Quantum Key Distribution

Table of contents

1. Introduction

Already in the late 1960's, the concept of using quantum encoding of photons for secure transmission of information was proposed by Stephen Wiesner.

Quantum cryptography (a misnomer for "secure quantum communication") involves encoding of information transmitted from place to place in quantum states (Box 1.1) of qubits (Box 1.2), as opposed to classical communication's use of bits. These qubits are sometimes called "flying qubits", whereas the term "stationary qubits" represent the physical qubits used for local computation by a quantum device.

A quantum state is a mathematical entity that provides a probability distribution for the outcomes of each possible measurement on a quantum system. Knowledge of the quantum state together with the rules for the quantum system's evolution in time exhausts all that can be predicted about the quantum system's behaviour.

Box 1.1: Quantum state

A qubit (quantum bit) is a basic unit of quantum information. It is the quantum version of the classic bit (binary bit) physically realised with a two-state quantum device. In classical computing the information is encoded in bits, where each bit can have the value zero or one. In quantum computing the information is encoded in qubits. A qubit is a two-level quantum system where the two basis qubit states are usually written as $|0\rangle$ and $|1\rangle$. A qubit can be in state $|0\rangle$, state $|1\rangle$ or (unlike a classical bit) in a linear combination of both states ($\alpha|0\rangle + \beta|1\rangle$). The name of this phenomenon is superposition.

Box 1.2: Quantum bit (qubit)

Qubit quantum states encoded either in the polarisation (Box 1.3) or in the spatial wave function of photons (photonic qubits) are the preferred flying qubits, because light transmission through optical fibres and through free space are well-developed technologies that are reliable enough for the transmission of photonic qubits even over long distances.

Polarisation is a property of transverse waves which specifies the geometrical orientation of their oscillations. In a transverse wave, the direction of the oscillation is perpendicular to the direction of motion of the wave (in contrast, in longitudinal waves, the displacement of the particles in the oscillation is always in the direction of propagation, so these waves do not exhibit polarisation). Transverse waves that exhibit polarisation include electromagnetic waves such as light waves and radio waves. An electromagnetic wave consists of a coupled oscillating electric field and magnetic field which are always perpendicular to each other; by convention, the polarisation of electromagnetic waves refers to the direction of the electric field. In linear polarisation, the fields oscillate in a single direction. In circular or elliptical polarisation, the fields rotate at a constant rate in a plane as the wave travels. The rotation can have two possible directions; if the fields rotate in a right-hand sense with respect to the direction of wave travel, it is called right circular polarisation, while if the fields rotate in a left-hand sense, it is called left circular polarisation. The spin of the photon spin is the quantum-mechanical description of light polarisation, where spin $+1$ and spin -1 represent two opposite

directions of circular polarisation. Light of a defined circular polarisation consists of photons with the same spin.

Box 1.3: Polarisation

Using photons for transmission of encoded quantum states is very attractive, because they undergo very little decoherence, even over large distances; they are, however, susceptible to loss and/or dispersion. Optical fibre is intrinsically lossy. Free space is either very low-loss (in the atmosphere) or lossless (in vacuum) but is subject to dispersion. In optical fibres, the photon loss rate increases exponentially with the distance. In vacuum and in the atmosphere, the photon dispersion rate grows quadratically with the distance.

Currently, the best-known application of secure quantum communication is Quantum Key Distribution (QKD). QKD exploits quantum mechanics phenomena to establish a shared secret cryptographic key between two parties without a (malicious) third party learning anything about that key, even if it can eavesdrop on all communication.

By using quantum superposition or quantum entanglement and transmitting information in quantum states, a quantum communication system can be implemented between two parties. An important and unique property of QKD is the ability of the two communicating parties to detect the presence of any third party (eavesdropper) trying to gain knowledge of the shared secret key. This results from a fundamental law of quantum mechanics: the process of measuring a quantum system disturbs the quantum system's state. A third party trying to eavesdrop on the key must somehow measure it, thus causing a disturbance that can be detected by the communicating legitimate parties. Provided that the disturbance caused by eavesdropping remains below a certain threshold, a shared secret key can be produced that is guaranteed to be secure, i.e. the eavesdropper has no information about it.

QKD security thus relies on the laws of quantum mechanics and -in theory- has provable information-theoretic security. In contrast, classical public-key cryptography used for secret key establishment relies on the computational difficulty of certain hard one-way functions, without any mathematical proof whatsoever that these one-way functions cannot be reversed.

2. Generic QKD protocol

A QKD key exchange protocol requires that sender and receiver dispose of a quantum communication channel which allows quantum states to be transmitted; this channel is either an optical fibre or free space. Sender and receiver also need to be able to communicate via a classical communication channel; this channel can range from a dedicated transmission link to the public internet.

QKD protocols are designed under the assumption that eavesdroppers have unlimited computing and storage resources and can interfere in any way with either communication channel. This requires guaranteed authenticity and integrity of messages exchanged over the classical communication channel to prevent man-in-the middle attacks. A small pre-shared key (secured in hardware of a QKD appliance pair), expansion of the pre-shared key based on QKD key exchange results, and message authentication based on WCA (Box 2.1) are typically used for this purpose. QKD implementations often use a transactional message authentication scheme where message authentication is performed repeatedly.

Wegman-Carter Authentication (WCA) message authentication is based on secretly selecting a hash function (using a salt) from a library of Universal Hash Functions (UHFs) and sending its output to a Pseudo-Random Function (PRF), to create a Message Authentication Code (MAC). The WCA scheme is information-theoretically secure (i.e. secure against adversaries with unlimited computing and storage capabilities), provided that the authentication key is uniformly distributed.

Box 2.1: Wegman-Carter Authentication (WCA) (Heisenberg principle)

QKD protocols perform several functions, which are described in sequential order below, but which would typically be performed in overlap or in parallel in actual QKD implementations.

There are many variants of the generic QKD protocol which is described below.

2.1. Quantum exchange

Upon establishment of the quantum and classical communication channels, a quantum exchange protocol is executed, in which a sequence of photonic qubits is exchanged between sender and receiver through the quantum communication channel. The quantum states of these photons are prepared and/or measured according to randomly selected bases by sender and receiver.

In contrast to classical physics, the act of measurement is an integral part of quantum mechanics. Measuring an unknown quantum state changes that state in some way. This is a consequence of quantum indeterminacy (Box 2.2) and can be exploited to detect any eavesdropping on quantum communication (which necessarily involves measurement) and, even more importantly, it can also be exploited to calculate the amount of information that has been intercepted.

Quantum indeterminacy (Heisenberg principle) is a fundamental principle of quantum mechanics which postulates that there is a lower limit to the precision with which one can measure two independent parameters relating to the same object such as its speed and position or the energy emitted and the duration of emission.

Box 2.2: Quantum indeterminacy (Heisenberg principle)

2.2. Classical post-processing

The quantum exchange protocol is in fact the only quantum part of a QKD protocol. The remaining parts of a QKD protocol consist of classical post-processing of the measurements obtained by the quantum exchange protocol, in concert with the execution of classical post-processing protocols over the classical communication channel.

2.2.1. Raw cryptographic key calculation

First, sender and receiver announce which bases they have used to prepare/measure the qubits exchanged over the quantum channel. The bits corresponding with qubits for which sender and receiver have used different bases are then discarded. The retained bits constitute the so-called raw cryptographic key (aka “sifted key”).

2.2.2. Quantum exchange error rate calculation

Next, an estimate of the quantum exchange error rate is calculated. Typically, a randomly chosen small percentage of the bits of the raw secret key are selected and compared between sender and receiver to calculate this estimate.

Differences between the sender’s quantum state preparations/measurements and the receiver's measurements (i.e. quantum exchange errors) may be caused by measurements made by an eavesdropper or by unfavourable environmental conditions (e.g. imperfections in the transmission medium and photon detectors, or physical disturbances during quantum exchange). Because it is not possible to distinguish between these two types of errors (malicious interference and noise), guaranteed QKD security requires the assumption that all errors are due to eavesdropping.

If the quantum exchange error rate exceeds a certain predetermined threshold, the established raw cryptographic key must be discarded. Typically, the QKD protocol is then restarted.

2.2.3. Error reconciliation

If the quantum exchange error rate remains below the predetermined threshold, there are typically still errors in the raw secret key that need to be identified, and the affected bits need to be corrected (or discarded). Error reconciliation is performed to correct any such errors and to minimise the amount of information leaked to eavesdroppers on the classical communication

channel. This results (with a very high probability) in a perfectly matched and error-free secret key shared between sender and receiver, and in determination of the Quantum Bit Error Rate (QBER).

If the QBER exceeds a certain predetermined threshold, the established secret key must be discarded and the QKD protocol is then typically restarted.

Error reconciliation is done by means of specialised bi-directional correction mechanisms, e.g. the Cascade protocol, Low-Density Parity-Check (LDPC) codes or the Winnow Machine Learning (WML) algorithm. Error reconciliation is highly resource demanding and typically takes a major part of QKD protocol post-processing. It may therefore have considerable impact on the QKD key generation rate, depending on actual implementation choices (LDPC demands larger computational and memory resources than either Cascade or Winnow, but it requires less communication resources). New error reconciliation techniques, for example Tree Parity Machine (TPM), a type of Artificial Neural Network (ANN) inspired by biological neural networks, have been shown to demand less computing and communication resources. This would result in higher key generation rates, which is attractive given the increasing interest in satellite and global QKD connections.

2.2.4. Entropy estimation

If the determined QBER value remains below the predetermined threshold, entropy (Box 2.3) estimation is performed, to account for secret key information leaked, i.e. how much information the eavesdropper could have gained about the shared secret key (this is known because of the errors that were introduced by eavesdropping).

Entropy is a scientific concept as well as a measurable physical property that is most commonly associated with a state of disorder, randomness or uncertainty.

Box 2.3: Entropy

Key information may have been leaked when executing the quantum key exchange protocol over the quantum channel (e.g. using non-ideal optical transmitters that produce insecure multi-photon pulses) or when performing error reconciliation over the classical communication channel. In general, conservative entropy estimations are made (though QKD implementations may differ considerably in this respect).

2.2.5. Privacy amplification

The entropy estimation is input for the privacy amplification process. Privacy amplification is a method for reducing (and effectively eliminating) an eavesdropper's partial information about the established shared secret key, which could have been gained both by eavesdropping on the quantum communication channel and on the public communication channel.

Privacy amplification transforms the established shared secret key into a new one, in such a way that the eavesdropper has only negligible information about it. This is done by means of universal hashing, i.e. randomly choosing a hash function from a publicly known set. The chosen hash function takes as its input the established shared secret key and outputs a new and shorter shared secret key. The amount by which the key is shortened is determined based on the entropy estimation value.

Privacy amplification ensures that the probability of an eavesdropper having any knowledge of the new cryptographic key can be reduced to an arbitrary low value (albeit at the cost of shortening the new shared secret key).

2.2.6. Key comparison

In the last step of the QKD protocol, the sender and receiver each calculate a hash of their instance of the (new) shared secret key. If these hashes match, the QKD protocol is considered to have completed successfully.

If they do not match, the established (new) secret key must be discarded and the QKD protocol is then typically restarted.

3. QKD protocol types

Charles Bennett and Gilles Brassard embraced the concept proposed by Stephen Wiesner and worked it out as the BB84 (Bennett and Brassard 1984) QKD protocol. In 1989, they demonstrated the first BB84-based QKD implementation, in which the photon detector produced different audible signals ("clicks"), depending on whether a "0" or "1" bit had been encoded in the photon; it was therefore said to be "fully secure against deaf eavesdroppers". The term "clicking" is still used in the description of modern photonic equipment, though such equipment no longer produces audible signals.

Many other QKD protocols have been proposed and designed after BB84. There are several different approaches for quantum exchange protocols, but they can be divided into two main categories depending on which quantum mechanics properties they exploit:

1. **Prepare and Measure (P&M) based quantum exchange protocols**
   P&M QKD protocols are based on the superposition of quantum states of photonic qubits.

2. **Entanglement based quantum exchange protocols**
   The quantum states of two (or more) separate quantum systems can become linked together in such a way that they must be described by a combined quantum state, not as individual quantum systems. This is known as quantum entanglement and implies that performing a measurement on one quantum system affects the other. Quantum teleportation is a communication method that involves transmitting quantum state by exploiting the properties of quantum entanglement. It works by first creating pairs of entangled photons and then sending one photon of each pair to the sender and the other one to the recipient. The sender measures the state of the qubits that hold the quantum information and the state of the entangled photons at the same time. These interactions change the state of its photons, and because they are entangled with the receiver's photons, the interactions instantaneously change the state of the receiver's photons too. In effect, this "teleports" the quantum state of the sender's qubits to the receiver's photons. However, the receiver cannot reconstruct the quantum information until the sender sends the result of its quantum state measurements over the classical communication channel in the form of bits.

   An advantage of typical entanglement-based key exchange protocols is that they produce secret keys which are true random numbers, based on underlying quantum mechanics properties.

The two main approaches for quantum exchange protocols described above can each be further divided into three families of QKD protocols based on the method used for coding:

1. **Discrete Variable QKD (DV-QKD) protocols**
   Discrete Variable (DV) coding uses the polarisation quantum states of single photons.

2. **Distributed Phase Reference QKD (DPR-QKD) protocols**
   Distributed Phase Reference (DPR) coding uses the phase or arrival times of single photons.

3. **Continuous Variable QKD (CV-QKD) protocols.**
   Continuous Variable (CV) coding uses the quadrature of the quantised electromagnetic field using coherent states and homodyne or heterodyne detection techniques (Box 3.1). DV-QKD technology offers a superior pathway forward in terms of cost and form factor because it is compatible with current optical fibre telecommunications technology. For example, the GG02 QKD protocol (see below) has attracted a lot of interest. Some well-known DV-QKD protocols, such as B92 (see below) can be transformed to CV-QKD protocols and such variants are also being researched and implemented.

Homodyne detection is a method of extracting information encoded as modulation of the phase and/or frequency of an oscillating signal, by comparing that signal with a standard oscillation that would be identical to the signal if it carried null information. "Homodyne" relates to the use of a single frequency, in contrast to the dual frequencies employed in heterodyne detection.

Box 3.1: Homodyne versus heterodyne detection

Current QKD protocols and QKD implementations are mostly optimised for use with state-of-the-art optics technology and often use readily available optical components that implement parts of the QKD technology.

There is a growing interest for QKD use cases in satellite networks. QKD systems that must be able to operate over Free-Space Optical (FSO) communication channels need to mitigate several problems that exist in this environment, such as for example atmospheric turbulence. This requires optimisation and even modification of the QKD protocols that are being used and furthermore, their actual implementations need to be tailored to the FSO environment as well.

A few widely implemented used QKD protocols are described below. It should be noted that several other QKD protocols have been proposed and developed, some of which have been implemented in commercially available QKD products.

3.1. BB84 (Bennett and Brassard 1984) protocol

The Bennett and Brassard 1984 (BB84) QKD protocol, named after its inventors Charles Bennett and Gilles Brassard, and the year of publication (1984), is a P&M DV-QKD protocol. It was originally

described using photon polarisation states to transmit the information. However, any two pairs of conjugate photon quantum states can be used for the protocol. Indeed, many optical fibre-based QKD products that are labelled as BB84 implementations use phase-encoded instead of polarisation-encoded photon quantum states.

The security of the original BB84 protocol is based on encoding the information in four non-orthogonal quantum states, these are all photon polarisation states. Quantum indeterminacy implies that these quantum states cannot be measured without disturbing the original quantum state (no-cloning theorem). BB84 uses two pairs of quantum states, with each pair conjugate to the other pair, and the two quantum states within a pair orthogonal to each other. Pairs of orthogonal quantum states are referred to as a basis. The usual photon polarisation state pairs used for the BB84 protocol are either the rectilinear basis of 0° (vertical) and 90° (horizontal) and the diagonal basis of 45° and 135°.

The first step in the BB84 protocol is quantum exchange. The sender creates a random bit (0 or 1) and then randomly selects one of its two bases (rectilinear or diagonal). The sender then prepares a photon with a polarisation state depending both on the bit value and the selected basis and transmits it to the receiver using the quantum communication channel. The sender also records the state, the measurement basis used, and time of each photon sent. This process is repeated for each bit to be sent.

According to the laws of quantum mechanics, no possible measurement distinguishes between the four different photon polarisation states, as they are not all orthogonal. The only possible measurement is between any two orthogonal states. As the receiver does not know the basis (rectilinear or diagonal) the photons were encoded in, all it can do is to select a basis at random to measure in (either rectilinear or diagonal). The receiver does this for each photon that is received, and also records the time, the measurement basis used and the measurement result.

After the receiver has measured all the photons that have been received, it communicates with the sender over the classical communication channel. The sender broadcasts the basis each photon was sent in, while the receiver broadcasts the basis each photon was measured in. Both sender and receiver discard photon measurements where the receiver used a different basis than the sender (on average, this will be half of them), retaining the other measurements made as the bits of a so-called raw shared secret key (aka “sifted key”).

To check for the presence of an eavesdropper, sender and receiver then compare a small percentage of the bits of the raw secret key. If an eavesdropper has gained any information about the photons' polarisations, this will have introduced errors in the receiver's measurements. Unfavourable environmental conditions might also cause errors. Because it is impossible to distinguish between these two types of errors, guaranteed security requires the assumption that all errors are due to eavesdropping. If more than a certain predetermined number of bits are found to be different, the raw secret key is discarded, as its security cannot be guaranteed. The predetermined value is chosen so that if the number of bits known to an eavesdropper is smaller than this value, privacy amplification can be used to transform the raw shared secret into a smaller

shared secret key, while at the same time reducing the eavesdropper's knowledge of the key to an arbitrarily small amount.

It should be noted that the BB84 protocol requires the generation of genuine random numbers for its keys, which may or may not be provided by an embedded Quantum Random Number Generator (QRNG) component.

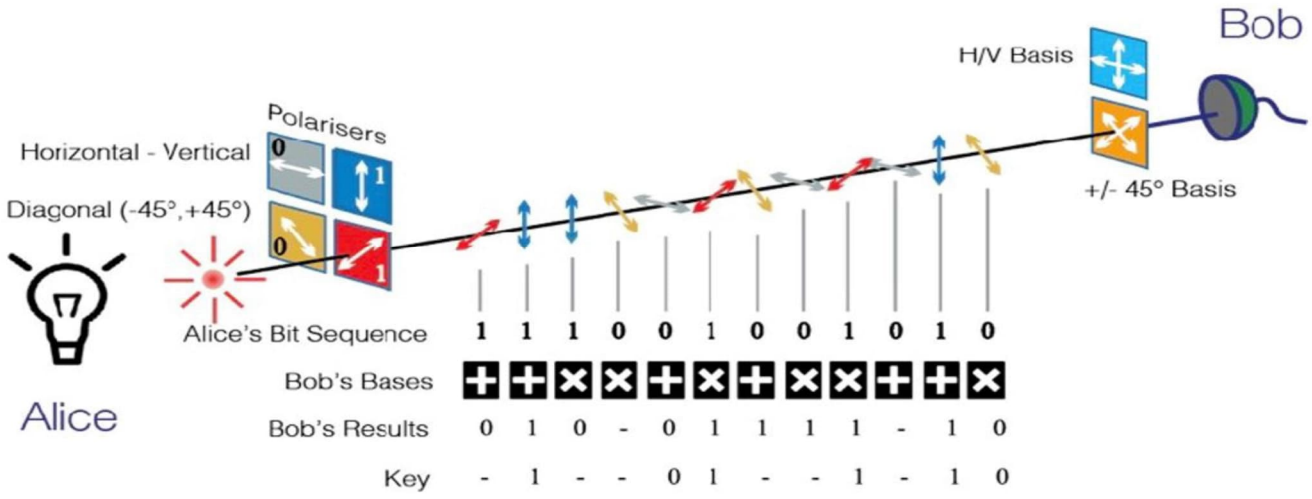

Figure 3.1 Schematic overview of the BB84 QKD scheme (source: Chegg)

3.2. E91 (Ekert 1991) protocol

The Ekert 1991 (E91) QKD protocol, named after its inventor Artur Ekert and the year of publication (1991), is an entanglement-based DV-QKD protocol, which uses Einstein-Podolsky-Rosen (EPR) entangled pairs of photons. These photon pairs are created by a common source and then distributed so that sender and receiver each end up with one photon from each EPR-entangled pair (Box 3.2).

> The Einstein-Podolsky-Rosen (EPR) paradox refers to a thought experiment that Albert Einstein, Boris Podolsky and Nathan Rosen formulated in 1935, in order to argue that quantum mechanics was an incomplete theory. In their view (which was shared by many other leading physicists at the time), quantum particles carry physical attributes not included in the quantum mechanics theory, and the uncertainties in quantum mechanics theory's predictions are due to ignorance of these attributes (which were later called 'local hidden-variables').

Box 3.2: Einstein-Podolsky-Rosen (EPR) paradox

The entangled photon polarisation states are perfectly correlated in the sense that if sender and receiver both measure whether their photons have vertical or horizontal polarisations, they always get the same answer. The same is true if they both measure any other pair of complementary (orthogonal) polarisations. Nonetheless, the results are completely random; it is impossible for the sender to predict if it (and thus the receiver) will measure vertical or horizontal polarisation.

Importantly, any attempt at eavesdropping destroys these correlations in a way that sender and receiver can detect.

In the E91 quantum exchange protocol the sender measures each photon it receives using a randomly chosen selection from the set (0°, 45°, 90°) and the sender measures each photon it receives using some basis from the set (45°, 90°, 135°). Sender and receiver keep their series of basis choices private until measurements are completed.

The measurements are then divided into two groups: a group of measurements where the same measurement basis was selected by sender and receiver and a group containing all other measurements. To detect eavesdropping, they can compute a test statistic using the correlation coefficients between the sender's bases and the receivers, like that associated with Bell's theorem test experiments. If there is an error in this value, sender and receiver can conclude that the quantum channel is not secure because an eavesdropper has introduced local realism to the quantum system, thereby violating Bell's theorem (Box 3.3). On the other hand, if this value turns out to be correct, the quantum exchange protocol is successful, and the first group of measurements can be used to generate the shared secret key.

Bell's theorem is used to prove that quantum mechanics is incompatible with 'local hidden-variable' theories. It was introduced by physicist John Stewart Bell in a 1964 in response to the Einstein-Podolsky-Rosen (EPR) paradox. Bell carried out an analysis of quantum entanglement and deduced that if measurements are performed independently on the two separated halves of a pair of entangled particles, then the assumption that the outcomes depend upon 'local hidden-variables' within each half implies a constraint on how the outcomes on the two halves are correlated. This constraint would later be named the "Bell inequality". Quantum mechanics predicts correlations that violate this inequality and multiple variations on Bell's theorem have been tested experimentally in physics laboratories many times. All these "Bell tests" have found that the hypothesis of 'local hidden-variables' is inconsistent with the way that quantum entanglement works. While the significance of Bell's theorem is not in doubt, its full implications for the interpretation of quantum mechanics remain unresolved.

Box 3.3: Bell's theorem

It should be noted that in the E91 protocol, the randomness of the generated keys is guaranteed by the randomness of the readouts of the entangled photon pairs.

3.3. B92 (Bennett 1992) protocol

The Bennett 1992 (B92) QKD protocol, named after its inventor Charles Bennett and the year of publication (1992), is a modified version of the BB84 QKD protocol. While the BB84 QKD protocol uses four different photon polarisation states, the B92 QKD protocol only uses two: one from the rectilinear basis, conveniently 0° (vertical) polarisation state, and one from the diagonal basis, conveniently 45° polarisation state.

The B92 protocol is easier to implement than the BB84 protocol but is considered less secure. It can also be implemented as a CV-QKD protocol where the two different states just differ by phase and homodyne detection is used to measure these states.

3.4. BBM92 (Bennett, Brassard and Mermin 1992) protocol

The Bennett, Brassard and Mermin 1992 (BBM92) QKD protocol, named after its inventors Charles Bennett, Gilles Brassard and Nathaniel David Mermin, and the year of publication (1992), is a simplified version of the E91 QKD protocol. The photon source must still produce EPR-entangled pairs of photons, but the need to perform a Bell inequality test is removed.

3.5. SSP99 (Six-State Protocol 1999) protocol

The Six-State Protocol 1999 (SSP99) QKD protocol, which was proposed by Andrea Pasquinucci and Nicolas Gisin in 1999, is a modified version of the BB84 QKD protocol. While the BB84 QKD protocol uses four different photon polarisation states, the SSP99 QKD protocol uses six and is therefore considered more secure than the original BB84 QKD protocol.

3.6. GG02 (Grosshans and Grangier 2002) protocol

The Grosshans and Grangier 2002 (GG02) QKD protocol, named after its inventors Frédéric Grosshans and Philippe Grangier, and the year of introduction (2022), was the first of a series of CV-QKD protocol proposals. Various CV-QKD protocols have subsequently been proposed, such as one-way, two-way and MDI-QKD protocols (explained in Chapter 4). At present, CV-QKD can be realised using low-cost off-the-shelf optical components compatible with current telecom fibre technology. CV-QKD protocols are attractive for implementation reasons but their security is quite involved.

3.7. SARG04 (Scarani, Acín, Ribordy and Gisin 2004) protocol

The Scarani, Acín, Ribordy and Gisin 2004 (SARG04) QKD protocol, named after its inventors Valerio Scarani, Antonio Acín, Grégoire Ribordy and Nicolas Gisin, and the year of publication (2004), was derived from the BB84 protocol. It uses different qubit encodings with the objective to provide more robustness when used with multi-photon (faint laser) sources than the BB84 protocol (which was developed for use with single-photon sources). SARG04 provides more resistance to Photon Number Splitting (PNS) attacks (explained in Chapter 4) but its QBER is significantly higher than that of BB04 when used over noisy quantum channels.

4. QKD implementation issues

Implementation of QKD faces several practical challenges. This is predominantly due to limits imposed on the optical transmission distance and on the cryptographic key generation rate (which is typically several orders of magnitude lower than the maximum optical transmission rate). In particular, the propagation of photons through optical fibres or free space is subject to photon loss or dispersion, the extent of which increases with distance. The Pirandola-Laurenza-Ottaviani-Banchi (PLOB) repeaterless bound is a fundamental limit on the quantum capacity of direct quantum communication, i.e. communication without optical amplifiers. For optical fibres, the effective operational distance of QKD products is limited to a few 100 km at the current state of optics technology.

A way to overcome the distance limitation and at the same time achieve much higher key generation rates consists of deploying an intermediate node between the communicating the parties, which implements a limited form of device-independent quantum cryptography (Box 4.1).

Quantum cryptographic protocols are device-independent if their security does not rely on trusting that the quantum devices used to implement the protocol are truthful. The security analysis of these protocols includes scenarios of imperfect or even malicious devices. Device-independent quantum cryptography is based on "self-testing" quantum devices, the internal operations of which can be uniquely determined by their input-output statistics. Bell inequality tests are typically used for checking the “honesty” of the quantum devices. Several unconditionally secure device-independent quantum protocols have been proposed, even taking into account that the actual devices performing the Bell inequality tests may not be ideal (i.e. “noisy”).

Box 4.1: Device-independent quantum cryptography

Examples of this approach are Measurement Device-Independent QKD (MDI-QKD) and Twin-Field QKD (TF-QKD).

MDI-QKD was already proposed in 2012. In MDI-QKD, neither endpoint (sender or receiver) is configured as an optical receiver (as is done in conventional QKD protocols), but rather both endpoints are configured as optical transmitters. The two optical transmitters send photons to an intermediate node, called mid-station, which couples and measures the photons using Bell inequality testing. The endpoints can distil a shared secret key from the two-photon interference measurement results disclosed by the mid-station. The MDI-QKD protocol is protected against a malicious attempt by someone compromising the mid-station to gain information about the secret key because the legitimate endpoints can always detect any attempt to alter the correct operation of the mid-station, as this would manifest as a form of regular eavesdropping. In MDI-QKD it is no longer necessary to take special measures to protect optical receivers of endpoints from outside attacks. The focus shifts to protecting the optical transmitters of endpoints (where the optical pulses are prepared locally by a trusted user), which is much easier than protecting the optical receivers of endpoints (where optical pulses are received from the outside, prepared by

someone who is potentially untrusted and possibly interested in breaking the security of the system). MDI-QKD also makes it possible to implement multiparty QKD networks (star topology).

The advantage of TF-QKD, compared to MDI-QKD, is that it is designed to generate key bits from single-photon interference in the intermediate node, thus removing the need to remedy photon losses via sophisticated techniques. TF-QKD was introduced in 2018 and it was then shown that the secret key generation rate of the TF-QKD protocol was optimal on 550 km of standard optical fibre. The theoretical result was confirmed in an experimental demonstration. One of the further developments in terms of achieving still higher cryptographic key generation rates at such long distances is the Sending-Not-Sending (SNS) version of the TF-QKD protocol. In 2021, a research team in China developed an experimental TF-QKD system that tolerates a channel loss beyond 140 dB across a distance of 833.8 km, a new record for fibre-based QKD.

QKD security relies on the fundamental laws of quantum mechanics and has provable information-theoretic security. In contrast, classical public-key cryptography used for cryptographic key establishment relies on the computational difficulty of certain hard mathematical one-way functions, without any proof that these one-way functions cannot be reversed. In principle, the security of QKD protocols can be proven mathematically without imposing any restrictions on the abilities of an eavesdropper, something which is not possible with classical key exchange schemes; this is often referred to as “information-theoretic” or "unconditional security". In practice, however, QKD protocol implementations are only conditionally secure, dependent on a key set of assumptions, including:

- the laws of quantum mechanics apply;
- sender and receiver can securely authenticate each other;
- a single photon-source is used (for DV-QKD);
- there are no differences in photon detector efficiency.

QKD protocol implementations must ensure that the quantum mechanics properties on which their unconditional security relies are not compromised in any way; this is however easier said than done.

An inherent important drawback of QKD is that it relies on mutually authenticated message exchange over the classical communication channel, to thwart man-in-the-middle attacks.

Theoretically, DV-QKD technology assumes a single-photon source, which is very difficult to implement. Most currently available discrete variable QKD implementations therefore use faint laser sources, which are multi-photon sources. This opens a pathway for eavesdropper attacks, called Photon Number Splitting (PNS) attacks. An eavesdropper can split the multi-photon source of the sender and retain one photon for itself. The other photons are then transmitted to the receiver without leaving any trace that eavesdropping took place.

Various techniques have been developed to counter the PNS threat. For example, with the decoy-state technique the sender transmits each photonic qubit using a random light intensity. When

the quantum transfer is completed, the sender publicly announces the intensity used to send each of the photonic qubits. A PNS attack will reduce the intensity of the photonic qubits at the receiver end, which allows for detection of PNS attacks by monitoring the bit error rate associated with each intensity level.

The photon detectors which are used in QKD devices are tuned to detect incoming photons during a very short time window (just a few nanoseconds). Due to variances in manufacturing, there will always be differences between the photon detectors and their respective detection windows will be shifted by some small but finite amount. An eavesdropper can take advantage of this by first capturing a photon sent by the sender and then generating a “fake” photon that is sent to the receiver. The eavesdropper manipulates the phase and timing of the faked photon in such a way that it prohibits the receiver from detecting the eavesdropping. The only way to eliminate this vulnerability is to eliminate differences in photon detector efficiency, which is practically impossible (nonzero manufacturing tolerances always result in optical path length differences, wire length differences, etc.).

There are several other known attacks on QKD systems, including:

- side-channel attacks (to gain information from the leakage);
- trojan-horse attacks (probing the equipment with light to gain information about device settings);
- imperfect encoding attacks (initial states that do not conform to the protocol);
- multi-photon emission attacks (emitting more than one photon in a pulse so that information is redundantly encoded on multiple photons);
- phase correlation attacks (information leakage by non-phase-randomised pulses);
- bright-light attacks (manipulating the photon detectors with bright light);
- back-flash attacks (learning which photon detector clicked and hence know the corresponding bit value);
- efficiency mismatch and time-shift attacks (partially controlling which photon detector will click, to obtain information on the encoded bit) and manipulation attacks of the local oscillator reference).

For each of these attack categories, specific countermeasures have been devised. However, second-generation attacks (e.g. the use of very bright laser light to damage components within a QKD system) target these countermeasures themselves and therefore need to be addressed as well.

In addition to the various quantum attacks described above, QKD implementations are vulnerable to classic attacks on their components. The exact nature of such attacks is highly dependent on the QKD use case and on its operational environment.

An interesting research area is so-called Device-Independent QKD (DI-QKD), where the correctness of the quantum exchange part of the QKD protocol (based on entangled photons and

Bell inequality self-testing) is assured without any assumption whatsoever about the device being used. MDI-QKD and TF-QKD (see above) can be considered to constitute partly DI-QKD solutions.

Appendix A - References

[Springer 2021] Quantum Key Distribution: An Introduction with Exercises

[ETSI 2018]
Implementation Security of Quantum Cryptography - Introduction, challenges, solutions

[NOREA 2024] Random Number Generation

[npj 2022] Finite key effects in satellite quantum key distribution

Appendix B - Acronyms and abbreviations

aka	also known as
ANN	Artificial Neural Network
B92	Bennett 1992
BB84	Bennett and Brassard 1984
BBM92	Bennett, Brassard and Mermin 1992
bit	binary digit
CV	Continuous Variable
CV-QKD	Continuous Variable Quantum Key Distribution
dB	decibel
DI-QKD	Device-Independent Quantum Key Distribution
DPR	Distributed Phase Reference
DPR-QKD	Distributed Phase Reference Quantum Key Distribution
DV	Discrete Variable
DV-QKD	Discrete Variable Quantum Key Distribution
E91	Ekert 1991
e.g.	exempli gratia
EPR	Einstein-Podolsky-Rosen
etc.	et cetera
ETSI	European Telecommunications Standards Institute
FSO	Free-Space Optical
GG02	Grosshans and Grangier 2002
H	Horizontal

i.e.	id est
km	kilometre
laser	light amplification by stimulated emission of radiation
LDPC	Low-Density Parity-Check
MDI-QKD	Measurement Device-Independent Quantum Key Distribution
npj	*N*ature *P*artner *J*ournals
P&M	Prepare & Measure
PLOB	Pirandola-Laurenza-Ottaviani-Banchi
PNS	Photon Number Splitting
PRF	Pseudo-Random Function
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
QRNG	Quantum Random Number Generator
qubit	quantum bit
SARG04	Scarani, Acin, Ribordy and Gisin 2004
SNS	Sending-Not-Sending
SSP99	Six-State Protocol 1999
TF-QKD	Twin-Field Quantum Key Distribution
TPM	Tree Party Machine
UHF	Universal Hash Function
V	Vertical
WCA	Wegman-Carter Authentication

WML	Winnow Machine Learning