a practical QKD system should accept some deviations from an idealized model. In other words, it should be based on a refined security model that takes imperfections into account in a quantitative manner.

EXAMPLE: Multi-photon signals emitted by a laser, which are originally outside the domain of Bennett Brassard protocol of 1984 (BB84), can be taken care of by the idea of "tagging" in the security proofs, that is, they are assumed to be completely known to an adversary.

For concreteness, in what follows the case of weak coherent state pulse (WCP) implementation of QKD will be considered, taking into account its transmission and receiving units. However, much of the discussion can be extended to the case of entanglement-based QKD, which has two receiving units and also the case of continuous variable QKD systems.

4.5.1 Source

Typical assumptions on the source include:

a) **Phase randomization**

It is often assumed that the signal emitted by the source is phase-randomized, so that it can be described as a classical mixture of signals with definite photon number. While this is a good assumption for laser diodes that are switched on and off, so that the phase of each pulse is random due to the vacuum fluctuations, this assumption will fail in some other settings, e.g. when mode-locking is used to generate short pulses with a high repetition rate, when short pulses are cut out from a continuously operated laser by amplitude modulation, or in the Plug&Play scenario, where a strong reference signal to the weak signal pulse becomes available.

If the source is not phase randomized, one has either to take this into account in the security analysis, or one has to destroy the phase by active phase randomization. The latter procedure requires true sources of randomness.

b) **Photon statistics**

In QKD protocols it is important to know the photon number distribution of the source, for example to take the photon-number splitting attack into account, or to make use of decoy states.

The photon number statistics needs to be verified in any QKD protocol. Moreover, assurance is needed that no degradation of the statistics happens over the lifetime of the QKD device.

c) **Degrees of freedom**

Usually, the signal sources are modelled as single mode (regarding frequency, timing, spatial modes), with only one degree of freedom, such as polarization, or phase between two modes, as carrier of the quantum information. The actual source must be characterized to verify that there are no side-channels in the other degrees of freedom (frequency, timing, spatial mode).

d) **Security boundary on optical channel**

It must be assured that from the outside, no reading of the internal settings of the sending unit can be carried out, nor can any of its internal components (lasers, modulators) be modified. As a usual minimal security measure, monitored optical isolators shall be required.

4.5.2 Detection unit

a) **Degrees of freedom**

It is assumed that the detection unit reacts only to the degree of freedom into which the quantum signal is encoded, that means for example, that for polarization coding, the detectors monitoring two polarization modes do not behave differently for other degrees of freedom, such as timing, spatial modes, etc.

b) **Efficiencies**

It is assumed in most proofs that the detection probability is independent of any settings made in the measurement. Also, within one setting, the detection efficiency must be equal for all signals. In practice, single-photon counters show different detection efficiency, so that this difference must be either counteracted by a proper set-up, or taken into account in the security proof.

c) **Security boundary on optical channel**

It must be assured that from the outside, no reading of the internal settings of the receiver unit can be carried out, nor can any of its internal components (detectors, modulators) be modified. As a usual minimal security measure, monitored optical isolators shall be required.

4.6 Classical assumptions (shielding, electronic side-channels)

The classical assumption under this clause is covered in the GS QKD 008 [1] Security Specification.

4.7 Classical protocol

The classical part of a QKD protocol aims at establishing the secret key from the data. It contains typically several elements as follows:

- To test the data set.
- To precondition the data set, for example by deleting part of the data in a sifting procedure, or by adding some noise on some of the data. These are the simplest elements of advantage distillation. More advanced advantage distillation methods might also be applied.
- To reconcile the data (error correction).
- To apply privacy amplification to meet the security target.

For all these elements, it must be specified whether the communication needs to be authenticated or not, which thresholds in data testing are to be used, what decisions are taken at any step of the protocol, which exact methods (function) for error correction and privacy amplification are to be used, and how the parameters for these protocols are to be determined from the testing state.

It is of utmost importance that all details listed above fit in to the security proofs of the overall device. This includes, for example, the question of whether a random permutation on the signals shall be done or not, whether the privacy amplification function can be known and kept fixed through several QKD rounds and so on.

It should also be pointed out that it is absolutely necessary to include in all protocol specifications and applicable security proofs all parameters regarding the finite size effects of the key. That is, one have to specify the block size on which privacy amplification is being performed, as this is one of the very essential parameters in the security analysis.

In the following clause, the elements of a typical QKD protocol in the prepare and measure category are described to demonstrate what aspects of such protocols are especially critical .The classical protocol starts after the quantum phase. In this case, the assumptions for the steps are in the following form:

1) Alice prepares a random sequence of bits and corresponding bases. She prepares accordingly quantum signals and sends these over the quantum channel to Bob.

2) Bob measures the signals he receives in arbitrarily chosen bases and obtains a sequence of bits, corresponding to the bases.

4.7.1 Sifting

A few alternatives are available to process the data by sifting. The example below includes presifting and inverse sifting:

EXAMPLE:

1) Bob replies with a sequence of time slots numbers indicating time slots in which he measured signals. For each time slot he also sends the measurement basis.

2) Alice answers with a sequence consisting of: Identical Basis, Non-identical basis.

3) Alice and Bob keep the bits corresponding to the identical bases. This is the sifted key.

4.7.2 Error estimation

1) Alice selects randomly a sub-string of the sifted key and sends to Bob the corresponding bit positions and bit values. Bob compares this substring to the corresponding one in his sifted key and announces the result. Alice and Bob use that result to estimate the error rate.

2) If the error rate is below a certain limit established by the security proof, the protocol continues. Otherwise, it is aborted.

3) The openly exchanged bits are discarded from the sifted key.

NOTE: This stage can be carried out in the inverse manner or symmetrically (each party sends a substring). The relative and total amount of the opened bits is essential for a good statistical estimate.

Alternatively this stage can be skipped altogether, assuming an estimate of the error rate - e.g. error of the previous key generation round. This can lead to failure of the Error Correction (Reconciliation phase) and potentially losing the full block.

4.7.3 Error Correction (Reconciliation)

A strict one-way error correction protocol (forward direction) is considered as an example:

EXAMPLE:

1) Alice uses an error rate and a publicly announces error correction code to generate parity bits that are guaranteed to be sufficient to reconcile Bob's key with her one under the selected error correction code.

2) Alice sends the parity bits to Bob (see below method of transmission).

3) Bob applies the error correction procedure to his sifted key. Alice's sifted and Bob's corrected keys become the reconciled key.

4) Bob compares his reconciled and his sifted keys. On this basis he establishes a post reconciliation error estimate. He communicates this estimate to Alice. If the error rate is below a certain limit established by the security proof the protocol continues, otherwise it is aborted.

NOTE 1: In case the error estimate has underestimated the actual difference between the sifted keys of Alice and Bob, this phase fails with high probability either by an explicit failure (in this case the sifted key has to be discarded altogether) or this is revealed in the subsequent confirmation phase (see below).

NOTE 2: One needs to specify whether to encrypt the parity information with the one-time-pad or not. If the parity information is un-encrypted, one needs to show how this information is included in the privacy amplification step. In that case an exact counting of the amount of information opened during error correction needs to be done. If the parity information is encrypted, one needs to take the amount of key consumption into account in calculating the final key generation rate.

NOTE 3: Other alternative methods for error correction include, for example, reverse reconciliation and advantage distillation protocols. Notice that a security proof that works for forward reconciliation may not necessarily work for reverse reconciliation and vice versa. One needs to specify in detail which specific protocol is used together with the parameters and a clear proof of security (that would achieve the desired failure probability ε).

4.7.4 Confirmation

Alice and Bob can check with high probability if the error correction is successful by performing a confirmation test. One way to do so is that they compute and compare a hash value of a suitably chosen function of their reconciled key. An advantage of passing the confirmation test ensures identic keys for Alice and Bob even if only a rough estimation of the error rate has been carried out in the error estimation process.

One needs to specify clearly the confirmation protocol used together with the parameters and verify that they are consistent with a security proof that shall provide the desired failure probability.

NOTE: One clearly needs to take the information leakage to Eve during this confirmation test into account.

4.7.5 Privacy Amplification

The objective of privacy amplification is to reduce the probability that the eavesdropper has any knowledge on the key below a certain upper boundary ε. To obtain this goal the process described below is to take place:

1) Alice and Bob independently compute the final key length, which depends on security proof, protocol parameters, including error rate, and reconciled (confirmed) key block length.

2) Alice selects randomly an appropriate hashing function belonging to a publicly known 2-universal class and communicates it to Bob.

3) Alice and Bob perform hashing with this function on their reconciled (confirmed) keys. The results are the final keys of Alice and Bob.

NOTE 1: The block size for finite key effects enters in Step 1 of the protocol.

NOTE 2: One needs to specify whether to use a new or the same hash function in a new round of QKD, and connected to that, whether random reshuffling of bits is required or not.

4.7.6 Authentication

The communication via the public channel needs to be authenticated to avoid a man-in-the-middle attack. Various methods might be suitable:

a) Information Theoretic Authentication

   This uses universal-2 hashing functions (as pioneered by Carter and Wegman). This method requires a shared random secret for the first round of QKD, otherwise the problem of distribution of an initial secret key needs to be solved. Subsequent rounds of QKD can use secret keys generated in preceding QKD rounds. The security parameter ε of the combined QKD protocol and the authentication protocol follows from the composability statement of the respective security proofs.

b) Other Authentication Methods

   In ongoing research, other methods of authentication are being discussed. The authentication mechanism needs to be secured only until the time a key is accepted, but may be broken later without compromising the security of that key.

NOTE: Although not strictly necessary from a theoretical point of view all communication exchanges on the public channel should be authenticated, as a default option. This option can be overruled only in case a detailed security analysis of post-processing explicitly demonstrates that authentication of some communication rounds can be skipped.

4.7.7 Common Sources of Mistakes in Classical Protocols

This clause highlights some of the typical mistakes. The list outlined here is not exhaustive, but its serves to highlight some common pitfalls.

1) Failure to mention which information to authenticate:

   a) Why authentication?

      Authentication is crucial. Without authentication, Bob has no advantage over Eve. In fact, Eve can simply launch a man-in-the-middle attack by impersonating as Bob to Alice and Alice to Bob by tapping in to both classical and quantum channels.

   b) What to authenticate?

      Unless otherwise instructed, we think Alice and Bob should authenticate everything (including e.g. who the sender and the intended receiver of the message are, the main text of the message, and a time-stamp for a whole message). This relieves from the need of a detailed analysis at the expense of a small loss in potential key rate.

   c) Is it enough to choose a secure authentication function?

      It is not enough to say that one has chosen a secure authentication *function* (e.g. a two-universal hash function). One must study authentication from a *protocol* level. The whole authentication protocol must be chosen in such a way to withstand standard attacks such as "intercept and replay" attack. Ideally, a formal proof of security of the whole authentication protocol should be provided.

NOTE 1: If something is not authenticated or some information is not sent at all, the burden of proof rests on the manufacturer to show that such a simplified authentication scheme is still secure.

2) A two-way protocol (e.g. Cascade) is used whereas a security proof with one-way protocol is cited as justification.

NOTE 2: Some security proofs (e.g. the original Shor-Preskill's proof) refer to only one-way error correction protocols. Should two-way protocols such as Cascade be used, it is important to provide a new proof that applies to the actual implementation.

3) Parameters in error correction or privacy amplification are not fully specified.

   It is not enough to say that one has performed error correction or privacy amplification. One must also show that the parameters used are consistent with the desired security parameter ε.

4) Finite size effects are not fully considered.

   Many key rate formulas refer to the asymptotic key rate of infinitely many signals. In practice, any

   QKD protocol is done with a finite number of signals. It is important to use a security proof and a key rate formula that consider the finite size effects.

5) Missing/wrong prescriptions for dealing with multiple-clicks.

   Real-life devices may have dark counts or receive multi-photon signals, thus resulting in detection events in multiple detectors. One needs to specify how to deal with those multiple-clicks events and which security proof can be applied to prove the security of a practical QKD system with such events.

6) Information leakage not fully taken into accounts.

During the classical phase, information may be leaked to an eavesdropper. Examples of the kind of information leaked include error syndrome and location. It is important to check that a security proof still works, despite such information leakage. Also, authentication consumes some amount of secrets shared by Alice and Bob, thus reducing the net key generation rate. It is important to take such key consumption into account.

7) Side information may be unintentionally disclosed in the classical post-processing protocol.

During the classical protocol, side information may be unintentionally disclosed, thus compromising security. For instance, if Alice and Bob disclose too fine-grained the synchronization information, then Eve may learn additional information by studying the information in the timing side channel.

Annex A (informative): Authors & contributors

The following people have contributed to the present document:

STF:

Norbert Lütkenhaus, Institute of Quantum Computing, University of Waterloo

Hoi-Kwong Lo, University of Toronto

Rapporteur:

Suhairi Saharudin , MIMOS Berhad

Zalhan, Md Yusof, MIMOS Berhad

Other contributors:

Momtchil Peev, AIT Seibersdorf

Jean-Marc Merolla, CNRS

Norziana, Jamil, MIMOS Berhard

History

Document history		
V1.1.1	December 2010	Publication