International Telecommunication Union

ITU-T Technical Report

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(24 November 2021)

ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N)

Technical Report FG QIT4N D2.3

Quantum key distribution network protocols: Quantum layer

(Pre-published version)

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

Quantum information technology (QIT) is a class of emerging technology that improves information processing capability by harnessing principles of quantum mechanics which is expected to have a profound impact to ICT networks.

The ITU Telecommunication Standardization Advisory Group established the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N) in September 2019 to provide a collaborative platform to study the pre-standardization aspects of QITs for ICT networks.

The procedures for establishment of focus groups are defined in Recommendation ITU-T A.7.

Deliverables of focus groups can take the form of technical reports, specifications, etc., and aim to provide material for consideration by the parent group in its standardization activities. Deliverables of focus groups are not ITU-T Recommendations.

FG QIT4N concluded and adopted all its Deliverables as technical reports on 24 November 2021.

Number	**Title**
FG QIT4N D1.1	QIT4N terminology: Network aspects of QITs
FG QIT4N D1.2	QIT4N use cases: Network aspects of QITs
FG QIT4N D1.4	Standardization outlook and technology maturity: Network aspects of QITs
FG QIT4N D2.1	QIT4N terminology: QKDN
FG QIT4N D2.2	QIT4N use cases: QKDN
FG QIT4N D2.3	QKDN protocols: Quantum layer
FG QIT4N D2.3	QKDN protocols: Key management layer, QKDN control layer and QKDN management layer
FG QIT4N D2.4	QKDN transport technologies
FG QIT4N D2.5	QKDN standardization outlook and technology maturity

The FG QIT4N Deliverables are available on the ITU webpage, at https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx.

For more information about FG QIT4N and its deliverables, please contact tsbfgqit4n@itu.int.

Summary

This technical report is a deliverable of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N) which studies and reviews protocols in the quantum layer of a quantum key distribution network (QKDN). It mainly focuses on quantum key distribution (QKD) protocols in the quantum layer, where QKD is an essential part of the QKDN and is an emerging technology expected to strengthen the security of the current communication network.

This technical report endeavours to give an overall review of the QKD protocols, including different types of QKD protocols, their workflows, protocol features, parameters, commercialization status. For this reason, it briefly discusses the security of QKD, specifically the security of protocols in their relation to real world QKD systems. More generally, this technical report discusses the potential of integration of QKD in future networks and provides an overview of considerations and suggestions for future work on QKDN protocols.

Keywords

QKD; quantum key distribution; quantum key distribution network; protocols

Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

Disclaimer

Sample projects, reference articles, specific companies, products or services mentioned in this report are only for the purposes of technical analysis. Their mention does not imply that they are endorsed or recommended by ITU, ITU's Secretariat, the Focus Group or the editors of this report, in preference to others of a similar nature that are not mentioned.

Chief editor:	Hao Qin National University of Singapore Singapore	Email: hao.qin@nus.edu.sg
Co-editors:	Peng Huang Shanghai Jiao Tong University China XT Quantech	Email: huang.peng@sjtu.edu.cn
	Hongyu Wu QuantumCTek China	Email: hongyu.wu@quantum-info.com

Acknowledgments

The editors express their appreciation to all participants of Working Group 2 of the Focus Group on Quantum Information Technology for Networks (FG QIT4N) for their invaluable inputs, thorough review and all comments provided during the development of this report. Appreciation is also given to all the contributors of this report including but not limited to: Momtchil Peev (Huawei Technologies Duesseldorf GmbH (HWDU), Germany), Yingming Zhou (Shanghai XT Quantech Co. Ltd, China), Jiajun Ma (QuantumCTek Co., Ltd. China) and Yichen Zhang (Beijing University of Posts and Telecommunications, China).

CONTENTS

Page

Technical Report ITU-T FG QIT4N D2.3

Quantum key distribution network protocols: Quantum layer

1 Scope

This Technical Report studies and reviews protocols and their security in the quantum layer of quantum key distribution networks (QKDNs). In particular, the scope of this technical report covers aspects of different types of quantum key distribution (QKD) protocols and their security, the protocol workflows, features and parameters, the commercialization status of QKD systems, the potential of integrating QKD in future networks as well as considerations and suggestions for future work on QKDN protocols.

2 References

[ITU-T Y.3800] Recommendation ITU-T Y.3800 (2019), *Overview on networks supporting quantum key distribution*.

[ITU-T Y.3801] Recommendation ITU-T Y.3801 (2020), *Functional requirements for quantum key distribution networks.*

[ITU-T Y.3802] Recommendation ITU-T Y.3802 (2020), *Quantum key distribution networks - Functional architecture*.

3 Terms and definitions

This Technical Report uses QKDN related terms defined in [b-QIT4N D2.1].

4 Abbreviations and acronyms

This technical report uses the following abbreviations and acronyms:

CV	Continuous-Variable
DI	Device Independent
DV	Discrete-Variable
EB	Entanglement Based
GMCS	Gaussian Modulation Coherent State
ITS	Information-Theoretic Security
MDI	Measurement Device Independent
OTP	One-Time Pad
P&M	Prepare-and-Measure
PNS	Photon-Number-Splitting
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
QKDN	QKD Network
RNG	Random Number Generation
SPD	Single Photon Detector
TF	Twin Field

5 Introduction

The term “protocol” is a very broad concept which generally refers to a list of steps to be performed by participating entities to reach their goal [b-ETSI GR QKD 007]. In the context of quantum key distribution networks (QKDN), different kinds of protocols are involved, in which only the quantum key distribution (QKD) protocol is a relatively new concept to standards developing organisations (SDOs).

A cryptographic protocol is an abstract or concrete protocol that performs a security-related function and applies cryptographic methods [b-Dong] and as it will be shown in this report, QKD protocols [b-ITU-T X.1710] own features of cryptographic protocols. A QKD protocol can be recognized as a key establishment protocol where two remote parties negotiate a secret symmetric key following a step-by-step procedure, in which every step is security concerned. Unlike classical solutions based on algorithms, QKD protocols need to be implemented using dedicated hardware to transmit quantum states through physical channels and software to post process classical information to output random bits as keys. In this sense, a QKD protocol can also be considered as a kind of communication protocol, where a communication protocol is a system of rules that allow two or more entities of a communication system to transmit information through any kind of variation of a physical quantity [b-Popovic]. This technical report aims to introduce QKD protocols in the background of QKDN and provide some perspectives for standardization.

QKD is one of the most important outputs of quantum information science that is reaching a level suited for real life realization. This technology has already been made commercially available and has been deployed in test and production environments. QKD allows two remote parties, a sender (known as Alice) and a receiver (known as Bob), to establish a secret key over a quantum channel.

Under a number of assumptions, the key establishment process is guaranteed to be secure against unbounded adversaries. This, in principle, makes QKD protocol a key establishment scheme with information-theoretic security (ITS) that has been proposed and widely addressed to date.

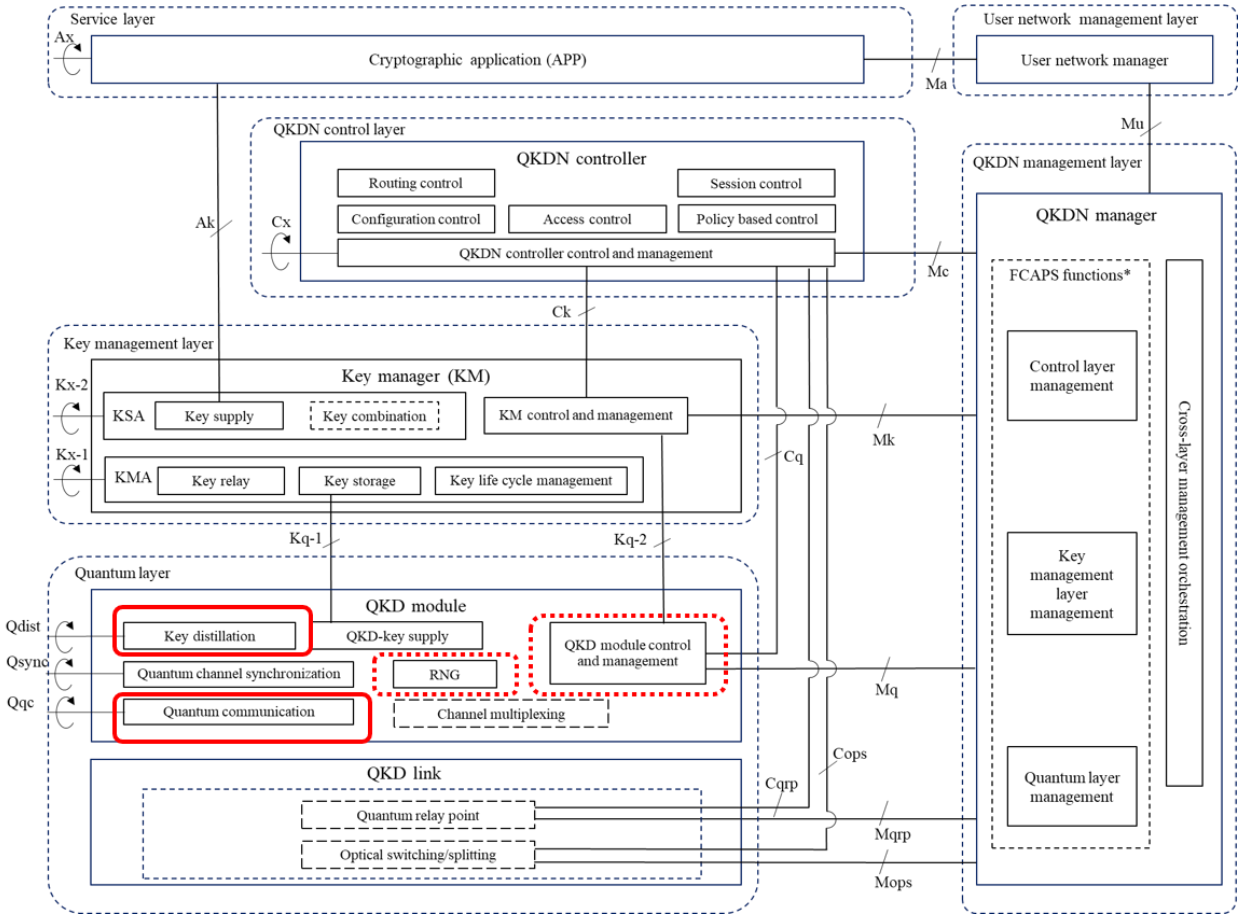
The BB84 protocol, developed by Charles Bennet and Gilles Brassard in 1984, was the first QKD protocol to be invented [b-Bennett-1] and has been widely studied and implemented in various commercial QKD systems. Since then, many other QKD protocols have been developed and experimentally demonstrated with some being implemented in commercial products and deployed in QKDNs. Despite these efforts and the progress made in QKD protocol development, none of these protocols are standardized. Majority of the existing QKD protocols are currently available in various reported versions from literature and the industry while the procedures of implementing them can only be found in literature. To promote the deployment of QKDNs and foster the growth of industry, it will be beneficial to have well-studied and widely deployed QKD protocols that are standardized in normative language – especially in a subsequent phase when component and subsystem level interoperation will be expected.

Even now, a task of paramount importance is to enable and to facilitate the security certification and evaluation of commercial QKD systems to bring confidence on the security targets to potential customers; QKD protocol standardization can help and facilitate such progress. In classical cryptography, many public key and symmetric key-based cryptographic protocols have been standardized [b-FIPS PUB 197], [b-ISO/IEC 18033-3] and [b-RFC8017], which is usually considered as the very first step towards security certification.

This report aims to give an overall review of QKD protocols, along with their features and parameters from the perspective of standardization. Although there are a large number of QKD protocols existing in literature, many of them were not attractive for commercial purposes at the time this report was written. This report focuses on QKD protocols that have been commercialized or, from the authors' point of view, have potential to be commercialized in the near future. This report follows the prepare & measure (P&M) paradigm and uses the classical cryptographic jargon of the actors i.e., Alice who refers to the QKD transmitter, Bob who refers to the QKD receiver and Eve refers to the attacker (Eve's name comes from the similarly sounding eavesdropper). Additional parties named either Charlie or Fred who may function as a QKD transmitter or receiver may also be used where appropriate.

Noting the large number of research review papers that cover a much wider scope on QKD protocols, this report intends to focus on the basic concepts and introduce QKD protocols in the context of standardization and not repeat contents that have already been discussed.

NOTE – For more technical details on QKD protocols, interested readers can refer to widely recognized review papers [b-Gisin-1] and [b-Scarani-1] and recently published papers with up-to-date information [b-Diamanti], [b-Pirandola-1] and [b-Xu].



NOTE - The scope of this report covers key distillation and quantum communication module (solid red line); parameters reported to QKD control and management module and assumption for RNG (dotted red line).

Figure 1: Functional architecture model of QKDN [ITU-T Y.3802]

6 Protocols in the quantum layer of a QKDN

A typical QKDN consists of several layers; namely, the quantum layer, key management layer, QKDN control layer, QKDN management layer and the service layer, see Figure 1 [ITU-T Y.3802].

Compared to traditional communication networks, the quantum layer is unique to QKDN. In the quantum layer, QKD protocols are implemented in QKD modules and symmetric keys are established through point-to-point QKD links. This technical report mainly focuses on QKD protocols in the quantum layer of QKDN and reviews their security while the classical layers are reviewed in [b-QIT4N D2.3 2].

In the quantum layer of a QKDN, the main protocols involved are QKD protocols which establish symmetric keys between two trusted nodes. Other protocols and interactions may also be involved to assist the QKD process and QKDN operations such as synchronization protocols. As specified in the functional architecture model of QKDN, see Figure 1 of [ITU-T Y.3802], the quantum layer mainly consists of QKD modules and QKD links, along with several interfaces and other layers. Each box as a functional element inside QKD modules and links has been detailed in [ITU-T Y.3802].

A QKD protocol is realized inside the QKD module, specifically in the "Qqc" interface of the quantum communication function box and the "Qdist" interface of the key distillation function box which are referred as the quantum channel and classical channel, respectively, see Figure 1. The source of randomness for the quantum communication and key distillation functions is the random number generation (RNG) function box, see Figure 1.

NOTE – While the assumption of RNG in QKD protocols is discussed in this report, RNG protocols and other aspects of RNG are outside the scope of this report and are not discussed.

The QKD module control and management function is responsible for the overall control and management of the functional elements in the QKD modules and communicates with functions in other layers. Several parameters of QKD protocols in the channel status are needed to be transferred to this function box and then sent through difference interfaces. This report specifies the parameters of each QKD protocol, however, the interaction protocols of the QKD module control and management function with other layers is covered in [b-QIT4N D2.3 2]. Similarly, the QKD-key supply function box receives QKD-key requests from a key management agent (KMA) and supplies QKD-keys to the KMA, which involves another classical protocol discussed in [b-QIT4N D2.3 2].

The other function boxes in the quantum layer i.e., the quantum channel synchronization and optional channel multiplexing in the QKD module and, in the QKD link, the optical switching/splitting function and the optional quantum relay link are referred to as QKDN transport technologies which is composed of the physical layer and where the implementations of QKD protocols take place. In the QKD module, the quantum channel synchronization function box provides clock and timing synchronization for the quantum channel with adequate precision to support quantum signal transmission and measurement. The optional channel multiplexing function box enables the wavelength division multiplexing of quantum and classical channels. In the QKD link, the optical switching/splitting function enables the switching or splitting of quantum channel traffic and synchronization signal; while the optional quantum relay point function box serves as an untrusted intermediate point in the QKD link as required by the QKD protocol to extend the QKD distance, such as with measurement-device-independent (MDI) and twin field (TF) QKD protocols, which will both be discussed later.

As outlined in Figure 1, it is important to take note that the focus of this technical report is limited to the core protocols in the quantum layer of the QKDN, i.e., QKD protocols, which includes the quantum communication and key distillation function boxes, as well as the relevant parts of the RNG

and QKD module control and management function boxes. Other possible involved protocols and interaction mechanisms in the quantum layer are discussed elsewhere.

7 General aspects of a QKD protocol

Since the development of the BB84 protocol (the first QKD protocol) in 1984, many new QKD protocols have been proposed in the past few decades. The motivation for developing new QKD protocols have been mainly to:

- improve QKD performance: key rate and distance
- reduce implementation complexities and device requirements
- improve QKD theoretical and implementation security level

There could be hundreds, or more, of QKD protocols that have been proposed by the research community, however, only a few are well studied and have been implemented in experiments. Although they differ in their detailed steps, QKD protocols generally follow the same pattern in the workflow and this Clause presents the general workflow of a QKD protocol and classifies QKD protocols in different ways.

7.1 Workflow

There are two main stages in a QKD protocol: the raw key exchange stage (also known as quantum communication stage) and classical post-processing stage. The raw key exchange is carried through the quantum channel while the classical post-processing is carried through the classical (authenticated – see below) channel. This general procedural description can apply to all kinds of QKD protocols while the specific steps vary in different QKD protocols.

7.1.1 Raw key exchange

The raw key exchange can be done following a prepare-and-measure (P&M) scheme:

- **Step 1:** Alice encodes classical information on the quantum states. In particular, she encodes a classical random variable *a* on a set of non-orthogonal quantum states.
- **Step 2:** Alice then sends these quantum states through a communication channel (the quantum channel) to Bob.
- **Step 3:** At the output of the quantum channel, Bob measures the received quantum states to obtain a classical random variable *b* which is partially correlated with the random variable *a* of Alice.
- **Step 4:** By repeating this process, Alice and Bob exchange a significant number of quantum states and generate two sets of partially correlated data on each side. These two sets of data are called the *raw key*.

Note that the quantum states are realized by physical systems in the quantum regime (typically very weak signals) whereby a perfect cloning of an arbitrary unknown quantum state is forbidden and is at the heart of QKD security.

The raw key exchange can also be realized through the entanglement-based (EB) or the MDI schemes, in which more advanced techniques such as entangled photons generation and Bell state measurements are involved. Some of these schemes have attractive advantages in terms of

performance and security enhancement but are also faced with technological challenges. Nevertheless, both academia and the industry are in progress to commercialize these technologies.

7.1.2 Classical post-processing

After raw key exchange, Alice and Bob progress to the second stage of a QKD protocol, the classical post-processing, where they process their raw key (partially correlated and partially secret bit strings) by exchanging information over a classical channel. This stage consists of the following steps:

– **Step 1: Sifting**: Alice and Bob exchange classical message to indicate which orthogonal subsets of *a* have been used in preparation (typically basis or quadrature) have been used for the encoding or the measurement in the raw key exchange stage. The two parties then discard the part of the raw key for which encoding, and measurement basis are inconsistent. What they keep is called the *sifted key*.

– **Step 2: Parameter estimation**: Alice and Bob compare a random subset of their sifted key and estimate their statistics to know different parameters of the quantum channel: e.g., channel transmission and quantum bit error rate (QBER) – QBER refers to the fraction of non-identical bits between Alice's and Bob's sifted key bit strings. Based on such parameter estimation, Alice and Bob can estimate the mutual correlation between their sifted key and compute an upper bound of information that is accessible to an eavesdropper (Eve) for a given attack model. Concerning a particular security proof, if the upper bound of Eve's information is higher than Alice and Bob's mutual information (a measure of the mentioned correlation), then no secret key can be generated, for which reason Alice and Bob abort the QKD protocol. Otherwise, they proceed to the next step.

– **Step 3: Error correction (information reconciliation)**: In this step, Alice and Bob agree on an identical bit string by using classical error correction techniques. Information reconciliation can be realized by Bob sharing a key identical to Alice's data (direct reconciliation) or by Alice sharing a key identical to Bob's data (reverse reconciliation). After error correction, the partially correlated key of Alice and Bob becomes fully correlated but some information may be leaked to Eve in all preceding steps or during transmission over the quantum channel.

– **Step 4: Privacy amplification:** In this step, Alice and Bob process the correlated key output from error correction to eliminate the information of the key that Eve may have. Here the fraction of the key that needs to be discarded is based on the upper bound information of Eve as computed in the parameter estimation for direct or reverse reconciliation with a given security proof. After removing the corresponding fraction of the key, Alice and Bob have an identical *secret key* which is fully unknown by Eve up to negligible ε failure probability (ε, see Clause 8). Usually in this step, two universal hash functions are used.

– **Additional steps:** Some protocols feature additional steps such as pre-processing, advantage distillation, post-selection etc. However, these additional steps can be typically subsumed in the four general steps outlined above.

7.2 Categories of QKD protocols

QKD can be implemented using many different protocols and there are several approaches that can be used to classify QKD protocols. Classification could be done based on:

a) the sending and measurement settings as in the raw key exchange e.g., prepare-and-measure (P&M), measurement device independent (MDI) and entanglement based (EB) schemes.

b) whether the QKD devices are trusted or not e.g., device dependent QKD protocols, device independent (DI) QKD, and one-sided DI QKD (including MDI and source independent) protocols.

c) the direction of communication e.g., two-way QKD for bi-directional quantum information exchange and one-way QKD when quantum information is sent from one to another.

d) the different encoding and decoding methods i.e., discrete-variable (DV)-QKD and continuous-variable (CV)-QKD. This is the most common approach to classify QKD protocols and the two schemes differ as follows:

   i) In DV-QKD schemes, the sender typically encodes information with discrete variables of finite dimension such as phase, polarization or time bin of single photons and the receiver uses single photon detectors (SPDs) to decode information.
   Some examples of DV-QKD schemes include BB84 protocol [b-Bennett-1], E91 protocol [b-Ekert], B92 protocol [b-Bennett-2], six-state protocol [b-Bruß], BBM92 protocol [b-Bennett-3], SARG04 protocol [b-Scarani-2], coherent-one way protocol [b-Gisin-2] and [b-Stucki], DPS protocol [b-Inoue-1] and [b-Inoue-2], RRDPS protocol [b-Sasaki-1] and [b-Zhang-1], Twin-Field protocol QKD [b-Lucamarini] and [b-Ma], DV MDI protocol [b-Lo-1], [b-Braunstein] and DI QKD protocol [b-Acín].

   ii) In CV-QKD schemes, the sender typically encodes information using the position and momentum quadrature of a quantized electromagnetic field in an infinite dimensional Hilbert space. The receiver then uses the coherent detection such as homodyne or heterodyne detection to decode information.
   Some examples of CV-QKD schemes include Gaussian-modulation-based CV protocol [b-Grosshans-1], discrete-modulation-based CV protocol [b-Silberhorn, b-Ralph], [b-Lin] and CV-MDI protocol [b-Pirandola-2].

8 Security of QKD protocols

In this clause, some important security aspects of QKD protocols will be briefly addressed.

A QKD protocol is a set of steps to establish a key [b-ITU-T X.1710]. In the context of a mathematical system model based on the theory of quantum mechanics some QKD protocols can be proven to be ITS, or more precisely composably ε-secure as outlined below. The property of composability means that QKD protocols need not be considered in isolation and can be combined with other composably ε-secure protocols to yield wider security frameworks.

In the real world, it is QKD implementations that are important. QKD protocol security does not automatically imply security of a QKD implementation (models can never capture the full complexity of real implementations) but they are intimately related. Such issues are the subject of intensive study at present as briefly outlined below.

8.1 The notions of security of QKD protocols

Security proofs of QKD protocols were initially established under the assumption that legitimate parties (Alice and Bob) can perform infinite runs of the protocol and thus hold an infinite quantity of

exchanged data to distil the key. This is often referred to as *asymptotic analysis*, giving rise to an *asymptotic key rate*. This obvious idealization neglects statistical deviations and a failure probability related to the finite runs of the protocol. A study of *finite size* effects can take this into account to determine the secure secret key rate. This requires extensive and non-trivial analysis called *finite size analysis*. The security proofs for some QKD protocols have not yet been extended to a finite size analysis. In fact, this "feat" has been accomplished in only a few cases.

Further, a rigorous finite size analysis is in fact based on *composability* and ε-*security*. The latter concepts have been introduced to QKD in [b-Ben-Or] and [b-Renner] and are nicely summarized in [b-Müller-Quade] (see also [b-Portmann]).

"A QKD protocol is ε-secure as it is ε-indistinguishable from a (hypothetical) ideal one, which is perfectly secure."

Two ε-secure protocols (with ε' and ε", respectively) are composable if they can be combined to a joint ε-secure protocol with $\varepsilon \leq \varepsilon'+\varepsilon''$. This implies that the combination has a well-defined security and that composable ε-secure protocols can be stacked together like building blocks. There exist QKD protocols (typically the ones for which finite size analysis has been successfully performed) that are known to be composably ε-secure [b-Müller-Quade] but not all QKD protocols are known to be composably ε-secure. Composability is a powerful characteristic that enables the security of end-to-end protocols of complex cryptographic applications to be rigorously analysed. An important example is that QKD protocols require authentic classical communication. However, this is not a deficiency of QKD (as often claimed citing the fact that there is no good reason to assume authenticity of classical communication) as composability allows the utilization of other well-established protocols to enable ε-security in completely untrusted environments [b-Müller-Quade].

The security proof of a QKD protocol starts from a set of assumptions and derives a composable ε-security statement. These assumptions range from very general, such as the validity of quantum mechanics, to the more specific, such as the validity of a certain model of some part of the protocol. If the requisite assumptions are satisfied, composably ε-secure QKD protocols are immune to any attacks by an arbitrarily powerful eavesdropper equipped with unlimited resources. A further discussion is given in [b-ETSI GS QKD 005].

8.2 Assumptions in the security proofs of QKD protocol

Based on quantum physics theory, QKD protocol security can be established independently of computational assumptions, which is often known as "unconditional security" or "ITS". Note that here the "unconditional" only refers to the computation power is not limited, which does not mean the security can be guaranteed under any condition. There are certain "conditions", also known as assumptions, that QKD protocols typically utilised in security proofs. These assumptions mainly include:

– **Assumption 1:** The classical channel communication must be authentic which means that Eve can listen but is not allowed to modify the messages exchanged between Alice and Bob on the classical channel without being detected. In another words, the information integrity is required to be protected on the classical channel. Note that the classical channel is public, there is no assumption on the confidentiality.

– **Assumption 2:** The random number generators used by Alice and Bob need to be truly random which means that the produced random bit string is unpredictable in principle.

– **Assumption 3:** The model, implicit in the QKD protocol is faithful. (If the protocol is implemented then the hardware and software the devices of Alice and Bob must exactly and only reproduce the functionality stated in the protocol description.)

– **Assumption 4**: Alice's and Bob's devices are security-wise isolated from the outside environment. Note that this condition is an implicit corollary of **Assumption 3**.

Achieving **Assumption 1** in practice is challenging as there are no natural authentic channels. Even though composability with ε-secure authentication protocols can be utilized for authentication, it should be noted that authenticated is not the same as an authentic channel. In the former, all sent messages must arrive. No authentication method can prevent messages from not being received.

Note that these conditions/assumptions are required from P&M schemes. Next generation protocols (such as DI, MDI and semi-DI QKD protocols) rely on a different version of **Assumption 3**.

8.3 Implementation security

In any modern cryptography it is universally assumed that Eve is able to get detailed comprehensive information on the devices of Alice and Bob. This follows *Kerckhoffs' principle* for cryptography primitives.

NOTE – Kerckhoffs' principle: Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi [b-Kerckhoffs].

The issue of implementation security is highly relevant for the practical applicability of QKD. The question in short is: *is it possible to realize QKD modules (appliances that utilize QKD protocols in their functionality) that are highly secure as a consequence of the security of QKD protocols?* An immediate question that arises is: *are the sufficient conditions for security (the assumptions), mentioned above, fulfilled in practical implementations or not*. Naturally, QKD devices might be highly sophisticated and not exclusively restricted to the execution of a "pure" QKD functionality but dedicated to a full-scale security framework, supported e.g., by the aforementioned composability feature of QKD protocols.

This is a theme that is of paramount importance to security practitioners [b-ETSI White Paper 27] and is therefore subject to intense on-going work. Examples are provided in [b-ISO/IEC 23837 CD2] and [b-ETSI PP]. While this work is still in progress there is little doubt that it will be completed successfully. QKD implementation security is not in the scope of this report. However, note that important aspects of this theme are attacks rooted in a mismatch between a simple idealized mathematical model that underlines a QKD protocol and a realistically relevant QKD module realization. The additional degrees of freedom in the latter could allow for *quantum hacking* attacks (also known as side channel attacks), including time shift attacks, blinding attacks, detector saturation attacks, spatial mode mismatch attacks, Trojan horse attacks and so on.

Among these attacks, the blinding attack [b-Gerhardt] and [b-Lydersen] is an important one as a bad implementation could affect all the non-MDI based QKD protocols in DV-QKD. Where single photon detectors (SPDs) can be forced to be operated in linear mode (no longer sensitive to a single photon level power) under relatively high-power light illumination, it can open up a chance for Eve to fully control the SPD detection results with strong (and classical) light pulses. There is also a CV-QKD version of the blinding attack [b-Qin-1] and [b-Qin-2], in which Eve attempts to control the homodyne detector measurement results by sending powerful light. To prevent these types of attacks

on systems using vulnerable detectors, legitimate parties need to e.g., monitor either the input light power on the detectors or the operating status of the detectors.

Threats to QKD modules mainly occur at the QKD link ports which are the interfaces of the QKD transmitter and the QKD receiver. Through these ports, the eavesdropper can try to send light into a QKD module to affect its internal components behaviour or detect light leakage which might carry key information from a QKD module, or even send probe light and detect its reflections to learn about key encoding information. Since a QKD link is an open channel for the QKD transmitter and receiver to exchange quantum signals, even if the internal components of a QKD module are protected by own security packages, the eavesdropper can still send or receive light through QKD link ports. More information on this theme can be referred to [b-ETSI White Paper 27] and [b-Xu].

On the other hand, even though attacks on QKD modules are feasible in principle, they are still difficult to implement in a realistic environment compared to the attacks that can be realized remotely with only digital signals. Quantum hacking attacks require access to the physical layer with optical signals to interrupt the QKD module process. The eavesdropper needs to physically connect or couple to the QKD link and establish a physical station in-between the two trusted nodes to launch her attack strategy. Moreover, so far, attacks have been only proven or demonstrated with the assumption of Kerckhoffs' principle in place, there has been no successful attack demonstrated yet with Eve have no internal information of Alice and Bob's devices, i.e., black box quantum hacking.

To counter potential implementation security loopholes, various approaches ranging from attack-excluding countermeasures in implementations to QKD protocol modifications are being put to use. The important point to underline here is that in contrast to the mathematical security of a QKD protocol, implementations of any cryptographic scheme can only be secure at any point of time to the best of our present knowledge (on device modelling). Loopholes are being efficiently closed in the framework of *QKD certification* (evaluating the level of practical security [b-ISO/IEC 23837 CD2] and [b-ETSI PP]). QKD-enabled communication security is based on different principles from techniques based around assumptions on attackers with limited computational resources and is a complimentary tool to help secure networks.

9 Introduction of discrete variable QKD protocols

9.1 Overview

DV-QKD protocols are QKD protocols that detect signal pulses with single-photon detectors. There are various types of DV-QKD protocols with a few examples and their general overview provided below.

a) BB84 protocol

As the first ever QKD protocol, the BB84 protocol [b-Bennett-1] is one of the most well studied and widely implemented QKD protocol. The protocol was originally designed to emit optical pulses with a perfect single photon source. This, however, proved challenging to engineer and an alternative approach of using an attenuated laser source was developed.

With this new approach, the protocol was observed to be vulnerable to the so-called photon-number-splitting (PNS) attack [b-Brassard] which dramatically reduced the key rate of the protocol. The decoy state method was proposed later as a solution to defeat the PNS attack. The key rate of the decoy-state-based version of the BB84 protocol [b-Hwang], [b-Lo-2] and [b-Wang-1], i.e., decoy state BB84, was then observed to approach the original BB84.

The BB84 protocol has been implemented in several QKD network testbeds such as the DARPA QKD network [b-Elliott], SECOQC QKD network [b-Poppe] and Tokyo QKD network [b-Sasaki-2]. It has also been demonstrated in a satellite-to-ground QKD experiment [b-Liao-1].

b) E91 protocol

The E91 protocol [b-Ekert] was the first QKD protocol that involves the use of quantum entanglement. This protocol detects information leakage by monitoring the violation of Bell inequality of data obtained by measuring the bipartite quantum states shared between the legitimate communication parties. It is, however, challenging to engineer an entangled-photon source which outputs high-fidelity entangled photon pairs with high repetition rate. Thus, the entangled-photon source is a bottleneck in implementing a high speed E91 protocol.

c) B92 protocol

B92 protocol [b-Bennett-2] can be considered as a simplified version of the BB84 protocol that transmits two non-orthogonal quantum states instead of four. The original B92 protocol transmitted two weak coherent pulses at different phases with a bright reference pulse, while a modified version of the protocol uses single photon pulses and removes the reference pulses. By comparison, the original B92 protocol is more robust against channel losses.

d) Six-state protocol

Six-state protocol [b-Bruß] can be considered as a revised BB84 protocol that uses six quantum states on three orthogonal bases instead of four states on two bases. The benefit of using extra quantum states is to make the protocol easier to detect information leakage and thus produces a higher key rate. On the other hand, the additional two quantum states and one orthogonal basis increase the complexity of the system.

e) BBM92 protocol

BBM92 protocol [b-Bennett-3] can be considered as an entanglement-based version of BB84 protocol. It detects information leakage by monitoring the correlation of the data obtained by measuring the bipartite quantum states shared between the legitimate communication parties which are ideally supposed to be entangled.

Due to its use of passive optical elements, BBM92 is naturally resistant against Trojan Horse attacks that attempt to probe the status of active elements to gain information about the prepared state [b-Gisin-3]. BBM92 does not require a decoy state implementation as it is relatively straightforward to distribute single-photon states using entangled photon pairs -- one to each remote party using spontaneous parametric down-conversion (SPDC).

The BBM92 protocol was implemented in the SECOQC QKD network testbed [b-Poppe] and Tokyo QKD network testbed [b-Sasaki-2].

f) SARG04 protocol

SARG04 protocol [b-Scarani-2] can be considered as a revised BB84 protocol with a different information encoding/decoding rule. By this revision, the protocol is more robust against the PNS attack than the original BB84 protocol (without using the decoy state method) when attenuated laser pulses are used.

The SARG04 protocol has been demonstrated in the Tokyo QKD network testbed [b-Sasaki-2].

g) COW protocol

The coherent-one-way (COW) protocol [b-Gisin-2] and [b-Stucki] is designed by sending a sequence of weak coherent optical pulses that share a common phase. The protocol detects the information leakage by monitoring the visibility of interference of the optical pulses. The protocol is experimentally simple to implement and, to some extent, intrinsically robust against the PNS attack.

The COW protocol was demonstrated in the SECOQC QKD testbed networks [b-Poppe].

h) DPS protocol

The differential-phase-shift (DPS) protocol [b-Inoue-1] and [b-Inoue-2] is designed by sending a sequence of weak coherent optical pulses with common intensity, while the information is carried by the relative phase between adjacent pulses. The protocol has similar features to the COW protocol, i.e., simple to implement and robust against the PNS attack.

The DPS protocol was demonstrated in Tokyo QKD testbed networks [b-Sasaki-2].

i) RRDPS protocol

The round-robin-differential-phase-shift (RRDPS) protocol [b-Sasaki-1] can be considered as a revised version of the DPS protocol with the original fixed optical delay line replaced by a variable one. Although this revision increases the complexity of the system, a prominent feature of this protocol is that the information leakage estimation does not depend on the bit error rate, but only on the protocol's configuration parameters. This feature bestows the protocol a better tolerance of bit errors and the finite-sized-key effects.

j) MDI-QKD protocol (discrete variable)**:**

Measurement-device-independent QKD (MDI-QKD) protocol [b-Lo-1] and [b-Braunstein] was proposed to remove all the security requirements of the measurement module. This protocol involves two transmitters with one receiver between them. As a typical setting of the DV-based MDI-QKD protocol, the transmitters encode information in a similar way as the BB84 protocol, while the receiver performs a joint Bell-state measurement on the states received from the two transmitters. MDI QKD is an effective solution to defeat all kinds of detector-based attacks in the QKD receiver.

k) TF-QKD protocol

Twin-field quantum key distribution (TF-QKD) protocol [b-Lucamarini] is an MDI-type QKD protocol. Thus, it removes all security requirements on the receiver module but, in comparison, TF-QKD protocol is based on single-photon interference instead of two-photon interference as in conventional DV-MDI-QKD protocols. This revision enables the protocol to break the fundamental point-to-point key rate bounds that apply to most QKD protocols.

l) DI-QKD protocol (discrete variable)**:**

In contrast to the MDI-QKD protocol that removes all security requirements on the QKD receiver, the DI-QKD protocol [b-Mayers], [b-Barrett] and [b-Acín] was developed to remove most of security requirements on both the QKD transmitter and receiver while a small number of security requirements remain such as no information leakage.

DV based DI-QKD can be considered as a revised E91 protocol with different measurement settings and post-processing method. Like the E91, the DI-QKD protocol detects information leakage via monitoring the violation of Bell inequalities.

9.2 Decoy state BB84 protocol

9.2.1 Workflow

Quantum communication stage

- **Step 1: Quantum state preparation:** Alice prepares quantum states as carriers of key information. It mainly includes bases selection, states preparation, and pulse intensity modulation (decoy state modulation). Alice and Bob select two sets of orthogonal bases (encoding basis for Alice and measurement basis for Bob) in the two-dimensional Hilbert space, and the two sets of bases are conjugate to each other. Each set of bases contains two orthogonal quantum states; therefore, four quantum states will be prepared at the transmitter. The short pulse emitted by weak coherent pulse source is used as carrier of information and combined with intensity modulation to achieve decoy state. Taking the commonly used three-intensity decoy-state protocol as an example, the quantum state pulse can be modulated into three different intensities, which can be used as the signal state, the decoy state, and the vacuum state (which is another decoy state with zero intensity), respectively.
- **Step 2: Information encoding:** Alice randomly loads the quantum state used to encode the key information on the corresponding pulse. Firstly, according to the random number sequence, the quantum states that need to be encoded on the light pulse are determined through the relation between the binary bits 0, 1 and the quantum states. Then, based on the determined quantum state information, the quantum state used to encode the key information is modulated onto the corresponding pulse, while the binary bits information loaded on the quantum state is saved.
- **Step 3: Quantum state transmission:** Alice sends quantum state pulse loaded with key information to Bob through quantum channel such as optical fibre or free space, and Alice records the intensity of the emitted pulse and encoded key information.
- **Step 4: Quantum state measurement:** Bob's raw key acquisition includes detection and decoding. Bob first randomly selects a measurement basis to measure the pulses loaded with quantum states from transmitter, then detects the demodulated photon signal in the single photon detectors (SPDs) and records these detectors' response to get raw key.

Classical post-processing stage

- **Step 1: Sifting:** This is comparison between the encoding basis used by the transmitter and the measurement basis used by the receiver. Only the key with the same basis used in the transmitter and receiver will be retained to generate the sifted key.
- **Step 2: Error correction:** First, parameter estimation, also known as bit error estimation, is performed. This analyses the sifted key to estimate the quantum bit error rate (QBER). Afterwards, the quantum bit errors in sifted key at both parties are corrected by using certain algorithm to obtain consistent key, which is corrected key.
- **Step 3: Privacy amplification:** This refers to a process in which the transmitter and receiver perform mathematical processing on the corrected key to eliminate information that eavesdroppers may have and extract the final secret key.

Parameters reported to other layers

– Quantum channel status: QBER, channel loss, estimated secret key rate

– QKD module status: decoy state setting, output raw key rate, output secure secret key rate

NOTE – Other layers refer to the layers identified in Figure 1.

9.3 BBM92 protocols

9.3.1 Workflow

Quantum communication stage

– **Step 1: Quantum state preparation/generation:** The BBM92 protocol involves distributing entangled photon pairs [b-Bennett-3], one photon in each pair to each party, and uses the correlations of the measurement results (Step 3) between the two parties to establish a symmetric key. Such entangled photon states are commonly generated using SPDC. The entangled photon pair state can be prepared with only passive optical elements and does not rely on active optical elements that prepare a specific quantum state to be transmitted in every round.

– **Step 2: Quantum state transmission:** Entangled photon pairs are distributed over free space or optical fibre networks to Alice and Bob. With polarization-encoding, polarization states are used as quantum bits. In the scenario where optical fibres are used, undesired polarization rotation, due to time-varying birefringence imposed by fluctuations in temperature and mechanical stress, must be compensated for to ensure that the desired state is distributed.

– **Step 3: Quantum state measurement:** Alice and Bob's raw key acquisition includes detection and decoding. In the scenario where polarization-encoding is used, both parties may use passive optical elements to select a polarization-basis for measurement, e.g., a beam-splitter can be used to direct the photon randomly to measurement apparatus that measures in either one of two mutually unbiased bases (horizontal/vertical or +45°/-45°).

Classical processing stage

– **Step 1: Sifting:** Comparisons are made between the encoding polarization bases used by Alice and Bob. Only raw keys measured under the same basis by both parties will be retained to generate the sifted key.

– **Step 2: Error correction:** A parameter estimation, also known as bit error estimation, is first performed over a small portion of the sifted keys between Alice and Bob, which yields an estimated error rate of the entire ensemble. This is followed by an error correction algorithm that locates and corrects the erroneous bits between two sides.

– **Step 3: Privacy amplification:** This refers to a process in which Alice and Bob perform mathematical processing on the error-corrected keys to eliminate possible information leakage to eavesdroppers and extract the final keys.

Parameters reported to other layers

– Quantum channel status: QBER

– QKD module status: output raw key rate, output secure secret key rate

9.4 Commercialization status for DV-QKD

As BB84 with decoy states is the most well studied DV-QKD protocols, there are several companies have released products or prototypes based on this protocol, including but not limited to QuantumCtek and Qasky (China), KT Corp. (Korea), NEC, NTT and Toshiba (Japan), QRate (Russia), Toshiba (UK and Japan), MagiQ and BBN Raytheon (USA).

Other than BB84, ID Quantique (Switzerland) has released several products based on SARG04 and COW protocols while QUBITEKK(USA) and S-Fifteen Instruments (Singapore) offer QKD devices running the BBM92 protocol. SpeQtral (Singapore) also plans to implement the BBM92 protocol on their satellite QKD payload. The Austrian Institute of Technology (Austria) has realized the QKD prototype with E91 protocol.

More information on the commercialization status for DV-QKD can be found in [b-QIT4N D2.5].

10 Introduction of continuous variable QKD protocols

In CV-QKD protocols, Alice encodes information using the position and momentum quadrature of a quantized electromagnetic while Bob uses the homodyne or heterodyne detection to decode information. In the following, several CV-QKD protocols will be introduced.

10.1 Gaussian modulation coherent state

10.1.1 Protocol features

GMCS protocol [b-Grosshans-1] was proposed by Grosshans and Grangier in 2002, thus it is also known as GG02, is the most popular and well-studied CV-QKD protocol. GG02 uses Gaussian modulation of coherent states to encode information and uses a homodyne detection to perform the measurement, which can be fully realized with standard telecom components. To reach longer transmission, reverse reconciliation and post selection techniques were invented to overcome the 3 dB loss limits in the channel.

A similar protocol, the no switching GMCS protocol, which uses heterodyne detection (also known as conjugated or dual homodyne detections) instead of one homodyne detection and simultaneously measures the position and momentum quadrature was proposed later. The no switching GMCS protocol is suitable for passive measurement scheme as it eliminates the random measurement and sifting step.

The security proofs of GMCS CV-QKD have been well established including security against individual attacks, collective attacks in the asymptotic limit and recently, the composable security general attack in the finite size regime. However, to adapt the most rigorous security proof, it is necessary to add an energy test step to the original GMCS protocols (no switching and GG02) and a symmetrisation step to GG02.

From the implementation point of view, GG02 is probably the most mature CV-QKD protocol. It has been realized with standard telecommunication fibre for distances from 25 to 100 km in both lab systems and real field tests [b-Fossier], [b-Alleaume], [b-Lodewyck], [b-Huang-3], [b-Huang-4] and [b-Wang-3].

10.1.2 Workflow

Quantum communication stage

– **Step 1: Preparation:** Alice generates 2N random numbers (X, P). The N random numbers are prepared according to a centred normal Gaussian distribution with a modulation variance. Alice then prepares the coherent states to map the N random number coordinates (X, P) on the position and momentum quadrature in the phase space, then sends these coherent states through the quantum channel.

– **Step 2: Measurement:** Bob generates N random binary numbers *b* and for each pulse performs a homodyne detection to measure either position and momentum quadrature based on the random bit *b*. From the measurements, Bob thus obtains N classical random variables *y*.

Classical post-processing stage

– **Step 1: Sifting:** Bob reveals to Alice the values of random bit *b* and his choice on the quadrature measurement through a public authenticated channel. Alice thus keeps approximately N values of the 2N values in (X, P) with respect to Bob's choice of quadrature. These values are known as Alice's data: x. Thus, Alice and Bob share a sequence of N correlated classical variables (x, y).

– **Step 2: Parameter estimation:** Alice randomly selects a subset of M<N values from the N correlated variables in the previous step. Alice reveals the M values to Bob as well as their index in the sequence, so that both parties select the same random subset data (x', y'). The subset (x', y') will be used to estimate the parameters which characterize the quantum channel: channel transmission T and excess noise ξ. Based on these two values and Alice's variance, Alice and Bob can further estimate the mutual information between them and the upper bound of Eve's information χ_{AE} for direct reconciliation or χ_{BE} for reverse reconciliation. If I_{AB} is smaller than χ_{AE} or χ_{BE}, it means Eve can have more information than Alice and Bob, and the key generation protocol aborts (no key is output).

– **Step 3: Error correction** (information reconciliation)**:** Based on the estimation of I_{AB}, the Alice and Bob choose appropriate binary functions to convert the remaining classical values (x'', y'') into two bits strings on each side. For the reverse reconciliation, Bob sends Alice a syndrome as the reference for Alice to estimate Bob's measurements. By selecting a proper error correction code, Alice can compute a correct value to estimate Bob's measurements thus correcting the errors. For direct reconciliation, the procedure is inversed where Alice sends a syndrome to Bob and Bob performs estimations to correct errors.

– **Step 4: Privacy amplification:** In case of reverse reconciliation, based on the estimation of Eve's knowledge χ_{BE} in Steps 2 and 3 and the length of the bit strings after the error correction, Alice can compute the length *l* of the secret key which they can distil from the common bit string shared by the two parties. For direct reconciliation, Bob computes the length *l* of secret key based on χ_{AE}. Alice (reverse reconciliation) or Bob (direct reconciliation) creates a random hashing function to transform the N - M bit string into a l bits string and sends the description of the hashing function through the public authenticated channel to the other party. Alice and Bob both apply this function to their own bit string so that the two parties obtain identical bit strings with a length *l*, which is known as a secret key.

Parameters reported to other layers

– Quantum channel status: excess noise, channel transmission, estimated secret key rate.

– QKD module status: shot noise variance, sender modulation variance, output raw key rate, output secret key rate.

10.2 Unidimensional continuous-variable quantum key distribution

10.2.1 Protocol features

Unidimensional (UD) protocol [b-Usenko-1] and [b-Gehring] which relies on a single quadrature modulation at Alice's side while Bob performs a randomly switched homodyne detection. UD CV-QKD requires a single modulator, thus these protocols provide a simple experimental realization with respect to conventional GMCS CV-QKD [b-Gehring]. This also means that the trusted parties are not able to estimate the channel transmittance in the un-modulated quadrature, which remains an unknown free parameter in the protocol security analysis. This parameter, however, can be limited by considerations of physicality of the obtained covariance matrices. In other words, Eve's collective attack should be pessimistically assumed to be maximally effective but is still limited by the physicality bounds related to the positivity of the covariance matrix and its compliance with the uncertainty principle [b-Weedbrook].

UD CV-QKD was extended to squeezed states [b-Usenko-2], which were shown to be advantageous only in the direct reconciliation scenario if the anti-squeezed quadrature is modulated. Unfortunately, the squeezed-state UD CV-QKD protocol does not have a good performance in reverse reconciliation [b-Usenko-2]. Additionally, the application of UD modulation in the measurement-device-independent CV-QKD was reported only recently [b-Bai] and [b-Huang-2]. In addition to the advantages of UD itself, the protocol can also resist attacks against detectors.

The security of coherent-state UD CV-QKD was firstly studied in the asymptotic limits and recently extended to the finite-size regime [b-Wang-2] with a study of its composability security against collective attacks [b-Liao-2].

10.2.2 Workflow

The protocol proceeds as follows:

Quantum communication stage

– **Step 1: Preparation:** Alice produces coherent states, e.g., with a laser source. Then she displaces each coherent state in one of the quadratures (denoted as x) according to a random Gaussian variable. Assume that the modulated quadrature x to be the amplitude quadrature. In this case the displacement can be performed by an intensity modulator. The states are then sent to the remote trusted party Bob through a channel.

– **Step 2: Measurement:** Bob performs detection using a homodyne detector, measuring most of the time the x quadrature, and sometimes measuring the p quadrature to monitor whether the attack exists or not.

Classical post-processing stage

After a sufficient number of runs, Alice and Bob analyse the security and extract a secret key from the x quadrature data using a reverse-reconciliation procedure [b-Grosshans-1] and [b-Grosshans-2] similar to the one in *Clause 10.1.2* (with the security proof in appendix I).

Parameters reported to other layers

– Quantum channel status: excess noise, channel transmission, estimated secret key rate.

– QKD module status: shot noise variance, sender modulation variance, output raw key rate, output secret key rate.

10.3 Continuous-variable measurement-device-independent quantum key distribution

10.3.1 Protocol features

Measurement-device-independent quantum key distribution (MDI-QKD) [b-Braunstein] and [b-Lo-1] was introduced to overcome a vulnerability of QKD systems, i.e., side-channel attacks on measurement devices if they are not properly designed or implemented. The basic feature of the MDI scheme is that Alice and Bob do not need to perform the measurement, instead the measurements are performed by an intermediate relay, which does not need a security oversight. This idea can also be realized in the setting of CV-QKD with the promise of sensibly higher rates at metropolitan distances [b-Pirandola-2] and [b-Li]. Currently, CV-MDI QKD is neither fully implemented yet nor commercially available but may have some potential in future QKDNs.

10.3.2 Workflow

The protocol proceeds as follows:

Quantum communication stage

– **Step 1: Preparation:** Alice and Bob possess two coherent modes, A and B respectively, which are prepared in coherent states $|\alpha\rangle$ and $|\beta\rangle$. The amplitude of these coherent states is randomly modulated, according to a bi-variate Gaussian distribution. Each one of the parties send the coherent states to the intermediate relay using the insecure channel.

– **Step 2: Measurement:** The modes arriving at the relay, say A′ and B′, are measured by the relay by means of a CV-Bell detection. This means that A′ and B′ are first mixed on a balanced beam splitter, and the output ports conjugately homodyned: on one port it is applied a homodyne detection on quadrature $\hat{q}$, which returns the outcome q_-, while the other port is homodyned on quadrature $\hat{p}$, obtaining an outcome p_+.

Classical post-processing stage

The outcomes from the CV-Bell measurement are combined to form a new complex outcome γ which is broadcast over a public channel by the relay. There are two kinds of data processing methods after receiving relay's measurement results. The first one is that one of the legitimate parties modifies the data, while the other one keeps the original data [b-Li]. This kind of data processing method and the following security proof are based on entanglement swapping (see appendix II for more details) [b-Li]. The second one is that Alice and Bob don't need to modify the data, while the security proof need to be done based on conditional scenarios, which requires a relatively complex post-processing technique [b-Pirandola-2].

Parameters reported to other layers

– Quantum channel status: excess noise, channel transmission, estimated secret key rate.

– QKD module status: shot noise variance, sender modulation variance, output raw key rate, output secret key rate.

NOTE – Additional parameters regarding to the MDI setting may also need to be reported.

10.4 Discrete modulation coherent state (DMCS)

10.4.1 Protocol features

The first DMCS (Discrete Modulation Coherent State) CV-QKD protocol, i.e., two-state modulation, was proposed in 2009 [b-Zhao, b-Leverrier-1]. Later, four-state modulation [b-Leverrier-3], three-state modulation [b-Kamil] and arbitrary number of phase-encoded coherent states [b-Papanastasiou] were proposed.

Compared to the GMCS protocol, the DMCS protocol has the advantage that its reconciliation procedure is relatively simple. Under low signal-to-noise ratio, GMCS protocol currently only employs multidimensional reconciliation algorithm. The calculation of multidimensional reconciliation is, however, more complicated and has specific requirements on the signal-to-noise ratio at receiver. In the case of DMCS protocol, the binary LDPC code can be used directly since the coding is randomly selected among a finite number of determined quantum states.

The security proofs of DMCS CV-QKD have been well established. Currently, the theoretical security of the four-state protocol against collective attack in the asymptotic limit is proved [b-Ghorai] and [b-Lin]. However, the security proof of the multi-state modulation coherent state CV-QKD protocol against collective attacks in the finite-size regime has not yet been proven.

10.4.2 Workflow

Quantum communication stage

– **Step 1: Preparation:** Alice randomly draws a discrete alphabet with N letters. Each letter k is encoded into a coherent state with amplitude $a_k = ze^{j\phi_k}$, where z is a fixed radius in phase space (it is just the square root of the mean number of photons) and the phase is given by $\phi_k = \frac{2\pi}{N}k, k = \{0,1,\cdots,N-1\}$. We call each realization $C(z,N)$ of this encoding scheme a "constellation". And then Alice sends these coherent states through the quantum channel to Bob.

– **Step 2: Measurement:** Bob performs a homodyne measurement on a random quadrature (X, P), i.e., position quadrature or momentum quadrature. Take the four-state modulation coherent state CV-QKD protocol as an example, the PM scheme of the DMCS-CVQKD protocol is plotted in Figure 2.

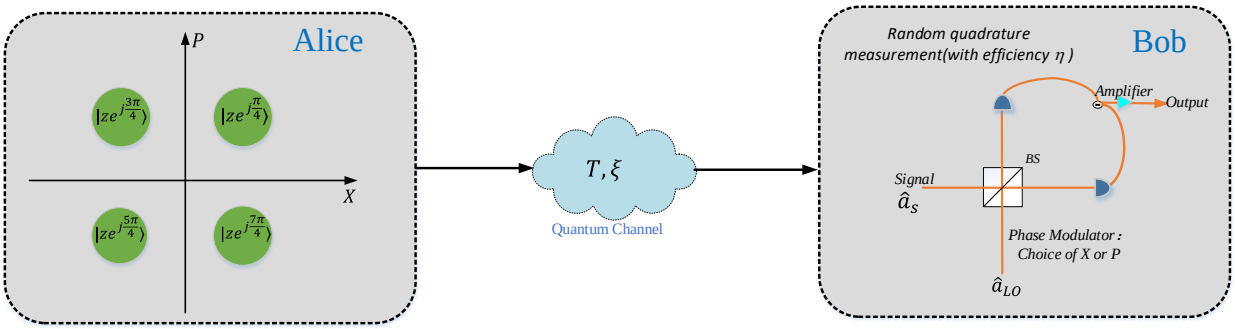


Figure *2*: Preparation-Measurement scheme of the DMCS-CVQKD protocol

Classical post-processing stage

– **Step 1: Sifting:** Bob informs Alice which of the X^B or P^B quadrature he randomly selected for each of his N measurements, such that Alice may respectively discard her N unused X^A or P^A quadrature values. After sifting, Alice and Bob share correlated random sequences of length N, herein defined as x and y.

– **Step 2: Parameter estimation:** Alice sends a part of bits of information to Bob that allow her to infer the characteristic of the quantum channel, i.e., channel transmission T and excess noise ξ, while Bob can compute the covariance matrix of quantum system. Based on the characteristics of the quantum channel and the covariance matrix of the quantum system, the legitimate party can judge whether the key generation protocol aborts or not.

– **Step 3: Error correction** (information reconciliation)**:** In DMCS CV-QKD protocol, the direct reconciliation channel is a BI-AWGN channel since the coding is randomly selected among a finite number of determined quantum states. Thus, a proper binary LDPC code can be directly used to correct errors. For the reverse reconciliation, the sign of the remaining classical values y which are labeled as u encodes the bit of the raw key while Bob reveals the absolute value y as side information to Alice through the classical authenticated (but not secure) channel. Alice utilizes the side information to reconstruct random variables v. Hence, the channel corresponding to the reverse reconciliation scenario, taking u as input and v as output is a BI-AWGN channel. After that, Alice chooses proper LDPC code to perform error correction.

– **Step 4: Privacy amplification:** Alice and Bob apply a random hash function to their corrected key so that they can obtain two identical strings, i.e., secure secret key.

Parameters reported to other layers

– Quantum channel status: excess noise, channel transmission, estimated secret key rate

– QKD module status: shot noise variance, sender modulation variance, output raw key rate, output secure secret key rate

10.5 Data interaction protocol for classical post processing in CV-QKD

After the quantum communication stage in CV-QKD system, the classical post processing is performed. It is essential to perform data interaction in such a procedure to achieve the same final key for the two remote legitimate parties, Alice and Bob. A general description of this stage is referred to in *Clause 7.1.2*.

Taking the GMCS CV-QKD protocol [b-Grosshans-1] and [b-Jouguet] using multidimensional reconciliation [b-Leverrier-2] as an example, a specific protocol procedure for data interaction is introduced for the step of error correction (information reconciliation) in *Clause 7.1.2*.

NOTE – This protocol is NOT a full CV-QKD protocol, but rather a protocol that is a part of the post processing for GMCS CV-QKD protocol and it does not include the step of privacy amplification.

The basic idea of the multi-dimensional reconciliation scheme [b-Leverrier-2] is that Alice and Bob choose proper mapping functions to convert the raw data into binary, quaternary and octal numbers of a group on each side which enable Alice and Bob to perform error correction using classical error correction code such as low-density parity-check (LDPC). Such process has been proven to be secure and no information is leaked to Eve. The multi-dimensional reconciliation scheme can extract up to one bit per symbol in low SNR regime on each side.

In general, such data interaction protocol can be divided in two stages:

– **Stage 1: Authentication procedure:** Alice and Bob realize the identity authentication with each other via pre-set symmetric key.

– **Stage 2: Data interaction procedure:** after the certified authentication, Bob sends data frames in the defined format with integrity protection of data to Alice via public authenticated channel. Alice reconstructs data via received data from Bob and performs key reconciliation.

Stage 1: Authentication stage

– **Step 1:** Alice and Bob store pre-set key in advance for verify the identity of both parties. Alice sends the message, hash value and key index of pre-set key to Bob. Then Alice waits for Bob's confirmation.

– **Step 2:** Bob receives all information from Alice and verifies Alice's certification. Similarly, Bob sends acknowledgment message and identification message to Alice and waits for Alice's conformation.

– **Step 3:** Alice receives all information from Bob and affirms Bob's identity. Finally, Alice sends the acknowledgment message to Bob.

After the three above steps completed, Alice and Bob verified the identity for each other.

Stage 2: Data interaction stage

Considering the multidimensional reconciliation protocol and the reverse reconciliation scheme for CV-QKD to beat 3dB channel loss limit, the data interaction stage includes three steps as follows:

– **Step 1:** Alice constructs data frames by mean of specific data format. The data frames consist of frame header and payload, where the header includes the version of data interaction protocol, the type of payload, the length of payload and session. In addition, the payload consists of side information generated by reconciliation procedure. The session is used to verify the legality and ensures the integrity of payload. The payload at Bob's side is processed by hash algorithm (e.g., Universal II hash) to generate hash values. The generated hash values are included in the session. Data frames at Bob's side are sent to Alice via classical channel.

– **Step 2:** Alice receives all data from Bob Alice calculates the hash values of received payload by using same hash algorithm and compares the hash values with received session to judge the integrity of payload. If the message integrity is achieved, Alice reconstructs data using raw data of Alice. In addition, Alice performs key reconciliation procedure by utilizing the side information from Bob.

– **Step 3:** Alice compares the hash value of decoding results and syndromes to determine whether the decoding results is discarded or not. Meanwhile, Alice sends the flag value which marks whether the key reconciliation is successful or not to Bob.

From the above steps, two data interactions are contained in GMCS CV-QKD protocol using the multidimensional reconciliation protocol.

10.6 Commercialization status for CV-QKD

The first commercial CV-QKD product on GG02 was released in 2012 by SeQureNet, a French start-up, aimed at research and study, with 1 MHz repetition rate and up to 80 km running distance [b-

Jouguet]. Since then, XT Quantech Co., Ltd (China) launched their no switching CV-QKD product in 2018 with a repetition rate of 10 MHz, and a typical secret key rate of 20kpbs@10dB and 1kpbs@18dB; and in 2019, XT launched a GG02 product with 10 MHz repetition rate and 25kpbs@10dB secret key rate [b-Huang-1]. Quintessence Labs from Australia has been working on no switching CV-QKD prototype [b-Weedbrook] while Huawei (Germany) launched its first CV-QKD prototype with discrete modulation protocol in 2018, with the possibility to further configure into Gaussian modulation.

More information on commercialization status for CV-QKD can be found in [b-QIT4N D2.5].

11 Standardization analysis and further suggestions

As it has been shown, QKD protocols own the features of both cryptographic protocols and communication protocols. Naturally, from a standardization perspective, QKD protocols should also follow similar routines as communication and cryptographic protocols. However, some experts believe that QKD, as an emerging technology, is still fast evolving in terms of research while others argue that QKD may be more suitable for a *de-facto standard* approach as it is only desirable in some niche markets which seems to be the current situation for QKD. In this clause some advantages and disadvantages of performing QKD protocol standardization are discussed.

11.1 Benefits of QKD protocol standardization

11.1.1 Definition of QKD protocols

Numerous QKD protocols have been devised over the past three decades. Despite recent standardization efforts for QKDN, there are still no standards established for a specific QKD protocol to date.

As presented above, QKD protocol involves complex procedures and processes to accomplish its goal of secure key establishment. Each step in this protocol related to key secrecy needs to be purposefully defined and precisely described. Since QKD is presently an emerging technology, a QKD standard should not be expected to skip the stage of protocol standardization. Standardization efforts can be found for similar emerging technologies e.g., optical communication protocol standards have been well established in SDOs and the post quantum cryptography (PQC) protocol standardization effort which is currently undertaken by NIST [b-NISTIR 8309].

The standardization of a QKD protocol would answer basic questions "*what is a QKD protocol and what does this protocol do?*" which could be the starting point for everything that is built around QKD protocols.

11.1.2 Certification of QKD protocols

As learned in previous technology developmental trajectories, protocol standardization is a critical step towards the certification of an instance of a given technology. Without a properly defined protocol, it would be extremely difficult to design and reach the goal of certification. In initial discussions at ETSI ISG QKD, it was also agreed that QKD protocol standardization will help the process of its certification.

The process of certification for any technology is complicated, not to mention for an emerging technology as QKD. In the process of certification, one can set different goals depending on the need and achieve them step by step. However, with regards to the complicated procedures of QKD

protocols, certification is not possible to be completed once and for all but rather diversely via many subtasks, which can then be combined to establish the whole process. Certification of QKD protocols, which is not within the scope of this report, would be a complicated and challenging task that QKD protocol standardization in itself will not solve and is in fact far from enough. However, it can make the certification process easier and may also serve as the first step and starting point towards QKD certification. Some pioneer certification work on QKD has been conducted by the research community [b-Sajeed], [b-Kumar] and, at the time of this report's publication, the [b-ISO/IEC 23837 CD2] work item was still under development in ISO/IEC JTC1 SC27/WG3.

NOTE – ITU-T FG QIT4N contributed some comments to the working draft of this ISO/IEC 23837 work item.

11.1.3 Interoperability in quantum layer

QKD protocol standardization may help the interoperability of QKD module communication in the quantum layer in a QKDN, which involves interoperability of QKD hardware, QKD software and between them.

QKD hardware interoperability usually occurs at the quantum communication stage (see *Clauses 7, 9 and 10*) through the quantum channel, different function modules can interoperate with each other inside a single QKD transmitter or receiver. Once the protocol and interfaces are defined, one can assemble the optical source, modulators, RNG and other functional modules from different vendors and make them interoperate with each other to realize a functional transmitter or receiver. This is the practice adopted by the research community and sometimes by the industry.

Interoperability between the transmitter and receiver in the quantum channel is a much more ambitious goal which would mean that a transmitter (Alice) from vendor A would be able to perform the quantum communication stage with a receiver (Bob) from vendor B. This idea is theoretically possible but extremely challenging from both a technical and standards point of view. So far, there has been no promising work to demonstrate the technical possibility and is not an active research topic in the community. Such an approach is even a big challenge for classical optical communication technologies. Regarding the current technology maturity of QKD technologies, such interoperability is unlikely to happen in the near future. However, there is a belief that with more progress on QKD photonic integrations, such interoperability is feasible. Nevertheless, QKD protocol standardization will help the interoperability at the quantum communication stage, taking into account the transport technology for QKD hardware [b-QIT4N D2.4]

QKD software interoperability usually happens at the post processing stage through the classical channel. It is possible to interoperate different software modules to perform different steps, see *Clause 7.1.2* such as error correction, two universal hash functions and so on. One can even use certain dedicated software to perform sub-tasks in one of the post processing steps.

Interoperability can also occur between QKD hardware and software. As shown in Figure 1, one can use QKD hardware from vendor A to interoperate with QKD control software from vendor B in the quantum communication stage. One can also use post processing (key distillation) and QKD key supply software from vendor A to interoperate with a QKD hardware of a transmitter and a receiver from vendor B. Once protocol steps and interfaces have been properly defined, interoperability is fairly easy to realize and has been already performed by both research and industry.

Above all, QKD protocol standardization will definitely be useful to realize interoperability of various aspects.

11.1.4 Confidence in QKD protocols

QKD protocol standardization will help real world users to be confident in QKD products that they deploy and use. Currently, there are no standards for any QKD protocols or any protocol framework in general. Confidence in QKD protocol procedures and their security proofs is currently purely based on the trust of QKD manufacturers and research articles. Users may need to perform their own study and analysis before being convinced or accepting anything. Such facts, on the other hand, may also limit the wider adoption of QKD by more potential users and applications. However, this issue can be somehow partially solved by the efforts of QKD protocol standardizations. If QKD products are complied with well-established QKD protocol standards, QKD users can be much more confident in their QKD deployments and applications without solely rely upon their trust of QKD manufacturers.

11.2 Disadvantages to QKD protocol standardization

One main concern of QKD protocol standardization, mainly from some in the research community, is that once some standards have been made on certain QKD protocols, it could prevent further innovation and research in QKD. Indeed, although QKD was invented a long time ago, its research is still evolving fast and researchers are still very active in developing new QKD protocols, techniques, security proofs etc.

However, the research community may neglect the fact that although the standardization procedure is complex, it is also comprehensive. QKD protocol standardization will not be completed in only one standard but, rather, by a step-by-step approach. Consented parts can be directly introduced for standardization while uncertain parts can remain as research topics. Also, revisions and updates to standards is always possible if there are new breakthroughs from research. QKD protocol standardization should not be a roadblock for innovation, but, rather, can enhance research activities. A very similar example to QKD technologies is optical communications in which research is still active while standards have been published in various SDOs including by ITU-T SG15.

In conclusion, QKD has significant benefits as detailed above but, for the protocol to move beyond academic research and progress into industrial commercialization, rigorous standardization is warranted.

11.3 Suggestions for future work

With consideration for the current gap in QKD protocol standardization progress, it is suggested to initiate QKD protocol and its related standardization work with the main concern of security:

– As some unique security features (*Clause 8*) of QKD protocol have not yet been introduced in SDOs, it is suggested to perform more studies on the security features of QKD protocols such as epsilon security (in *Clause 8.2*), ITS and beyond from a point view of standardization.

  NOTE – At the time of this report's publication, ISO/IEC JTC1/SC27/WG3 had initiated a call for contributions on the definition of the term ITS.

– As shown in *Clause 8*, security is the core of QKD technology and a challenging topic to address. Thus, it is expected to have more study on security issues of QKD protocols, including theoretical security and implementation security from standardization and certification perspectives.

– Standardization of specific QKD protocols (*Clauses 9 and 10*) still require further study, as the security proofs (see discussions in *Clause 8* and examples in the Appendix) and security

analysis for each protocol is very challenging and may be difficult to reach consensus. Even for the most mature protocol such as BB84 (*Clause 9.2*), it is expected to have many different versions and security analysis on it. In this direction, some in-depth study on certain QKD protocols from a standardization perspective will be useful.

– As shown in *Clause 7.1* and in the QKD protocol examples in *Clauses 9 and 10*, the QKD protocol workflow follows a certain pattern which can be further interpreted into a QKD protocol framework (some parts can be directly referenced to *Clause 7.1*). Thus, QKD protocol framework standards can be first considered to be initiated after this report.

– Current standardization work on QKD protocols (including non-normative technical reports and normative standards/Recommendations) could take references from and be compared with other protocol standards approaches in the ICT community. It is suggested to perform these tasks in ITU-T SG17, as security is the main topic; while topics related to security evaluation and certification may be considered to be carried out in ISO/IEC JTC1/SC27.

Appendix I

Security proof of UD CV-QKD

The security proof of UD CV-QKD uses the extremality of Gaussian states [b-Wolf] and subsequent optimality of Gaussian attacks [b-Navascués] and [b-García-Patrón]. In the reverse reconciliation the secret key rate can read:

$$K = \beta I_{AB} - \chi_{BE}, \tag{I-1}$$

where β represents the reconciliation efficiency.

$\chi_{BE} = S(E) - S(E|x_B)$ is the Holevo quantity [b-Holevo] which is the capacity of a bosonic channel between an eavesdropper (E) and the reference side of the information reconciliation (B), quantified as the difference of von Neumann entropy $S(E)$ of the state, available to an eavesdropper, and the entropy $S(E|x_B)$ of the eavesdropper state, conditioned by the measurement results of the remote trusted party B [b-Navascués] and [b-García-Patrón]. The positivity of the lower bound (1) means that the postprocessing algorithms are able to distil the secure key [b-Csiszar] and [b-Devetak] i.e., that the protocol is secure under given channel conditions. In the cases where channel noise is present, the collective attack can be accessed through the assumption that the eavesdropper holds the purification of the state, shared between A and B, thus the entropies of the substates of the generally pure state are equal: $S(E) = S(AB)$ and $S(E|x_B) = S(A|x_B)$. The calculation of the von Neumann entropies, contributing to the Holevo quantity, is done, using the covariance matrix formalism, explicitly describing the Gaussian states, through the symplectic eigenvalues $\lambda_{1,2}$ and λ_{cond} of the respective covariance matrices γ_{AB} prior to and$\gamma_{A\vee x_B}$ after the measurement so that:

$$\chi_{BE} = G\left(\frac{\lambda_1 - 1}{2}\right) + G\left(\frac{\lambda_2 - 1}{2}\right) - G\left(\frac{\lambda_{cond} - 1}{2}\right) \tag{I-2}$$

where $G(x) = (x+1)log(x+1) - xlogx$ [36] is the bosonic entropic function [b-Serafini].

As the states travel through the noisy and lossy channel, the covariance matrix is transformed according to the channel parameters. However, since there is no modulation in the p quadrature, the correlation, and, respectively, the channel transmittance in p cannot be estimated. The remote party can therefore only measure the variance of the channel output in p. Thus, C^p, which is the correlation between trusted modes in the p quadrature, is unknown due to the fact that the quadrature is not modulated, which means that the channel transmittance is not estimated in p. This unknown parameter is bounded by the requirement of the physicality of the state, which is given by the Heisenberg uncertainty principle, in terms of the covariance matrices being

$$\gamma_{AB_1} + i\Omega \geq 0 \tag{I-3}$$

where $\Omega = \bigoplus_{i=1}^{N} \omega$ is the symplectic form.

$$\omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{I-4}$$

Equation (I-4) imposes physical constraints on the possible values of C^p. Such constraint in the general case of noise present in both quadratures is given by the parabolic equation on the$\{V_B^p, C^p\}$ plane:

$$(C^p - C^0)^2 \leq \frac{V^2-1}{V}(1 - T^x V_B^0)\left(V_B^p - V_B^0\right), \tag{I-5}$$

with vertex (V_B^0, C^0), defined as

$$V_B^0 = \frac{1}{1 + T^x \varepsilon^x}, \tag{I-6}$$

and

$$C^0 = \frac{-V_B^0 \sqrt{T^x (V^2 - 1)}}{\sqrt{V}} \tag{I-7}$$

Eve's information can be still upper bounded and the lower bound on the key rate can be evaluated. The performance of the protocol was compared to standard one-way CV-QKD in the typical condition of a phase-insensitive thermal-loss channel (with the same transmittance and excess noise for both the quadratures). While the UD protocol is more fragile to channel loss and noise than conventional CV-QKD, it still provides the possibility of long-distance fibre-optical communication. In the limit of low transmissivity $T = T^x T^p$ and infinitely strong modulation, the key rate for the UD CV-QKD protocol with coherent-states and homodyne detection is approximately given by $\frac{Tlog2e}{3}$ [b-Usenko-1], which is slightly smaller than the similar limit for the standard one-way protocol with coherent states and homodyne detection [b-Grosshans-3] with a rate approximately given by $\frac{Tlog2e}{2}$.

The secret key rate considering the finite-size effect can be written as:

$$K_m^f = \frac{n}{N}\left(\beta I_{AB} - \chi_{BE}^{\delta_{PE}} - \Delta(n)\right) \tag{I-8}$$

where N is the total number of signals exchanged between Alice and Bob, in which n scales the number of signals used to extract the secret keys, and $N - n$ scales the number of the remainder of the signals for parameter estimation. $\chi_{BE}^{\delta_{PE}}$ represents the maximum of the Holevo information compatible with the statistics, except with the probability $\delta_{PE} \cdot \Delta n$ is a correction term for the achievable mutual information in the finite case

$$\Delta(n) \approx 7\sqrt{\frac{log_2(2/\overline{\epsilon})}{n}} \tag{I-9}$$

Appendix II

Security proof of CV MDI-QKD

The security of CV MDI QKD using coherent states has been first studied in the asymptotic limit [b-Pirandola-2], [b-Li] and [b-Ottaviani], and recently extended to finite-size [b-Zhang-2] and then composable security [b-Lupo], see *Clause II.3*. Some efforts were aimed at improving the performance of the protocols from a practical point of view, such as using squeezed states [b-Zhang-3], unidimensional modulated coherent states [b-Huang-2] and [b-Bai]. The asymptotic security analysis starts by considering the general scenario of a global unitary operation correlating all the uses of the protocol. However, using random permutations, Alice and Bob can reduce this scenario to an attack which is coherent within the single use of the protocol. After de Finetti reduction, this is a joint attack of both the links and the relay. Since the protocol is based on the Gaussian modulation and 'Gaussian detection' of Gaussian states, the optimal attack will be Gaussian. There are two kinds of security proof methods in the asymptotic limit. One is based on entanglement swapping and the other one is based on conditional scenarios.

For the security proof based on entanglement swapping [b-Li], if one further assumes that both Bob's initial two-mode squeezed state and the displacement operation inside himself are also untrusted, then the protocol could be seen as the well-known one-way CV-QKD protocol using coherent states and heterodyne detection. Thus, the entanglement-based (EB) scheme of CV-MDI QKD is just one specific case of the equivalent one-way model with more constraints on Eve, *see Clause II.1* [b-Li].

For the security proof based on conditional scenarios, before the unitary operation and the measurements, the global input state of Alice, Bob, and Eve is pure and Gaussian (Eve's ancillas are prepared in vacua). After unitary operation and before the measurements, their global output state is still pure, even though it could be non-Gaussian. Since local measurements commute, we can postpone Alice's and Bob's heterodyne detections after Eve's detection, whose outcome γ is obtained with probability p(γ). Thus, we have the conditional scenario, where Alice, Bob, and Eve share a conditional state. Using this conditional state, the secret key rate of the protocol could be derived, *see Clause II.2* [b-Pirandola-2] and [b-Ottaviani].

II.1 Security proof based on entanglement swapping

It is well known that the security of a PM scheme is equivalent to that of the corresponding entanglement based (EB) scheme for a QKD protocol. In the EB scheme, if one further assumes that both Bob's initial TMS state and the displacement operation inside himself are also untrusted, then the protocol could be seen as the well-known one-way CV-QKD protocol using coherent states and heterodyne detection. Thus, the EB scheme of CV-MDI QKD is just one specific case of the equivalent one-way model with more constraints on Eve. Therefore, the secret key rate of the equivalent one-way model should be a lower bound of the EB scheme. The secret key rate can be written as:

$$K_R = \beta I(a:b) - S(b:E) \tag{II-1}$$

where β is the reconciliation efficiency, $I(a:b)$ is the classical mutual information between Alice and Bob, $S(b:E)$ is the mutual information between Eve and Bob.

After the CV-Bell detection in Charlie, the covariant matrix $\gamma_{A_1CDB_1}$ is achieved. Using the covariant matrix $\gamma_{A_1CDB_1}$, the covariant matrix of the equivalent one-way model is:

$$\gamma_{A_1B_1'} = \begin{pmatrix} V_1 * I_2 & \sqrt{T(V_1^2-1)} * \sigma_z \\ \sqrt{T(V_1^2-1)} * \sigma_z & [T(V_1-1)+1+T\varepsilon'] * I_2 \end{pmatrix} \quad \text{(II-2)}$$

where $T = \frac{T_1}{2} g^2$, $\varepsilon' = 1 + \frac{1}{T_1}[2 + T_2(\varepsilon_2 - 2) + T_1(\varepsilon_2 - 1)] + \frac{1}{T_1}\left(\frac{\sqrt{2}}{g}\sqrt{V_B} - \sqrt{T_2}\sqrt{V_B+2}\right)^2$. We use $g = \sqrt{\frac{2}{T_2}}\sqrt{\frac{V_B}{V_B+2}}$ to achieve the lowest excess noise ε', Thus,

$$\varepsilon' = \varepsilon_1 + \frac{1}{T_1}[T_2(\varepsilon_2 - 2) + 2] \quad \text{(II-3)}$$

II.2 Security proof based on conditional scenarios

Indeed, assuming the asymptotic limit of many uses, large variance of the signal modulation, and ideal reconciliation efficiency, it is possible to obtain a closed formula for the secret key rate of CV-MDI QKD at any fixed value of the transmissivities and excess noise. In particular, two setups can be distinguished: the symmetric configuration, where the relay lies exactly midway the parties ($\eta_A = \eta_B$), and the asymmetric configuration ($\eta_A \neq \eta_B$). Assuming that Alice is the encoding party and Bob is the decoding party (inferring Alice's variable), the general expression of the asymmetric configuration takes the form:

$$\begin{aligned} R_{asy} = log_2 \frac{2(\eta_A + \eta_B)}{e|\eta_A - \eta_B|\bar{\chi}} + s\left[\frac{\eta_A \bar{\chi}}{\eta_A + \eta_B} - 1\right] \\ - s\left[\frac{\eta_A \eta_B \bar{\chi} - (\eta_A + \eta_B)^2}{|\eta_A - \eta_B|(\eta_A + \eta_B)}\right], \end{aligned} \quad \text{(II-4)}$$

where $\bar{\chi} := \frac{2(\eta_A+\eta_B)}{(\eta_A\eta_B)} + \varepsilon$, ε is the excess noise.

For pure-loss links ($\varepsilon = 0$) the rate of Equation (II-4) reduces to:

$$R_{asy} = log_2 \frac{\eta_A \eta_B}{e|\eta_A - \eta_B|} + s\left[\frac{2 - \eta_B}{\eta_B}\right] - s\left[\frac{2 - \eta_A - \eta_B}{|\eta_A - \eta_B|}\right]. \quad \text{(II-5)}$$

The asymmetric configuration, under ideal conditions, allows to achieve long-distance secure communication. In particular, for $\eta_A = 1$ the rate becomes:

$$R_{asy} = log_2 \frac{\eta_B}{e(1 - \eta_B)} + s\left[\frac{2 - \eta_B}{\eta_B}\right], \quad \text{(II-6)}$$

which coincides with the RR rate of the one-way protocol with coherent states and heterodyne detection. The performance degrades moving the relay in symmetric position with respect to Alice and Bob. In such a case, we set $\bar{\chi} = \frac{4}{\eta} + \varepsilon$ where $\eta := \eta_A = \eta_B$, and the rate is written as [b-Pirandola-2] and [b-Ottaviani]:

$$R_{sym} = log_2 \frac{\eta_B}{e^2 \bar{\chi}(\bar{\chi} - 4)} + s\left(\frac{\bar{\chi}}{2} - 1\right). \quad \text{(II-7)}$$

For pure-loss links, this simplifies to:

$$R_{sym} = log_2 \frac{\eta^2}{e^2(1 - \eta)} + s\left(\frac{2 - \eta}{\eta}\right), \quad \text{(II-8)}$$

and the maximum achievable distance is about 3.8 km of standard optical fibre from the relay.

II.3 Finite-size analysis and composable security

Finite-size analysis and composable security have been developed for CV-MDI QKD. In [b-Zhang-2] finite-size corrections have been studied assuming Gaussian attacks. The estimation of the channel parameters is provided within confidence intervals which are used to identify the worst-case scenario, corresponding to assuming the lowest transmissivity and the highest excess noise compatible with the limited data. The analysis showed that using signal block-size in the range of 10^6–10^9 data points is sufficient to obtain a positive secret key rate of about 10^{-2} bits/use. The composable security proof of CV MDI-QKD has been developed in [b-Lupo] using the lower bound provided by the smooth-min entropy. The security has been proven against general attacks using the optimality of Gaussian attacks for Gaussian protocols, and the de Finetti reduction of general attacks to collective ones. The lower bound to the key rate is given by:

$$R_n^{\varepsilon''} \geq \frac{n-k}{n}(\xi I_{AB} - I_E) - \frac{\sqrt{n-k}}{n}\Delta_{AEP}\left(\frac{2p\epsilon_s}{3}, d\right)\frac{+1}{n}log_2\left(p - \frac{2p\epsilon_s}{3}\right) + \frac{2}{n}log_2 2\epsilon - \frac{2}{n}log_2\left(\frac{K+4}{4}\right), \quad \text{(II-9)}$$

where ξ accounts for all sources of non-ideality in the protocol, I_{AB} is Alice-Bob mutual information and I_E is Eve's accessible information. The parameter $k = k_{ET} + k_{PE}$ is the number of signals used for the energy test and the parameter estimation, n is the total number of signals exchanged, and $K = K(n, \epsilon', k, d_A, d_B)$ is given by:

$$K(n, \epsilon', k) = max\left\{1, n(d_A + d_B)\frac{1 + 2\sqrt{\frac{ln\left(\frac{8}{\epsilon'}\right)}{2n}} + \frac{ln\left(\frac{8}{\epsilon'}\right)}{n}}{1 - 2\sqrt{\frac{ln\left(\frac{8}{\epsilon'}\right)}{2k_{ET}}}}\right\}. \quad \text{(II-10)}$$

The quantity $\epsilon'' = \frac{k_{ET}^4 \epsilon'}{50}$ is the overall security parameter with $\epsilon' := \epsilon + \epsilon_s + \epsilon_{EC} + \epsilon_{PE}$. Here ϵ comes from the leftover hash lemma, ϵ_s is the smoothing parameter, ϵ_{EC} is the error probability of the EC routine, and ϵ_{PE} that of the parameter estimation.

The result obtained by [b-Lupo] confirmed that CV MDI-QKD is composably secure against general attacks and the use of block-size of 10^7 -10^9 data points is sufficient to generate a positive key rate against general coherent attacks. [b-Lupo] also designed a novel parameter estimation procedure which is in principle more efficient. This approach may allow to perform the routine of parameter estimation using limited public communication. Further analysis is however needed to establish under which conditions this approach is fully composable.

Bibliography

[b-Acín] Acín, A., Brunner, N., Gisin, N., Massar, S., Pironio, S. and Scarani, V. (2007), *Device-independent security of quantum cryptography against collective attacks*. Physical Review Letters Vol. 98, No. 23, pp. 230501.

[b-Alleaume] Alleaume, R., Bouda, J., Branciard, C., Debuisschert, T., Dianati, M., Gisin, N., Godfrey, M., Grangier, P., Langer, T., Leverrier, A., Lutkenhaus, N., Painchault, P., Peev, M., Poppe, A., Pornin, T., Rarity, J., Renner, R., Ribordy, G., Riguidel, M., Salvail, L., Shields, A., Weinfurter, H. and Zeilinger, A. (2007), *SECOQC White Paper on Quantum Key Distribution and Cryptography*. ArXiv abs/quant-ph/0701168.

[b-Bai] Bai, D., Huang, P., Zhu, Y., Ma, H., Xiao, T., Wang, T. and Zeng, G. (2020), *Unidimensional continuous-variable measurement-device-independent quantum key distribution*. Quantum Information Processing Vol. 19, No. 53.

[b-Barrett] Barrett, J., Hardy, L. and Kent, A. (2005), *No Signaling and Quantum Key Distribution*. Physical Review Letters Vol. 95, No. 1, pp. 010503.

[b-Bennett-1] Bennett, C. H. and Brassard, G. (1984) *Quantum cryptography: Public-key distribution and coin tossing*, in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, pp. 175–179.

[b-Bennett-2] Bennett, C. (1992), *Quantum cryptography using any two nonorthogonal states*. Physical Review Letters Vol. 68, No. 21, pp. 3121-3124.

[b-Bennett-3] Bennett, C., Brassard, G. and Mermin, N. (1992), *Quantum cryptography without Bell's theorem*. Physical Review Letters Vol. 68, No. 5, pp. 557-559.

[b-Ben-Or] Ben-Or, M. and Mayers. D. (2004), *General security definition and composability for quantum & classical protocols.* arXiv:quant-ph/0409062.

[b-Brassard] Brassard, G., Lütkenhaus, N., Mor, T. and Sanders, B. C. (2000), *Limitations on Practical Quantum Cryptography*. Physical Review Letters Vol. 85, No. 6, pp. 1330-1333.

[b-Braunstein] Braunstein, S. L. and Pirandola, S. (2012), *Side-Channel-Free Quantum Key Distribution*. Physical Review Letters Vol. 108, No. 13, pp. 130502.

[b-Bruß] Bruß, D. (1998), *Optimal eavesdropping in quantum cryptography with six states*. Physical Review Letters Vol. 81, No. 14, pp. 3018-3021.

[b-Csiszar] Csiszar, I. and Korner, J. (1978), *Broadcast channels with confidential messages*. IEEE Transactions on Information Theory, Vol. 24, pp. 339-348.

[b-Devetak] Devetak, I. and Winter, A. (2004), *Relating Quantum Privacy and Quantum Coherence: An Operational Approach*. Physical Review Letters, Vol. 93, No. 8, p. 080501.

[b-Diamanti] Diamanti, E., Lo, H.-K., Qi, B. and Yuan, Z. (2016), *Practical challenges in quantum key distribution.* npj Quantum Information Vol. 2, No. 16025.

[b-Dong] Dong, L. and Chen, K. (2012). *Cryptographic protocol: Security Analysis Based on Trusted Freshness*.

[b-Ekert] Ekert, A. (1991), *Quantum cryptography based on Bell's theorem*. Physical Review Letters Vol. 67, No. 6, pp. 661-663.

[b-Elliott] Elliott, C., Pearson, D. and Troxel, G. (2003), *Quantum Cryptography in Practice*. Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM '03), pp. 227-238.

[b-ETSI GR QKD 007] Group Report ETSI GR QKD 007 (2018), *Quantum Key Distribution (QKD); Vocabulary*

[b-ETSI GS QKD 005] Group Specification ETSI GS QKD 005 V1.1.1 (2010) *Quantum key distribution (QKD); Security proofs*

[b-ETSI PP] Draft Group Specification ETSI DGS/QKD-016-PP, *QKD Common Criteria Protection Profile for QKD*, Early draft V.0.5.3

[b-ETSI White Paper 27] ETSI White Paper No. 27 (2018), *Implementation Security of Quantum Cryptography*.

[b-FIPS PUB 197] Federal Information Processing Standards Publication 197 (2001), *Announcing the ADVANCED ENCRYPTION STANDARD (AES)*

[b-Fossier] Fossier, S., Diamanti, E., Debuisschert, T., Villing, A., Tualle-Brouri, R., and Grangier, P. (2009). *Field test of a continuous-variable quantum key distribution prototype*. New Journal of Physics, Vol. 11, No. 4, p. 045023.

[b-García-Patrón] García-Patrón, R. and Cerf, N. J. (2006). *Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution*. Physical Review Letters, Vol. 97, No. 19, p. 190503.

[b-Gehring] Gehring, T., Jacobsen, C. S. and Andersen, U. L. (2016), *Single-quadrature continuous-variable quantum key distribution*. Quantum Information & Computation Vol. 16, No. 13-14, pp. 1081-1095.

[b-Gerhardt] Gerhardt, I., Liu, Q., Lamas-Linares, A., Skaar, J., Kurtsiefer, C., and Makarov, V. (2011), *Full-field implementation of a perfect eavesdropper on a quantum cryptography system*. Nature Communications, Vol. 2, No. 349.

[b-Ghorai] Ghorai, S., Grangier, P., Diamanti, E. and Leverrier, A. (2019), *Asymptotic security of continuous-variable quantum key distribution with a discrete modulation*. Physical Review X, Vol. 9, No. 2, p. 021059.

[b-Gisin-1] Gisin, N., Ribordy, G., Tittel, W. and Zbinden, H. (2002), *Quantum cryptography*. Reviews of Modern Physics Vol. 74, No. 1, pp. 145-195.

[b-Gisin-2] Gisin, N., Ribordy, G., Zbinden, H., Stucki, D., Brunner, N. and Scarani, V. (2004), *Towards practical and fast Quantum Cryptography*. arXiv:quant-ph/0411022.

[b-Gisin-3] Gisin, N., Fasel, S., Kraus, B., Zbinden, H., and Ribordy, G. (2006). *Trojan-horse attacks on quantum-key-distribution systems.* Physical Review A, Vol. 73, No. 2, p. 022320.

[b-Grosshans-1] Grosshans, F. and Grangier, P. (2002), *Continuous Variable Quantum Cryptography Using Coherent States*. Physical Review Letters Vol. 88, No. 5, pp. 057902.

[b-Grosshans-2] Grosshans, F., Assche, G. V., Wenger, J., Brouri, R., Cerf, N. J. and Grangier, P. (2003), *Quantum key distribution using gaussian-modulated coherent states*. Nature, Vol. 421, No. 6920, pp. 238–241.

[b-Grosshans-3] Grosshans, F. (2005), *Collective Attacks and Unconditional Security in Continuous Variable Quantum Key Distribution*. Physical Review Letters, Vol. 94, No. 2, p. 020504.

[b-Huang-1] Huang, D., Huang, P., Li, H., Wang, T., Zhou, Y. and Zeng, G. (2016), *Field demonstration of a continuous-variable quantum key distribution network*, Optics Letters, Vol. 41, pp. 3511-3514.

[b-Huang-2] Huang, L., Zhang, Y., Chen, Z. and Yu, S. (2019), *Unidimensional Continuous-Variable Quantum Key Distribution with Untrusted Detection under Realistic Conditions*. Entropy Vol. 21, No. 11, pp. 1100.

[b-Huang-3] Huang, D., Lin, D., Wang, C., Liu, W., Fang, S., Peng, J., Huang, P. and Zeng, G. (2015), *Continuous-variable quantum key distribution with 1 Mbps secure key rate*. Optics Express Vol. 23, pp. 17511.

[b-Huang-4] Huang, D., Huang, P., Lin, D. and Zeng, G. (2016), *Long-distance continuous-variable quantum key distribution by controlling excess noise*. Sci. Rep. Vol. 6, pp. 19201.

[b-Hwang] Hwang, W.-Y. (2003), *Quantum Key Distribution with High Loss: Toward Global Secure Communication*. Physical Review Letters Vol. 91, No. 5, pp. 057901.

[b-Inoue-1] Inoue, K., Waks, E. and Yamamoto, Y. (2002), *Differential Phase Shift Quantum Key Distribution*. Physical Review Letters Vol. 89, No. 3, pp. 037902.

[b-Inoue-2] Inoue, K., Waks, E. and Yamamoto, Y. (2003), *Differential-phase-shift quantum key distribution using coherent light*. Physical Review A Vol. 68, No. 2, pp. 022317.

[b-ISO/IEC 18033-3] ISO/IEC 10833-3:2010 (2010), *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers*

[b-ISO/IEC 23837 CD2] ISO/IEC 23837 Committee Draft 2, *Security requirements, test and evaluation methods for quantum key distribution*.

[b-ITU-T X.1710] Recommendation ITU-T X.1710 (2020), *Security framework for quantum key distribution networks*.

[b-Jouguet] Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P. and Diamanti, E. (2013), *Experimental demonstration of long-distance continuous-variable quantum key distribution*. Nature Photonics, Vol. 7, No. 5, pp. 378–381.

[b-Kamil] Kamil, B. and Weedbrook, C. (2018), *Security proof of continuous-variable quantum key distribution using three coherent states*. Physical Review A 97.2 (2018): 022310.

[b-Kerckhoffs] Kerckhoffs, A. (1883), *La cryptographie militaire*. Journal des sciences militaires, Vol. 9, pp. 5-38.

[b-Kumar] Kumar, R., Mazzoncini, F., Qin, H. and Alléaume, R. (2021). *Experimental vulnerability analysis of QKD based on attack ratings*. Scientific Reports Vol. 11, No. 9564.

[b-Leverrier-1] Leverrier, A. and Grangier, P. (2009), *Unconditional security proof of longdistance continuous-variable quantum key distribution with discrete modulation*. Physical Review Letters, Vol. 102, No. 18, pp. 1-4.

[b-Leverrier-2] Leverrier, A., Alléaume, R., Boutros, J., Zémor, G. and Grangier, P. (2008), *Multidimensional reconciliation for a continuous-variable quantum key distribution*. Physical Review A, Vol. 77, No. 4, pp. 042325.

[b-Leverrier-3] Leverrier, A. and Grangier, P. (2010), *Continuous-variable quantum key distribution protocols with a discrete modulation*. arXiv preprint arXiv:1002.4083.

[b-Li] Li, Z., Zhang, Y.-C., Xu, F., Peng, X. and Guo, H. (2014), *Continuous-variable measurement-device-independent quantum key distribution*. Physical Review A Vol. 89, No. 5, pp. 052301.

[b-Liao-1] Liao, S.-K., Cai, W.-Q., Liu, W.-Y., Zhang, L., Li, Y., Ren, J.-G., Yin, J., Shen, Q., Cao, Y., Li, Z.-P., Li, F.-Z., Chen, X.-W., Sun, L.-H., Jia, J.-J., Wu, J.-C., Jiang, X.-J., Wang, J.-F., Huang, Y.-M., Wang, Q., Zhou, Y.-L., Deng, L., Xi, T., Ma, L., Hu, T., Zhang, Q., Chen, Y.-A., Liu, N.-L., Wang, X.-B., Zhu, Z.-C., Lu, C.-Y., Shu, R., Peng, C.-Z., Wang, J.-Y. and Pan, J.-W. (2017), *Satellite-to-ground quantum key distribution*. Nature Vol. 549, No. 7670, pp.43-47.

[b-Liao-2] Liao, Q., Guo, Y., Xie, C., Huang, D., Huang, P. and Zeng, G. (2018) *Composable security of unidimensional continuous-variable quantum key distribution*. Quantum Information Processing Vol. 17, No. 113.

[b-Lin] Lin, J., Upadhyaya, T. and Lütkenhaus, N. (2019), *Asymptotic Security Analysis of Discrete-Modulated Continuous-Variable Quantum Key Distribution*. Physical Review X, Vol. 9, No. 4, p. 041064

[b-Lo-1] Lo, H.-K., Curty, M. and Qi, B. (2012), *Measurement-Device-Independent Quantum Key Distribution*. Physical Review Letters, Vol. 108, No. 13, pp. 130503.

[b-Lo-2] Lo, H.-K., Ma, X. and Chen, K. (2005), *Decoy State Quantum Key Distribution*. Physical Review Letters Vol. 94, No. 23, pp. 230504.

[b-Lodewyck] Lodewyck, J., Bloch, M., Garcia-Patron, R., Fossier, S., Karpov, E., Diamanti, E., Debuisschert, T., Cerf, N. J., Tualle-Brouri, R., McLaughlin, S. W. and Grangier, P. (2007), *Quantum key distribution over 25 km with an all-fiber continuous-variable system*. Physical Review A, Vol. 76, No. 4, p. 042305.

[b-Lucamarini] Lucamarini, M., Yuan, Z. L., Dynes, J. F. and Shields, A. J. (2018), *Overcoming the rate–distance limit of quantum key distribution without quantum repeaters*. Nature Vol. 557, No. 7705, pp. 400-403.

[b-Lupo] Lupo, C., Ottaviani, C., Papanastasiou, P. and Pirandola, S. (2018), *Continuous-variable measurement-device-independent quantum key distribution: Composable security against coherent attacks*. Physical Review A Vol. 97, No. 5, p. 052327.

[b-Lydersen] Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J. and Makarov, V. (2010), *Hacking commercial quantum cryptography systems by tailored bright illumination*. Nature Photonics, Vol. 4, pp. 686-689.

[b-Ma] Ma, X., Zeng, P. and Zhou, H. (2018), *Phase-matching quantum key distribution*. Physical Review X, Vol. 8, No. 3, pp. 031043.

[b-Mayers] Mayers, D. and Yao, A. (2004), *Self-testing quantum apparatus*. Quantum Information & Computation Vol. 4, No. 4, pp. 273-286.

[b-Müller-Quade] Müller-Quade, J. and Renner, R. (2009), *Composability in quantum cryptography*, New Journal of Physics, Vol. 11, No. 085006.

[b-Navascués] Navascués, M., Grosshans, F. and Acín, A. (2006). *Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography*. Physical Review Letters, Vol. 97, No. 19, p. 190502.

[b-NISTIR 8309] Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Kelsey, J., Liu, Y.-K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., Smith-Tone, D., (2020). *Status Report on the Second Round of the NIST Post-Quantum Cryptography*

[b-Ottaviani] Ottaviani, C., Spedalieri, G., Braunstein, S. L. and Pirandola, S. (2015), *Continuous-variable quantum cryptography with an untrusted relay: Detailed security analysis of the symmetric configuration*. Physical Review A, Vol. 91, No. 2, p. 022320.

[b-Papanastasiou] P. Papanastasiou, Lupo, C., Weedbrook, C. and Pirandola, S. (2018), *Quantum key distribution with phase encoded coherent states: Asymptotic security analysis in thermal-loss channels*, Physical Review A Vol. 98, p. 012340.

[b-Pirandola-1] Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J., Razavi, M., Shaari, J. S., Tomamichel, M., Usenko, V. C., Vallone, G., Villoresi, P. and Wallden, P. (2020), *Advances in Quantum Cryptography*. Advances in Optics and Photonics Vol. 12, No. 4, pp. 1012-1236.

[b-Pirandola-2] Pirandola, S., Ottaviani, C., Spedalieri, G., Weedbrook, C., Braunstein, S. L., Lloyd, S., Gehring, T., Jacobsen, C. S., Andersen, U. L. (2015), *High-rate measurement-device-independent quantum cryptography*. Nature Photonics Vol. 9, pp. 397–402.

[b-Poppe] Poppe, A., Peev, M. and Maurhart, O. (2008), *Outline of the SECOQC quantum-key-distribution network in Vienna*. International Journal of Quantum Information, Vol. 6, No. 2, pp.209-218.

[b-Popovic] Popovic, M. (2018). *Communication Protocol Engineering* (2nd ed.). CRC Press.

[b-Portmann] Portmann, C. and Renner, R. (2021), *Security in Quantum Cryptography*. arXiv:2102.00021v2 [quant-ph]

[b-Qin-1] Qin, H., Kumar, R. and Alléaume, R. (2016), *Quantum hacking: saturation attack on practical continuous-variable quantum key distribution*. Physical Review A, Vol. 94, No. 1, p. 012325.

[b-Qin-2] Qin, H., Kumar, R., Makarov, V. and Alléaume, R. (2018), *Homodyne-detector-blinding attack in continuous-variable quantum key distribution*. Physical Review A, Vol. 98, No.1, p. 012312.

[b-QIT4N D2.1] ITU-T Technical Report (2021), *Quantum information technology for networks terminology: quantum key distribution network*

[b-QIT4N D2.3 2] ITU-T Technical Report (2021), *Quantum key distribution network (QKDN) protocols part 2: Key management layer, QKDN control layer, and QKDN management layer*

[b-QIT4N D2.4] ITU-T Technical Report (2021), *Quantum key distribution network transport technologies*

[b-QIT4N D2.5] ITU-T Technical Report (2021), *Quantum information technology for networks standardization outlook and technology maturity: quantum key distribution network*

[b-Ralph] T. C. Ralph. *Continuous variable quantum cryptography*. Phys. Rev. A 61, 010303(R), (1999)

[b-Renner] Renner, R. (2008), *Security of quantum key distribution*. International Journal of Quantum Information, Vol. 6, No.1, pp. 1-127.

[b-RFC8017] Moriarty, K., Ed., Kaliski, B., Jonsson, J., and Rusch, A. (2016), *PKCS #1: RSA Cryptography Specifications Version 2.2*, RFC 8017, DOI 10.17487/RFC8017, November.

[b-Sajeed] Sajeed, S., Chaiwongkhot, P., Huang, A. *et al.* (2021). *An approach for security evaluation and certification of a complete quantum communication system.* Sci Rep 11, 5110.

[b-Sasaki-1] Sasaki, T., Yamamoto, Y. and Koashi, M. (2014), *Practical quantum key distribution protocol without monitoring signal disturbance*. Nature Vol. 509, No. 7501, pp. 475-478.

[b-Sasaki-2] Sasaki, M., Fujiwra, M., Ishizuka, H., Klaus, W., Wakui, K., Takeoka, M., Tanaka, A., Yoshino, K., Nambu, Y., Takahashi, S. and Tajima, A. (2011), *Tokyo QKD network and the evolution to Secure Photonic Network.* In CLEO:2011 - Laser Applications to Photonic Applications, OSA Technical Digest paper JTuC1.

[b-Scarani-1] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lutkenhaus, N. and Peev, M. (2009), *The security of practical quantum key distribution*. Reviews of Modern Physics, Vol. 81, No. 3, pp. 1301-1350.

[b-Scarani-2] Scarani, V., Acín, A., Ribordy, G. and Gisin, N. (2004), *Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations*. Physical Review Letters Vol. 92, No. 5, pp. 057901.

[b-Silberhorn] Silberhorn, C., Ralph, T., Lütkenhaus, N. and Leuchs, G. (2002), *Continuous Variable Quantum Cryptography: Beating the 3 dB Loss Limit*. Physical Review Letters, Vol. 89, No. 16, pp. 167901.

[b-Spedalieri] Spedalieri, G., Ottaviani, C. and Pirandola, S. (2013), *Covariance matrices under Bell-like detections*. Open Systems & Information Dynamics Vol. 20, No. 02, 1350011.

[b-Stucki] Stucki, D., Brunner, N., Gisin, N., Scarani, V. and Zbinden, H. (2005), *Fast and simple one-way quantum key distribution*. Applied Physics Letters Vol. 87, No. 19.

[b-Usenko-1] Usenko, V. C. and Grosshans, F. (2015), *Unidimensional continuous-variable quantum key distribution*. Physical Review A Vol. 92, No. 6, pp. 062337.

[b-Usenko-2] Usenko, V. C. (2018), *Unidimensional continuous-variable quantum key distribution using squeezed states*. Physical Review A Vol. 98, No. 3, pp. 032321.

[b-Wang-1] Wang, X.-B. (2005), *Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography.* Physical Review Letters Vol. 94, No. 23, pp. 230503.

[b-Wang-2] Wang, P., Wang, X., Li, J. and Li, Y. (2017), *Finite-size analysis of unidimensional continuous-variable quantum key distribution under realistic conditions*. Optics Express Vol. 25, No. 23, pp. 27995-28009.

[b-Wang-3] Wang, C., Huang, D., Huang, P., Lin, D., Peng, J. and Zeng, G. (2015), *25 MHz clock continuous-variable quantum key distribution system over 50km fiber channel*. Sci. Rep. Vol. 5, pp. 14607.

[b-Weedbrook] Weedbrook, C., Pirandola, S., García-Patrón, R., Cerf, N. J., Ralph, T. C., Shapiro, J. H. and Lloyd S. (2012), *Gaussian quantum information*. Reviews of Modern Physics Vol. 84, No. 2, pp. 621-669.

[b-Wolf] Wolf, M. M., Giedke, G. and Cirac, J. I. (2006), *Extremality of Gaussian Quantum States*. Physical Review Letters Vol. 96, No. 8, pp. 080502.

[b-Xu] Xu, F., Ma, X., Zhang, Q., Lo, H.-K. and Pan, J.-W. (2020), *Secure quantum key distribution with realistic devices*. Reviews of Modern Physics Vol. 92, No. 2, pp. 025002.

[b-Zhang-1] Zhang, Z., Yuan, X., Cao, Z. and Ma, X. (2017), *Practical round-robin differential-phase-shift quantum key distribution*. New Journal of Physics Vol. 19, No. 3, pp. 033013.

[b-Zhang-2] Zhang, X., Zhang, Y.-C., Zhao, Y., Wang, X., Yu, S. and Guo, H. (2017), *Finite-size analysis of continuous-variable measurement-device-independent quantum key distribution*. Physical Review A, Vol. 96, No. 4, p. 042334.

[b-Zhang-3] Zhang, Y.-C., Li, Z., Yu, S., Gu, W., Peng, X. and Guo, H. (2014), *Continuous-variable measurement-device-independent quantum key distribution using squeezed states*. Physical Review A, Vol. 90, No. 5, p. 052325.

[b-Zhao] Zhao, Y.-B., Heid, M., Rigas, J. and Lütkenhaus, N. (2009), *Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks*. Physical Review A Vol. 79, pp. 012307.