ISSN 1831-9424

European Commission

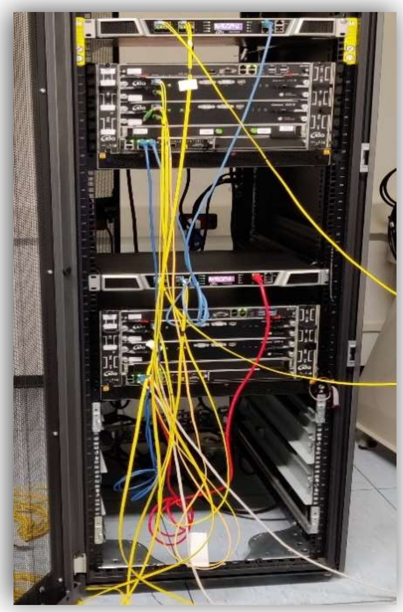
JRC TECHNICAL REPORT

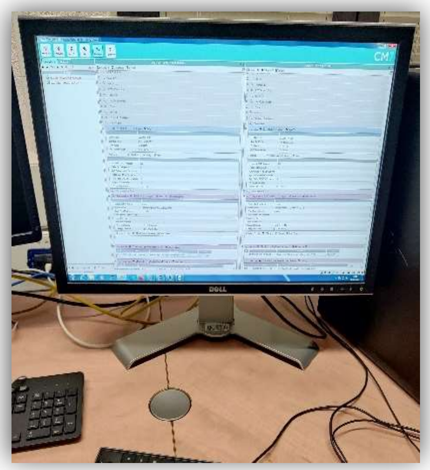
Quantum Key Distribution (QKD) Experimental Assessment

Overview and performance assessment of QKD system at JRC

Cerutti, I., Lewis, A., Bonavitacola, F.

2023





Joint
Research
Centre

This publication is a Technical report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The contents of this publication do not necessarily reflect the position or opinion of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication. For information on the methodology and quality underlying the data used in this publication for which the source is neither Eurostat nor other Commission services, users should contact the referenced source. The designations employed and the presentation of material on the maps do not imply the expression of any opinion whatsoever on the part of the European Union concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Contact information
Name: Isabella Cerutti
Address: : Via Enrico Fermi 2749, Ispra, Italy
Email: Isabella.cerutti@ec.europa.eu

EU Science Hub
https://joint-research-centre.ec.europa.eu

JRC132426

EUR 31594 EN

PDF ISBN 978-92-68-05663-9 ISSN 1831-9424 doi:10.2760/804200 KJ-NA-31-594-EN-N

Luxembourg: Publications Office of the European Union, 2023

© European Union, 2023

The reuse policy of the European Commission documents is implemented by the Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39). Unless otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (https://creativecommons.org/licenses/by/4.0/). This means that reuse is allowed provided appropriate credit is given and any changes are indicated.

For any use or reproduction of photos or other material that is not owned by the European Union permission must be sought directly from the copyright holders. The European Union does not own the copyright in relation to the following elements:
- page 11, Fig. 3 , from ref. [10], used with permission
- page 12, Fig. 4 , from ref. [11], open access reuse

How to cite this report: Cerutti, I., Lewis, A. and Bonavitacola, F., *Quantum Key Distribution (QKD) Experimental Assessment*, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/804200, JRC132426.

Contents

Abstract

Security of communication is an essential requirement for sensitive and critical information. The encryption protocols are currently used for protecting the data transmissions against possible eavesdroppers. However they are already under attack and will become vulnerable when quantum computers will be available. The development and the transition to more secure techniques for data communications are therefore required for the next decade and if possible even sooner.

Transmission of single photons (or quantum) in optical fibres represents a secure way of communicating, as possible attacks or eavesdrops would not pass undetected, thanks to the physical properties of quantum systems. The security principle of quantum communication is nowadays exploited in commercial equipment for the purpose of exchanging cryptographic keys required by the encryption algorithms. In such **quantum key distribution (QKD)** systems, the cryptographic keys are encoded into single photons and transmitted via optical fibres.

This document aims to assess the performance and limitations of QKD systems, and more specifically of the commercial QKD system by ID Quantique (IDQ) installed at JRC. After an overview of the QKD system and its configuration, performance assessment is reported for different cases of fibre link length or loss.

Executive Summary

This report describes tests of an ID Quantique Cerberis^3 two-wavelength optical fibre quantum key distribution system. The test were conducted to acquire experience to help the JRC support the ongoing project to construct an EU-wide Quantum Communication Infrastructure (EuroQCI).

Quantum key distribution is a technique for agreeing cryptographic keys between parties which exploits either quantum uncertainty and no-cloning or quantum entanglement to reveal the presence of an eavesdropper. Quantum randomness is used to generate the key. Several protocols exist, Cerberis uses the coherent-one-way (COW) protocol in which optical weak coherent pulses are prepared by one party and measured by the other party, security being based on the quantum uncertainty in the detection of consecutive pulses. The pulses are prepared simply by attenuating a laser and modulating its intensity.

Apart from the basic performance measure, which is the secret key rate, the most important parameters are the quantum bit error rate (QBER), which indicates how far the system is from the point of failure, and the monitoring-interferometer signal visibility, which indicates the margin of security. QBER is caused by errors in bit preparation and by dark counts, after-pulsing and jitter in the detector. A reduction of the signal visibility reveals the presence of an eavesdropper, so it is important that it remains high and stable in normal use.

Cerberis^3 is designed to operate over up to about 50 km of fibre, corresponding to 12 dB attenuation. In these tests, the send and receive units were mounted in the same rack and the signal passed either directly between them or over a distance of the order of 1 km in the JRC internal fibre network. Additional attenuation was introduced to simulate the loss over realistic distances, and the effect on the performance measured. Increasing attenuation from 6.9 dB to 10 dB led to an increase in key rate from 1456 to 2772 b/s at 1550nm and from 1554 to 1769 b/s at 1310nm. Further attenuation reduced key rate. The dark-count corrected QBER, however, was optimal at somewhat higher attenuations, near to 13 dB. Visibility was reduced by increasing attenuation to 10 dB, but only to 0.97 at 1550nm and to 0.98 at 1310 nm, which would not prevent the correct functioning of the monitoring channel.

Three states are used in the original COW protocol, based on quantum state $|\alpha\rangle$, a coherent pulse with average photon number α, and the quantum vacuum state $|0\rangle$, when no light is sent. Quantum bit (qubit) '0' is encoded with $|\alpha\rangle$ followed by $|0\rangle$, qubit '1' is encoded with $|0\rangle$, followed by $|\alpha\rangle$; the third state used is $|\alpha\rangle$ followed by $|\alpha\rangle$, for decoys added to increase the number of anomalous monitoring interferometer events which would be caused by an eavesdropper. A security weakness of this protocol has recently been published which has the effect of considerably reducing the distance over which the system can work. An improved protocol with additional decoy states: $|0\rangle$ followed by $|0\rangle$, is thought to mitigate the security limitation. ID Quantique provided new software incorporating this four-state COW protocol. In tests at JRC, the key rate after this upgrade was no worse than with the three-state protocol and, at low attenuations, even somewhat better.

Overall reliability of the system was also assessed, by measuring parameters over periods of several days. The system displayed good time stability, the variation of the performance being limited in the absence of changes of the external conditions.

Stalling of the system (i.e., quantum key accumulation on hold) occurred in some frames and the causes and system behaviour in these cases were investigated. Some hardware failures were recorded in the period, which are also noted. The overall conclusion is that the system performs as advertised, but is not completely reliable over a period of months. Maintenance would need to be planned accordingly. Much greater reliability would have to be achieved for satellite-borne nodes. Given that the security of COW is a topic of ongoing research, we recommend against using it in operational EuroQCI until the state of knowledge is improved, especially to give reassurance that the four-state protocol fully resolves known vulnerabilities.

1 Introduction

Digital communication enables the ubiquitous and continual exchange of information between entities (i.e., users, sensors, machines) of the digital society. The digital communication infrastructure is critical for the society, making it necessary to protect it against possible threats and security attacks. Robust and reliable security mechanisms can be used to protect the communication content and its integrity. In particular, cryptographic algorithms are commonly used for ensuring the data confidentiality (i.e., to prevent an unauthorized access to the data), the data integrity (i.e., to verify that the data has not been manipulated) and for authentication (i.e. to grant an authorize access with proper rights).

Classical cryptographic algorithms relies on mathematical operations that are proved to be so hard to invert as to be unfeasible with computing resources and time expected to be available to an adversary. This includes integer factorization in the RSA asymmetric cryptographic algorithm and the multiple non-linear substitutions, transpositions and mixing steps in the AES symmetric encryption algorithm. However, with the advent of faster computing platforms and with the first demonstration of quantum computing, the security of the classical cryptographic systems is jeopardized. Indeed, Grover's work [1] demonstrated that the speedup of quantum computers can halve the security level of the existing symmetric cryptographic algorithms (such as AES, SHA), that is to say, the key length must be doubled for the number of computation steps needed to break the cypher to be equivalent. Moreover, Shor's work [2] demonstrated that quantum computers would be able to break the existing public-key cryptographic algorithms (such as RSA, DSA, ECDH), making them unsecure even if the key length was greatly increased. For the time being, no sufficiently large quantum computer is available, but intensive efforts are being made to develop them.

Quantum communications has been advocated as a means of overcoming such security threats. It is based on the quantum physical principle that it is impossible to gain sufficient information about quantum states to reproduce them without perturbing the states (i.e., the so called no-cloning theorem). This physical principle is exploited for exchanging quantum states between two users (i.e., Alice and Bob) in a secure way.

Through a proper protocol Alice transmits quantum random states in a suitable basis to Bob, who measures them, generating a raw bitstream. After additional steps of basis reconciliation, classical error correction and privacy amplification, the final, shorter, common dataset is derived independently by Alice and Bob. This data – generated and exchanged by a quantum secure technique – can then be used as a key in classical symmetric encryption algorithms.

The data rate achieved by quantum communications (of the order of kb/s up to tens of kb/s) is still many orders of magnitude smaller than the rate required for typical optical transmission at e.g. hundreds of Gb/s per channel with hundreds of channels on the same optical fibre. So, in most use-cases, it is impractical to encrypt data with a random secret key of the same length as the message; unfortunately, because such "one-time pad" encryption is proved to be unconditionally secure. Instead quantum communications are used to distribute keys for classical symmetric encryption algorithms, such as AES with a key length long enough to resist a Grover algorithm attack, or any other known attack. If the secret key rate performance of QKD was very greatly improved, in principle it would be possible to use one-time pad encryption.

The advantages of QKD with respect to conventional key distribution are that it is not necessary to use a "courier" to distribute the keys, with associated risks of loss, theft, bribery or blackmail, and that QKD is not dependent on a mathematical assumption that an operation cannot be inverted, as is the case with key agreement by asymmetric cryptography.

However, some technical advances are still required to achieve such claims. First, although the security of the best established QKD protocols is proved by the scientific community and partially standardised, a full suite of standards and associated certification processes is not yet in place for independently verifying and controlling the security of QKD systems [3]. In addition, some of the less widely used QKD protocols still lack a security demonstration or scientific consensus on the security proof.

The European Commission has launched an initiative to construct a Quantum Communications Infrastructure (EuroQCI) throughout the Union, consisting of both terrestrial fibre links and satellite links, with QKD as its first application. The JRC works extensively with DG CNECT, as well as DG DEFIS, ESA, standards development organizations, member state governments and industrial and academic consultants on the design the design of EuroQCI. The Commission also finances research and development in quantum communications, especially in the EU Quantum Technology Flagship. It is therefore timely for us to gain practical experience with QKD systems, including commercial products. A call for tender for leasing QKD equipment was issued by JRC in 2019, to which only ID Quantique SA of Geneva responded, offering the Cerberis system detailed in this report. As the market develops, it is expected that products from other manufacturers will become available and we hope to test them in a similar manner.

This report is organized as follow. First the weaknesses of classical cryptography are reviewed to critically assess the benefits and the limitations of quantum cryptography. To better assess the state of the art of QKD systems, a commercial QKD equipment has been installed at JRC. In this report, the installation and characterization of the system is documented. The set-up and characterization are to provide insights on the level of security and robustness that can be expected with current commercial QKD systems.

2 Benefits and Limitations of Classical Cryptography versus Quantum Key Distribution (QKD) and Cryptography

Consider a cryptography system consisting of a source (Alice) that transmits information (plaintext) to a destination (Bob). To avoid that the information can be eavesdropped by another party (Eve), Alice encrypts the information (cyphertext), which can be then de-encrypted by Bob by applying the same encryption algorithm using a key shared by Alice or derived from it. A classical cryptographic system makes use of classical encryption algorithms, whose public keys are transmitted on a classical communication system (e.g., in an optical or radio communication network). Instead, in a quantum system, the keys are encoded in quantum states (e.g., state of photons) and transmitted in a dedicated quantum channel.

Both classical and quantum cryptographic systems suffer from different vulnerabilities. Here we identify the vulnerabilities of concern and we discuss whether and how a classical cryptographic system or a quantum one can overcome or mitigate them.

The vulnerabilities of concerns for cryptographic systems are:

1) **Attacks to an encrypted channel can pass undetected.** This is an issue especially when transmitting encryption keys. In addition, an eavesdropper could make electronic copies of the eavesdropped data and perform post-processing (e.g., exhaustive search decryption). To ensure the confidentiality and integrity of the exchanged keys, the following solutions can be put in place.

   Classical cryptography solution: all the recommended security counter-measures should be put in place to reduce the probability of attacks and increase the chances of detecting any attack.

   Quantum solution: With QKD systems, the security attacks of eavesdroppers *on the exchanged keys on the quantum channel* can be detected provided that:

   - The QKD protocol is unconditionally-secure.
   - The equipment at Alice and Bob has not been tampered and, when possible, it has been certified to operate according to the specifications and the protocols.
   - The sites hosting Alice and Bob equipment are inaccessible.
   - The installation of the system and thus the initial authentication of Alice and Bob (i.e., using an authentication certification key) are carried out in a trustworthy manner.

2) **Authentication of Alice and Bob is a critical step**. The authentication prior to the communication between Alice and Bob is an essential step to ensure that the parties are legitimate. Indeed a man in the middle could impersonate one of the parties or substitute all the message from one of the party, compromising the security of the communication. It is well acknowledged that authentication will never be perfect, meaning that there is always a non-zero probability of success from an attacker carrying out impersonation or substitution or a novel type of attack [4]. More specifically, no authentication scheme can prevent a man-in-the-middle from being successful with a probability lower than $|K|^{-1/2}$, where K indicates the size of the keyspace. This also means that for ensuring a success authentication probability p_{Auth}, the key must have at least – 2 log p_{Auth} bits [5]. To increase the security of the authentication process, the following solutions can be put in place.

   Classical cryptography solution: additional security for authentication can be achieved using public key infrastructure (PKI). A certification authority can verify the public key and the identity of a party and release a signed key and an authentication certificate, upon successful verification. In this way, Alice and Bob's identity can be certified before the authentication step can start.

   Quantum solution: the authentication steps is as for in the classical cryptography case. No additional solutions besides those available for classical cryptography are known that can be put in place specifically for quantum systems.

3) **Keys are generated by random number generators (RNG),** whose generated data can be predictable. The types of RNG [6] typically used are:

   - Pseudo-random Number Generators (PRNGs) are based on a deterministic method to generate random numbers, by expanding an initial seed. Thus they are predictable once the seed is known or due to the repetitiveness of the random sequence. Also, although the sequence of key bits are usually perfectly balanced between “0” and “1” bits, a strong long-range correlation exists, which can undermine cryptographic security.

- Cryptographically Secure PRNGs (CSPRNGs) are PRNGs specially designed to be resilient to certain cryptographic attacks. The main property is that given a sequence of *k* bits generated by a CSPRNG, it should be computationally infeasible to predict bit *k+1* with confidence greater than 1/2. Furthermore, even when all or part of the internal state of the CSPRNG is revealed, it should not be possible to deduce the numbers previously generated.

To overcome the weakness of RNGs, the following solutions can be put in place:

Classical cryptography solution: use True RNGs (TRNG) [6] based on unpredictable physical sources (e.g., thermal noise, oscillator phase-noise or jitter). However, TRNGs produce random data at relatively low rates (e.g. 20 kbps).

Quantum solution: Quantum random number generators (QRNG) [6] are a particular case of physical TRNG, that can provide true randomness and a key generation rate faster than alternative TRNGs. They are based on the detection of single photons which have either been transmitted through or reflected from a beam-splitter (half-silvered mirror). The photon starts in a quantum state which encompasses both the transmission path and the reflection path. Only when it is observed, is the path selected; at random. The randomness is therefore derived directly from the quantum measurement process.

QRNG can be used with classical cryptography and, hypothetically, a sufficiently fast classical TRNG could be used with QKD.

4) **Existing encryption protocols are not “quantum secure”**. With the advent of quantum computing, the security level of existing symmetric cryptographic algorithms (such as AES), will be halved using Grover’s approach [1]. Moreover, existing public-key cryptographic algorithms (such as RSA, DSA, ECDH) will become unsecure as demonstrated by Shor [2]. In the short term, an increase of the key length of the encryption algorithms can make them more secure against attacks, to the detriment of the processing time and complexity. In the long term, quantum computational attacks on cryptography are expected to scale too rapidly for this strategy to be effective: the longest key that could feasibly be used in encryption would not be long enough to be quantum secure.

To overcome the security concerns of the quantum-era, the following solutions can be put in place.

Classical cryptography solution: Either post-quantum encryption protocols [7] or one-time pad encryption would be necessary to overcome the security issues of the existing encryption protocols. Either solutions are not currently available: candidate post-quantum encryption protocols are still under discussion, most prominently in the exercise organised by NIST[1], and one-time pad encryption would require high rate and high security of key transmissions.

Quantum solution: one-time pad using key transmitted on quantum channels can overcome the shortcomings of the encryption algorithms. However, with current solutions, one-time pad can only support data rates limited to kbps.

In the current systems, the use of existing encryption algorithms with quantum-distributed keys does not completely address the security issue because it is theoretically possible for a computational attack, either quantum or classical, to be devised against the symmetric algorithm in which the key is to be used. However, there are good reasons to consider this risk rather remote. No plausible attack strategy on AES has been published, in the open literature at least. Symmetric algorithms are, in principle, easier to devise and make robust than asymmetric ones, because there is no need for a one-way trapdoor function. Grover’s search algorithm is believed to be optimal for an unstructured search, one for which the search must be done by brute force because no extra information is available [8][9]. Moreover, even if an attack were to be found, QKD can improve the security thanks to a more frequent update of the keys than would be possible by physical courier.

[1] [1] https://csrc.nist.gov/projects/post-quantum-cryptography

3 QKD system overview

A QKD system was assessed at JRC, to gain further knowledge about state of the art, performance and limitation of commercial equipment. This section describes the QKD system installed at JRC and reports its performance.

The installed QKD system is the Ceberis3 by ID Quantique SA (IDQ). It allows the creation of cryptographic keys by means of a quantum random generator and their exchange between two users by quantum key distribution over fibre optic lines.

3.1 QKD System Description

As shown in Figure 1, the Cerberis[3] QKD system consists of two nodes, designated Alice and Bob. The subsystems are:

- Quantum key distribution (QKD) units at Alice and Bob
- Quantum network controller (QNC) units at Alice and Bob
- Encryptors that uses the quantum-generated keys, installed at Alice and Bob.

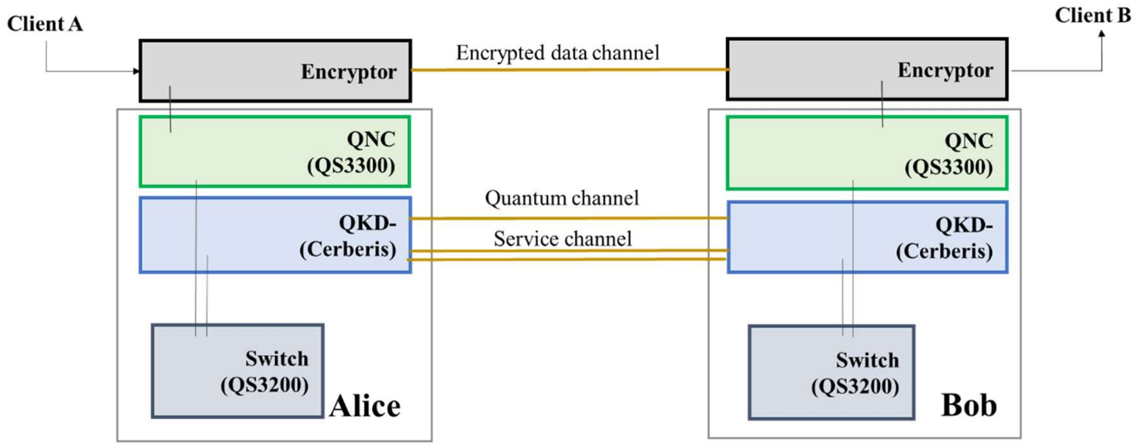


Figure 1: QKD system

Each node hosts:

- Quantum key distribution (QKD) blade: transmitter blade at Alice and receiving blade at Bob. The QKD transmitter generates the qubits that are received by the QKD receiving blade. It also supports synchronization and post-processing of quantum transmission.
- Quantum network controller (QNC) blade (QS3300): used for monitoring, managing the key and supporting the User Key Agents of the Key Entity Management System (KEMS).
- Switch blade (QS3200): used for internal communication (backplane) and chassis management.
- Encryptor: classical encryptor (based on AES256) which uses the quantum-generated key.

The nodes Alice and Bob are connected by three difference channels as follows:

- **Quantum channel**: single-mode fibre connecting QKD transmitter with QKD receiver. The quantum channel supports the qubit transmission from Alice to Bob. No active elements, such as amplifiers or repeaters, can be present in between.
- **Service channel**: a pair of single-mode fibres connecting the QKD blades. The service channels support the synchronization signals and information transmission for the QKD protocol.

- **Data channel**: a pair of single-mode fibres connecting the encryptors and carrying the quantum-encrypted data between Alice and Bob.

Note that while the network controllers, switches and encryptors are the same on the Alice and Bob sides, the QKD units are distinct: Alice's hardware is not the same as Bob's.

3.2 QKD System Configuration

The installed QKD system supports two quantum channels:

- 1550 nm
- 1310 nm

Each one is connected to a dedicated QKD system (i.e., transmitter at Alice and detector at Bob) and dedicated QNC. The pair of fibres for the service channels are connected to each QKD pair and are operating at around 1550 nm (corresponding to ITU channels 29 and 30).

The switch and the encryptors can be connected to both QNC. The overall setup with configured IP addresses is shown in Figure 2 and in Table 1 and Table 2.

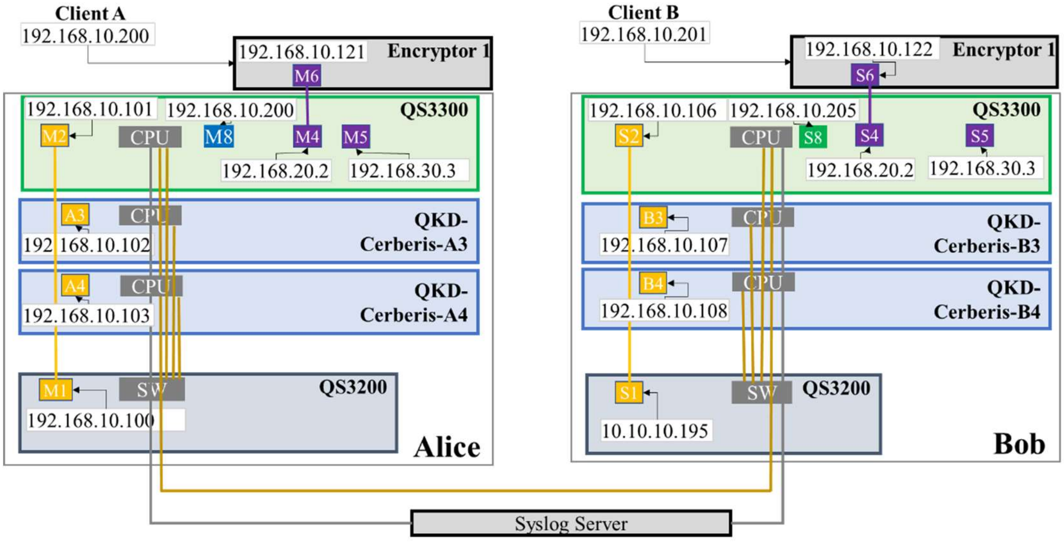


Figure 2: Configuration of the QKD system installed at JRC

Table 1: IP addresses of QKD system at Alice

ID	Description	IP address	Netmask	Gateway
M1	Switch	192.168.10.100	255.255.255.0	0.0.0.0
M2	QNC-CPU	192.168.10.101	255.255.255.0	0.0.0.0
A3	QKD-CPU	192.168.10.102	255.255.255.0	0.0.0.0
A4	QKD-CPU	192.168.10.103	255.255.255.0	0.0.0.0
M4	QNC-GbE2	192.168.20.2	255.255.255.252	0.0.0.0
M5	QNC-GbE3	192.168.30.3	255.255.255.252	0.0.0.0
M6	Encryptor1	192.168.10.121	255.255.255.252	0.0.0.0
M8	Syslog	192.168.10.200	255.255.255.0	0.0.0.0
M9	ShMM-BMC	0.0.0.0	255.255.255.0	0.0.0.0

Table 2: IP addresses of QKD system at Bob

ID	Description	IP address	Netmask	Gateway
S1	Switch	10.10.10.195	255.255.255.0	0.0.0.0
S2	QNC-CPU	192.168.10.106	255.255.255.0	0.0.0.0
B3	QKD-CPU	192.168.10.107	255.255.255.0	0.0.0.0
B4	QKD-CPU	192.168.10.108	255.255.255.0	0.0.0.0
S4	QNC-GbE2	192.168.20.2	255.255.255.252	0.0.0.0
S5	QNC-GbE3	192.168.30.3	255.255.255.252	0.0.0.0
S6	Encryptor1	192.168.10.122	255.255.255.252	0.0.0.0
S8	Syslog	192.168.10.205	255.255.255.0	0.0.0.0
S9	ShMM-BMC	0.0.0.0	255.255.255.0	0.0.0.0

3.3 Limitations and Installation Notes

- The attenuation of the service channel should be 15dB.
- The fibre length difference between the data channel and the service channel cannot exceed 15km.
- The attenuation of the quantum channel should be below 12 dB, corresponding to 50 km at 0.24 dB/km.
- Any optical attenuators used should be placed at Bob’s end.

4 QKD Architecture and Protocol

4.1 QKD Protocol

The QKD system by IDQ is based on the Coherent One-Way (COW) protocol [10][11][12]. In COW, the transmissions of the photons occur in a time slot of duration *T*. The bits '0' and '1' are identified by the different position in time of the photon in the time bin, consisting of two time slots (between vertical lines in Figure 3). Bit '0' is encoded with a pulse with average photon number α in the first time slot (|α⟩ state), and a vacuum state |0⟩ in the second time slot. Instead, bit '1' is encoded with a vacuum state |0⟩, followed by |α⟩ state. The bits are randomly selected by Alice and carry the key information.

In the COW receiver Bob (Figure 3), a small part of the signal is randomly spilled to a monitoring interferometer using a suitable coupler (beam splitter). When Alice sends two consecutive lit pulses, they interfere destructively in the interferometer and do not trigger the monitoring detector. Any detections there, for pulse pairs announced by Alice to be lit, indicate the presence of an eavesdropper Eve. Eve will be caught in this way if her detector does not trigger on one of Alice's consecutive lit pulses, so she does not know to resend it. Eve cannot avoid this happening frequently, she cannot detect every lit pulse since the weak coherent states always contain a substantial vacuum state component.

The function of the interferometer depends on the fact that attenuation of weak coherent pulses in fibre increases the proportion of the quantum vacuum state in each pulse but non-vacuum number states are still present, so consecutive pulses still interfere with each other, even after km of propagation. Whole pulses are not removed at random, instead, the average photon number is reduced continuously, the pulses remaining in coherent states. The attenuation is, in this sense, a semi-classical process, despite the quantum character of the signal.

In addition, "decoy states" consisting of two consecutive pulses |α⟩ in the same time bin, not encoding any data, are introduced in the COW protocol to better detect the presence of an eavesdropper by increasing the number of events where they can be revealed. In the original version of COW protocol – named as **COW3** in this report – these are the only decoy states used. In the revised COW protocol referred to as **COW4** [13], an additional decoy signal is introduced, consisting of two consecutive vacuum states |0⟩ in the same time bin. The encoding of COW3 and the schematic of the equipment at Alice and Bob are shown in Figure 3.

After transmission of a frame, Alice sends Bob, on an authenticated classical synchronization and distillation channel, the times of her decoy pulses. Bob discards any measurements he has made in these time bins and, on the same classical channel, sends Alice the times of remaining bins for which he has measured |α⟩|0⟩ or |0⟩|α⟩|. Alice and Bob now have agreed which time bins to use, and can construct the raw key. This key then undergoes error correction and "privacy amplification": a shorter, more secure key is derived from a longer, less secure one. These two steps require only classical computation.

The synchronization and distillation channel must be separately authenticated so that Alice and Bob know that they are really receiving information from the party they think they are receiving it from. It need not be encrypted: an eavesdropper is prevented by the quantum "no-cloning" theorem from storing a copy of the traffic on the quantum channel, so just knowing the times of the time bins Alice and Bob are using does not enable them to construct the key.

The security of the protocol is therefore based on no-cloning and on the quantum uncertainty in the measurement of vacuum or not vacuum.

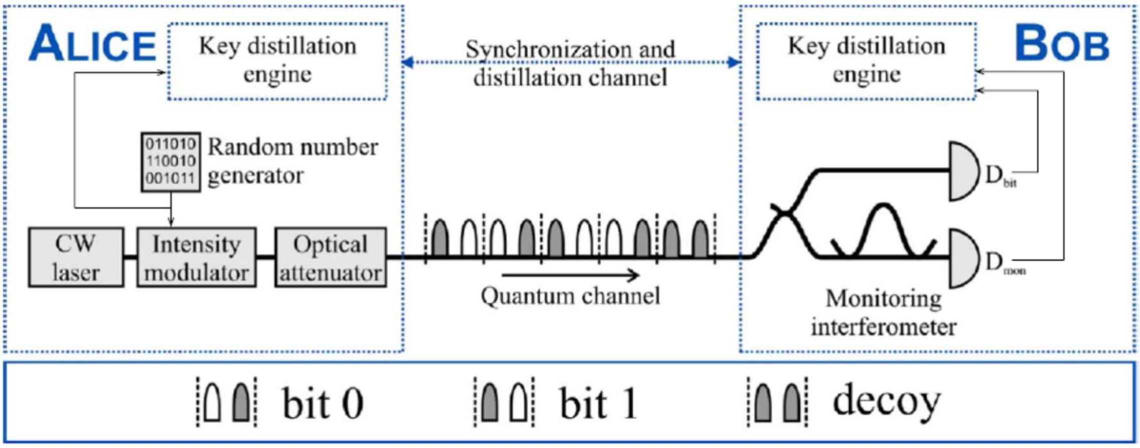


Figure 3: COW protocol (source: from [10], by permission)

4.2 Comparison with other QKD Protocols

COW falls into the class of prepare-and-measure QKD protocols, as opposed to entanglement-based. Its security is based on the uncertainty principle, the states used are not entangled.

COW is unusual in using the properties of the coherent state for themselves, not as an approximation of a true single photon state. Some QKD protocols, such as BB84, when implemented with weak coherent pulses, are vulnerable to "photon number splitting" attacks in which the small component of two or more photon states contained in the coherent state are used to copy the state. The decoy states used in COW are very different from those used to defend against photon number splitting, having in common only that they are additional states added for security purposes which do not encode key data.

Although a photon number splitting attack could be conducted against COW, it is detectable by a drop in visibility between data pulses [11].

The usual implementation of COW, as here, uses only time-bin encoding, although variants do exist with additional phase randomisation.

Moreover, COW uses a single basis of non-orthogonal signals, contrary to other prepare-and-measure protocols, such as BB84, in which two non-orthogonal bases are used, each one composed of two orthogonal signals. Thus, COW security relies mainly on the capability to receive and properly detect decoy signals for inferring the presence of an eavesdropper. Since in COW, typically, the average photon number is low and since the transmission of decoy signals cannot be increased excessively, as it would inversely decrease the key rate, the number of correctly received decoy signals is low, putting a tight bound on the security of the COW protocol [13].

COW's unique advantage is the simplicity of the hardware. No entangled photon source is needed, no true single photon source is needed, in the usual implementation no phase or polarisation modulation is needed and, most importantly, only two single photon detectors are required, the most expensive components.

4.3 Optical Architecture

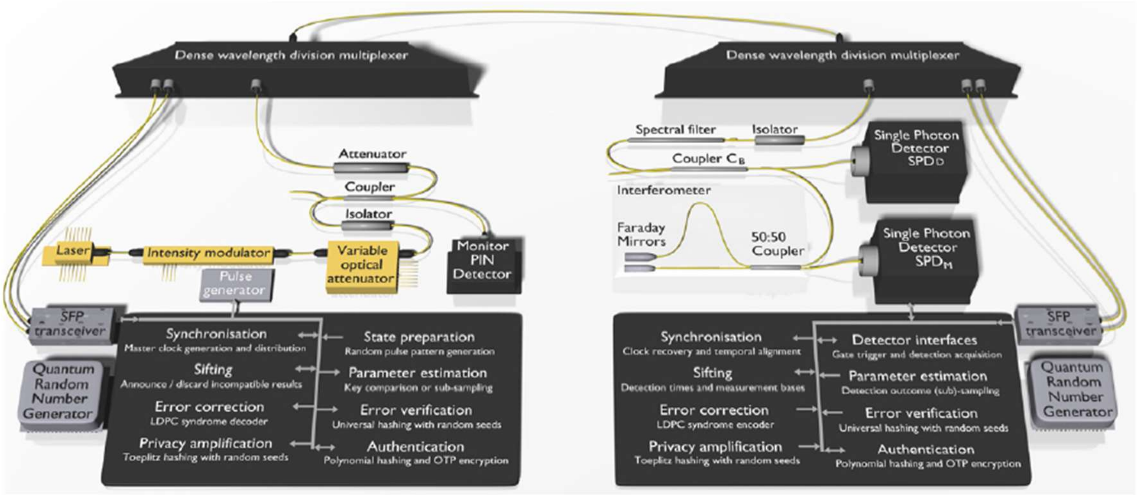

Dense wavelength division multiplexer
Dense wavelength division multiplexer
Attenuator
Coupler
Isolator
Laser
Intensity modulator
Variable optical attenuator
Monitor PIN Detector
Pulse generator
SFP transceiver
Quantum Random Number Generator
Synchronisation
Master clock generation and distribution
Sifting
Announce / discard incompatible results
Error correction
LDPC syndrome decoder
Privacy amplification
Toeplitz hashing with random seeds
State preparation
Random pulse pattern generation
Parameter estimation
Key comparison or sub-sampling
Error verification
Universal hashing with random seeds
Authentication
Polynomial hashing and OTP encryption
Spectral filter
Isolator
Coupler C_B
Single Photon Detector SPD_D
Interferometer
Faraday Mirrors
50:50 Coupler
Single Photon Detector SPD_M
Synchronisation
Clock recovery and temporal alignment
Sifting
Detection times and measurement bases
Error correction
LDPC syndrome encoder
Privacy amplification
Toeplitz hashing with random seeds
Detector interfaces
Gate trigger and detection acquisition
Parameter estimation
Detection outcome (sub)-sampling
Error verification
Universal hashing with random seeds
Authentication
Polynomial hashing and OTP encryption
SFP transceiver
Quantum Random Number Generator

Figure 4: Schematic representation of the optical setup for COW protocol (source: from [11], open access reuse)

The schematic of the optical setup implementing the QKD protocol at Alice and Bob is displayed in Figure 4 which includes also the protocol functions. At Alice's end, a laser source (multi-photon laser) generates the pulses which are then strongly attenuated by the intensity modulator and the variable optical attenuator. The intensity modulator is controlled by the quantum number generator which generates truly random bits, triggered by the synchronization signals. The phase of the pulses in consecutive time slots can be considered constant, given the long coherence time of the generator.

At Bob's end, an isolator prevents leakage of reflections or refractions from the detectors to a potential eavesdropper. The received pulses are then split by a coupler. Most of the optical power is directed in the branch toward the single-photon detector for receiving data (SPD_D). The coupler C_B spills a part towards an interferometer connected to a single-photon detector for monitoring (SPD_M). One branch of the interferometer is tuned to introduce a propagation delay of *T*, so that it produces a phase shift equal to the phase difference between two consecutive pulses (assuming a constant phase of the pulses generated by Alice), as required by the protocol, for detection of eavesdropping.

From advanced knowledge of the overall structure of Alice's signal, including the decoy states, Bob knows what statistics to expect for the detections in his two detectors. He should be able to infer the presence of an eavesdropper intercepting and resending pulses, when the statistics are anomalous, if a monitoring mechanism is implemented. A statistical method is necessary because, even in the absence of an eavesdropper, some counts will be recorded on the monitoring channel from dark-count errors in the detector.

At both Alice and Bob, an FPGA is used to boot up and optimize the system, to control the optical components, to distribute the synchronization signals, to monitor and estimate the QKD protocol parameters and to perform the post-processing operations of the COW protocols, e.g., sifting, error verification and correction, and privacy amplification.

5 QKD Performance

5.1 Testing Methodology and Metrics

The QKD system is set up with both quantum channels (at 1550 nm and 1310 nm). For testing purposes, the Alice and Bob nodes are mounted in the same rack and each quantum channel is transmitted on a single mode fibre with a fixed optical attenuator to simulate additional line attenuation.

After the initial start-up phase (performing boot up, clock synchronization and time-bin alignment, QBER optimization and visibility optimization and synchronization and security initialization), the system starts the quantum transmission and generation of the quantum keys. Time-average statistics are taken over one or more days of uninterrupted generation of keys, i.e., on a stable system running without any errors or shutdown events. The error bars indicate the confidence interval at 95% confidence level. The indicated loss is the nominal value on the optical attenuator (i.e., connector and fibre attenuation are assumed negligible).

Assessment of the system is based on metrics output by the software, based on the counts registered on the data bit detector D_{bit} and the monitoring detector D_{mon} (Figure 3).

The quantum bit error rate (QBER) is the fraction of incorrect data bits recorded on D_{bit}. The dark count rate is the fraction of counts recorded when no lit pulse has arrived.

The visibility V is calculated

$$V = 1 - \frac{N_{int}}{N_{non}} \frac{p_{non}}{p_{int}}$$

where N_{int} is the number of detections due to sequences which should interfere destructively and not be detected in the dark port, and N_{non} is the number of detections due to non-interfering sequences, p_{non}/p_{int} is the ratio between the number of interfering and non-interfering sequences sent [11]. (The "visibility" of an interferometer's output is ordinarily the difference between counts recorded at the constructive and destructive interference ports, divided by the sum of counts. Earlier research versions of COW did include a detector on the constructive interference port but it is not necessary for QKD.)

The collected metrics are:

- **raw QBER**: the QBER before correcting for dark counts;
- **dcc QBER**: the QBER value that has been corrected for dark counts and is that considered during privacy amplification;
- **avg. photon count**: number of photons that on average a qubit contains. In weak pulses as in COW, the average photon count is typically smaller than 1, i.e., some time slots are empty with no photons. To be considered that the average photon number set by Alice is 0.03;
- **accumulation time**: the time in seconds to accumulate the full raw key (of 995'328 bits). The lower is the higher is the key transfer and thus the secure key rate;
- **raw visibility**: the visibility before correcting for dark counts;
- **dcc visibility**: the dark count corrected visibility;
- **compression ratio**: for privacy amplification, the compression ratio is defined as the ratio of the final key length and the corrected key length. A compression ratio of zero means that no secret key could be distilled with the measured set of QBER, visibility and photon number values, QBER, visibility and photon number values;
- **key-block rate**: the secure key rate on a block of 995328 bits;
- **actual key rate**: the effective secure key rate[2];

[2] The documentation of the IDQ equipment did not report any detail on how the actual key rate is computed. It is likely that the actual key rate is the key rate cleared from the bits used for authentication, also referred

- **block count error**: number of quantum channel error detection in a hash block. Ideally it should be zero.

QBER is caused by different imperfections and effects:

- **Imperfections** due to qubit preparation imperfections (mainly given by the extinction ratio of the intensity modulator). According to ID Quantique, the contribution ranges between around 0.5 and 1 %.
- **Dark counts at the detectors.** They occur when the detector clicks in the presence of vacuum. Therefore, these errors become relevant at long distances or high loss. QBER due to dark counts can be estimated using the formula in [14] as follows:

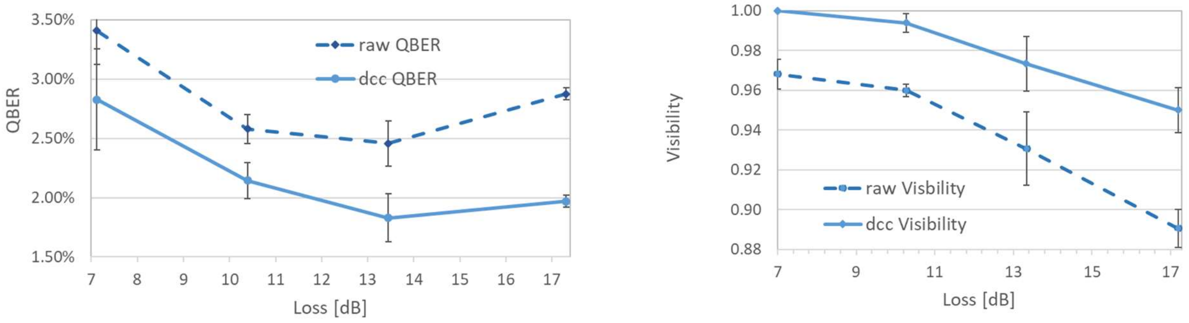
  $$\text{QBER} = \tfrac{1}{2}\, p_d\, (1- \mu\, t_B\, t\, d) \,/\, [p_d\ \ (1- \mu\, t_B\, t\, d) + (\mu\, t_B\, t\, d)]$$

  where t is the transmissivity, t_B is the splitting ratio at Bob's splitter, μ is the mean photon number per pulse ($\mu = |\alpha|^2$), f is the probability of decoy, d is the data efficiency of Bob's data detector, p_d is the probability of dark count at Bob's data detector.
- **Afterpulsing**. It occurs after an avalanche effect at the photodetector. As some trapping levels for the semiconductor remains populated with electrons, the detector must wait a fixed recovery time to empty the trapping levels. Otherwise, the detector may click in absence of an incoming pulse. Afterpulsing occurs especially at low loss.
- **Jitter**. The effect of the jitter is that some photons intended for a specific time bin are detected in the adjacent time bins. Although the contribution depends on the diode, ID Quantique estimates that jitter effect can cause a QBER around 0.2-0.5 % for a "bad" Wooriro diode[3].

5.2 Back-to-back Measurements

5.2.1 Three-state Coherent One Way (COW3): Quantum channel at 1550 nm

For the quantum channel set at 1550 nm using COW3 protocol, the time-averaged performance of the QBER, visibility and key rate are shown in Figure 5(a), Figure 5(b), and Figure 6, respectively. For the QBER and visibility, both the measured value (raw) and the dark-count corrected (dcc) value are presented.



(a) QBER vs. loss

(b) Visibility vs. loss

Figure 5: COW3: QBER and visibility of the quantum channel at 1550 nm for COW3

to as "authenticated key rate" in [11], which test the COW protocol using IDQ equipment (and using the same key block size).

[3] From an email exchange with IDQ personnel.

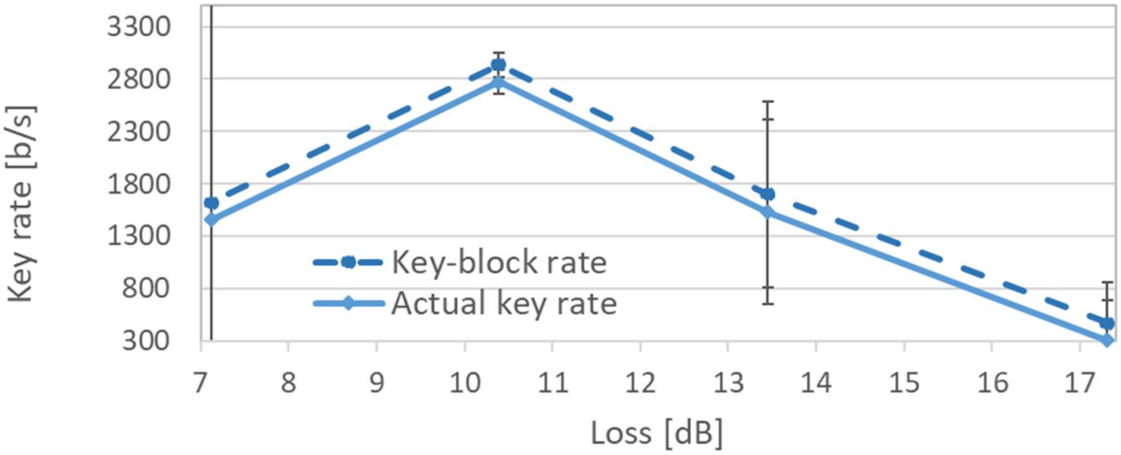


Figure 6: Key rate of the quantum channel at 1550 nm for COW3

The dynamic performance of the quantum channel at 1550 nm over a period of about 6 days is shown in Figure 7. The raw QBER is about 2.6% and the dark current corrected QBER is about 2.2%. The dark current corrected (dcc) visibility approaches 1 i.e. almost all the observed degradation is due to dark current. The key block rate is in the range of 3 kb/s. A limited number of errors occurs, in all cases at the start of a key block. This is shown in the bottom right-hand figure as a flat line at 0, the vertical axis being the fraction of a block where a stall occurred. IDQ explained that the QKD system is working properly but the FPGA may experience some race conditions between different processes triggered at the same time, leading to a brief stalling. The key accumulation quickly resumes, as soon as the triggered processes can access the FPGA resources and proceed as planned.

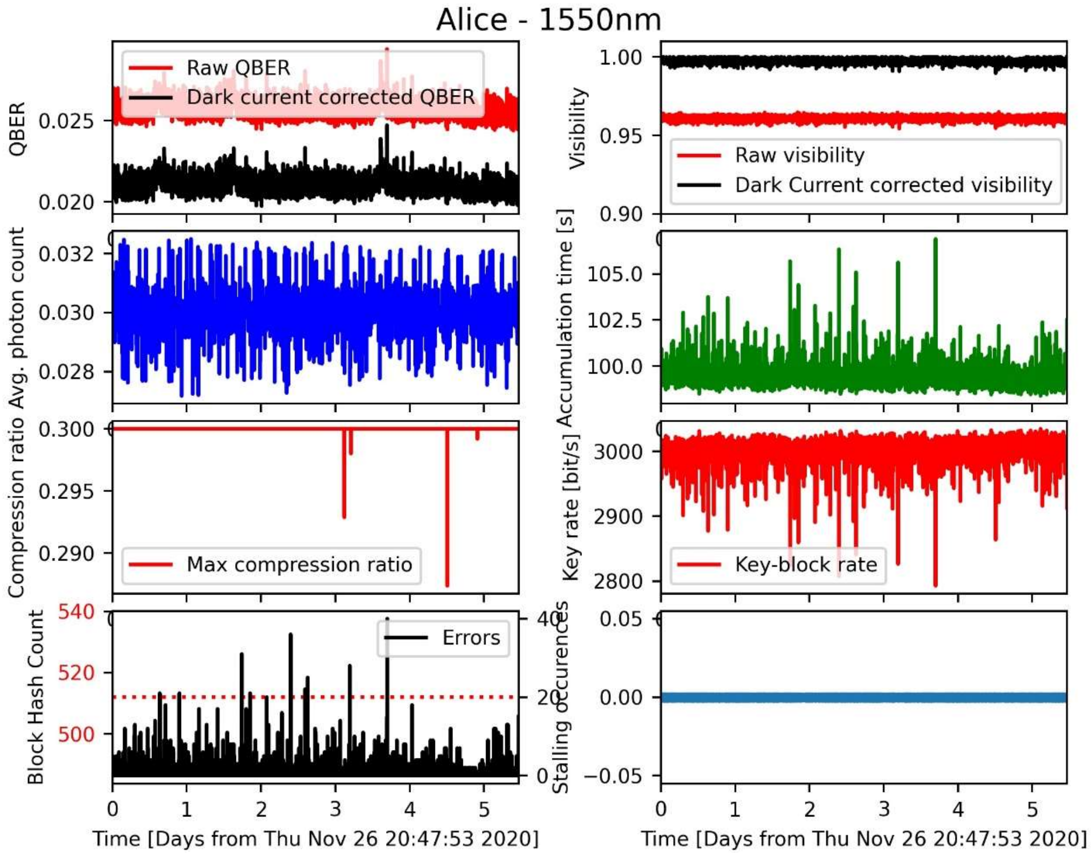
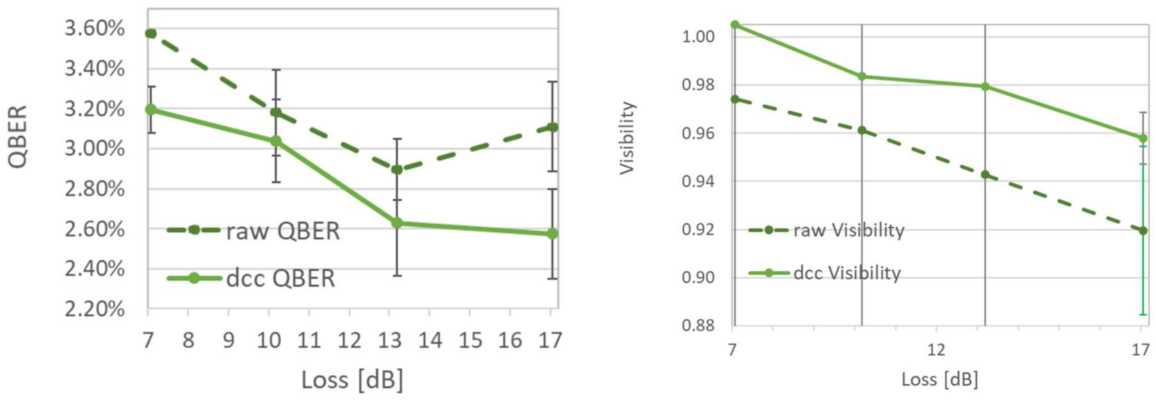


Figure 7: Dynamic performance of the quantum channel at 1550 nm with 10dB of attenuation for COW3

5.2.2 COW3: Quantum channel at 1310 nm

For the 1310nm quantum channel, the time-averaged performance of the QBER, visibility and key rate are shown in Figure 8 (a) and (b), and Figure 9, respectively.



(a) QBER vs. loss

(b) Visibility vs. loss

Figure 8: QBER and visibility of the quantum channel at 1310 nm for COW3

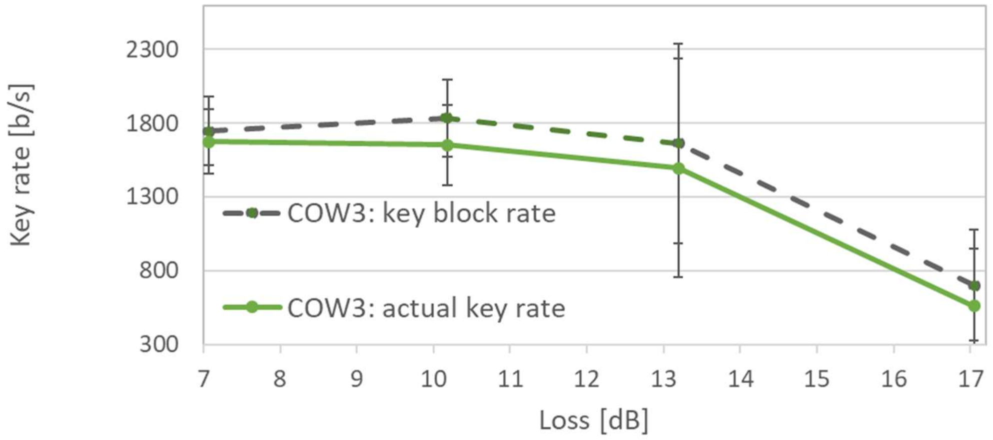


Figure 9: Key rate of the quantum channel at 1310 nm for COW3

5.2.3 COW3: Comparison between 1310 nm and 1550 nm systems

A comparison of the time-averaged performance of the quantum system at 1550 nm and 1310 nm is reported in

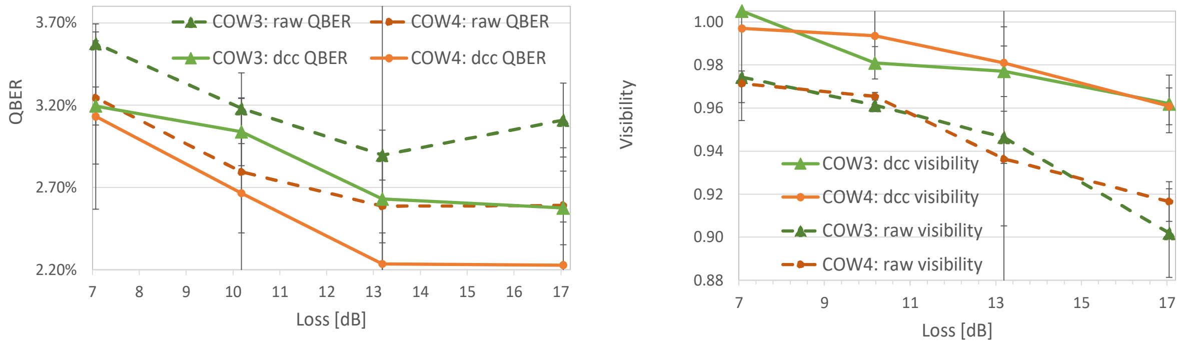
Table 3. The time-averages are averaged over multiple experiments. While the QBER is better at 1550 nm, the visibility is very similar for the two systems. Also the key rate (key block rate and actual key rate) for low attenuation (about 7 dB) is close for the two systems. However, for higher attenuation, the key rate is influenced by the compression ratio selected by the system, and other factors.

Table 3: Comparison between the time-averaged performance of the quantum channel at 1550 nm and 1310 nm in COW3

Attenuation [dB]	Quantum channel at 1550 nm				Quantum channel at 1310 nm			
	17.11 dB	13.25 dB	10.19 dB	6.92 dB	16.85 dB	12.99 dB	9.98 dB	6.87 dB
Raw QBER	2.88%	2.46%	2.58%	3.41%	2.97%	2.81%	3.23%	3.57%
Dcc QBER	1.97%	1.83%	2.14%	2.83%	2.61%	2.49%	3.07%	3.22%
Avg. photon count	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03
Accumulation time	115.88	105.18	98.37	236.87	101.91	98.49	100.66	187.96
Raw visibility	0.89	0.93	0.96	0.97	0.91	0.94	0.96	0.97
Dcc visibility	0.95	0.97	0.99	1.00	0.95	0.97	0.98	1.00
Compression ratio	0.09	0.18	0.29	0.30	0.07	0.18	0.20	0.30
Key block rate	472.11	1699.06	2936.63	1622.08	658.92	1783.61	1939.32	1631.00
Actual key rate	307.62	1530.49	2772.47	1456.21	511.14	1640.75	1769.59	1554.04
Block count error	9.51	3.03	2.39	1053.04	15.13	5.96	61.24	499.80

5.2.4 Three state versus four state Coherent One way (COW3 vs. COW4): Quantum channel at 1310 nm

Let us consider now the performance of COW4 protocol, which introduces a new decoy state, i.e., two vacuum-state pulses in succession. For the quantum channel set at 1310 nm, the time-averaged performance of the QBER, visibility and key rate are shown in Figure 10 (a) and (b) and Figure 11, respectively. The figure compares the performance to COW4 to the performance of COW3. COW4 is able to achieve a higher key rate at low loss, up to about 25% higher at 10 dB loss. Also, the QBER is improved, whereas the visibility of the two protocols is very similar, as one would expect since no additional lit pulses have been introduced.



(a) QBER vs. loss

(b) Visibility vs. loss

Figure 10: QBER and visibility of the quantum channel at 1310 nm for COW3 and COW4

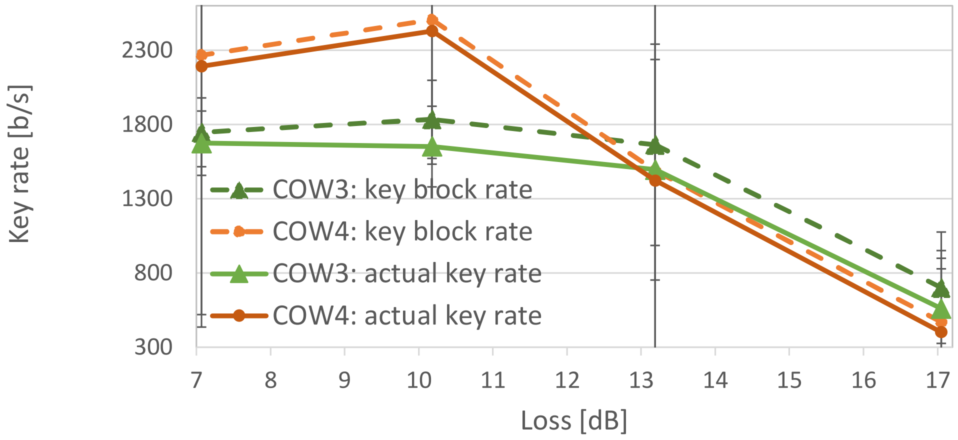


Figure 11: Key rate of the quantum channel at 1310 nm for COW3 and COW4

5.3 Field Test

5.3.1 COW3: Field test at 1310 nm

The quantum system was tested on the fibre connecting two buildings of the JRC in loopback configuration. More specifically the QKD equipment at Building 25b was connected to the fibre running from Building 25b to Building 5b, as shown in Figure 12. At Building 5, the optical fibre was cross-connected for enabling a loop-back to Building 25b. The line-of sight distance between the two buildings is approximately 300 m. Thus the propagation distance of the signal is at least 600 m (and higher if the fibre is not routed along the line-of-sight path). An additional attenuation is added to emulate longer propagation distance and to ensure that the QKD system works closer to the optimal working point (i.e., 12 dB of the considered QKD system).

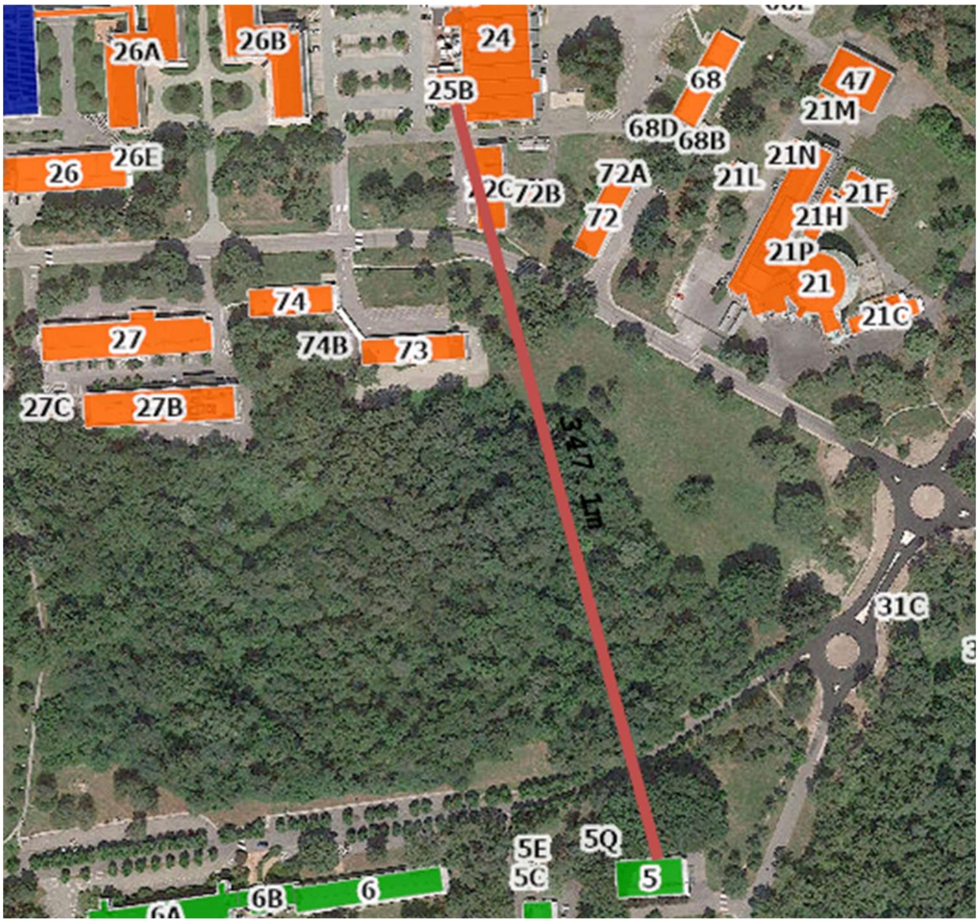
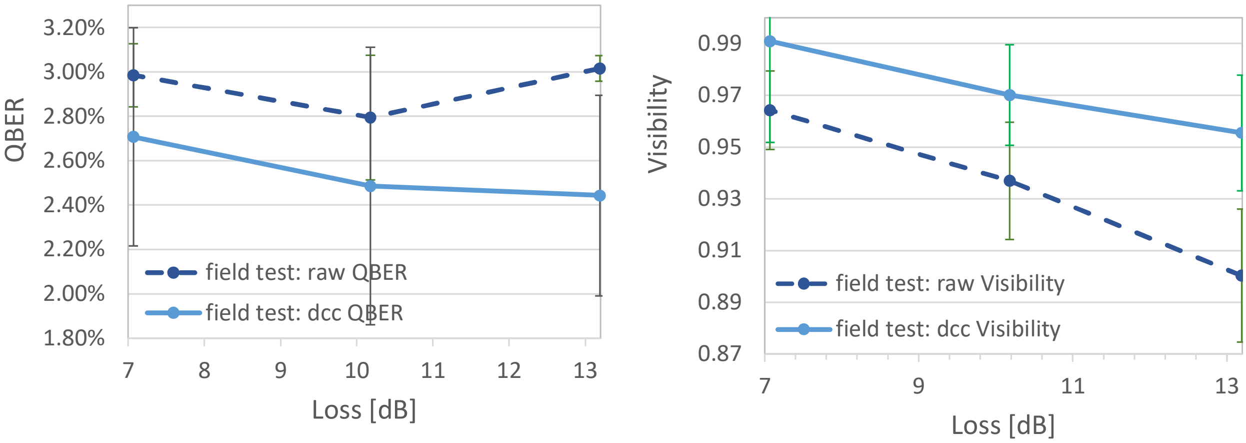


Figure 12: Map of JRC site with the Building 25b where QKD equipment is located and Building 5 where the loopback of the optical fibre was place. The line-of sight distance is about 300m

5.3.1.1 *Time-averaged performance*

For the quantum channel set at 1310 nm, the time-averaged performance of the QBER, visibility and key rate are shown as a function of the additional optical attenuation (i.e., in addition to the attenuation due to the propagation in field) in Figure 8 (a) and (b), and Figure 9, respectively. The maximum achieved key rate is about 2.5 kb/s.



(a) QBER vs. loss

(b) Visibility vs. loss

Figure 13: QBER and visibility of the quantum channel for the field test at 1310 nm

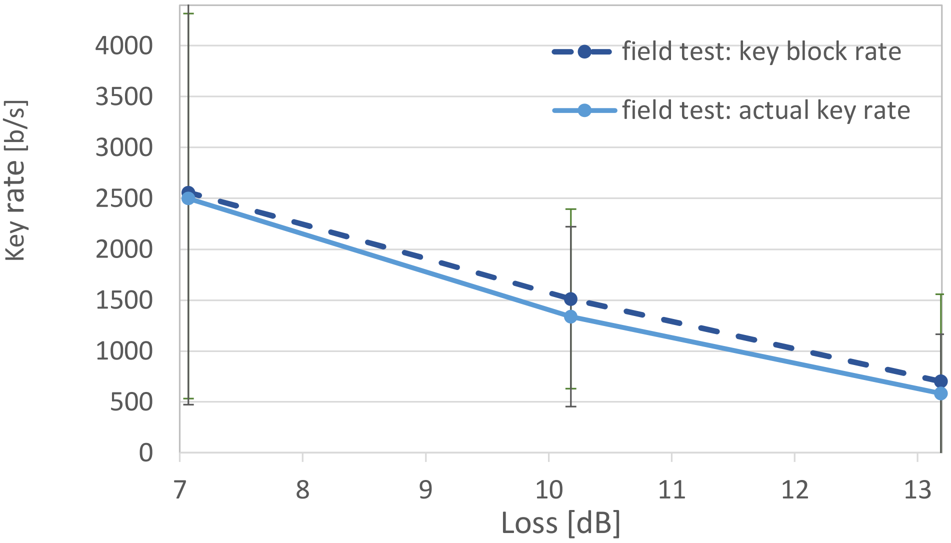


Figure 14: Key rate of the quantum channel for the field test at 1310 nm

5.3.1.2 *Variability of the performance in time*

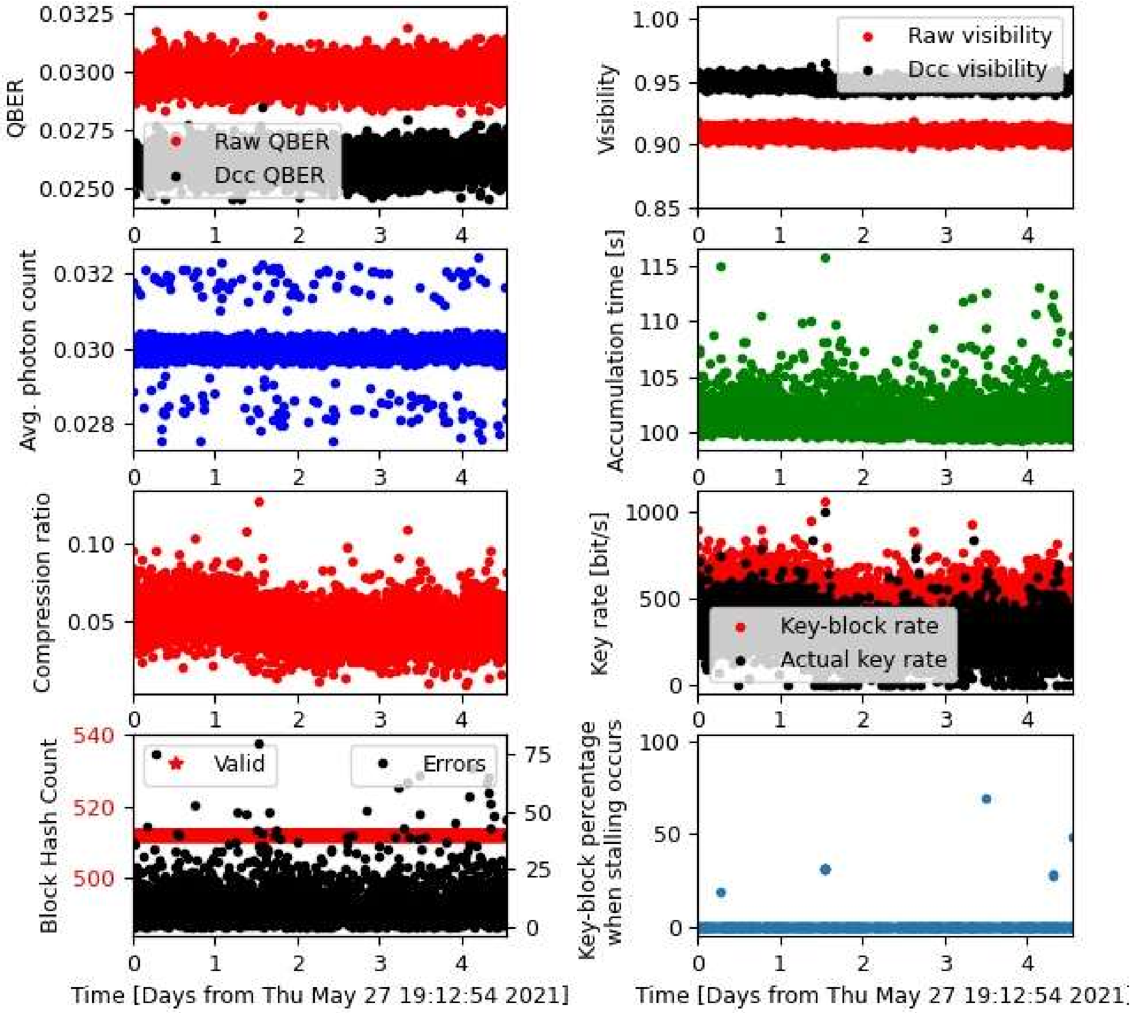


Figure 15: Performance in time for the test field at 1310 nm with 13dB additional attenuation (test on 28/5-1/6/2021)

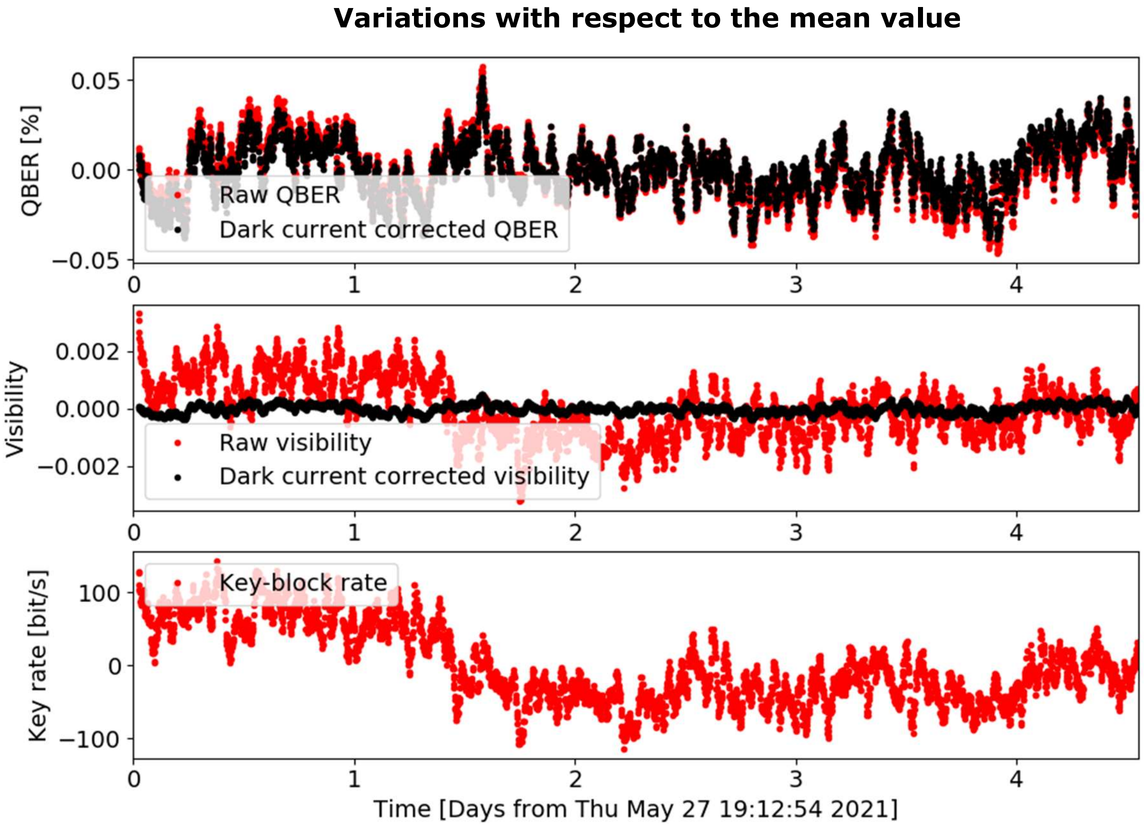
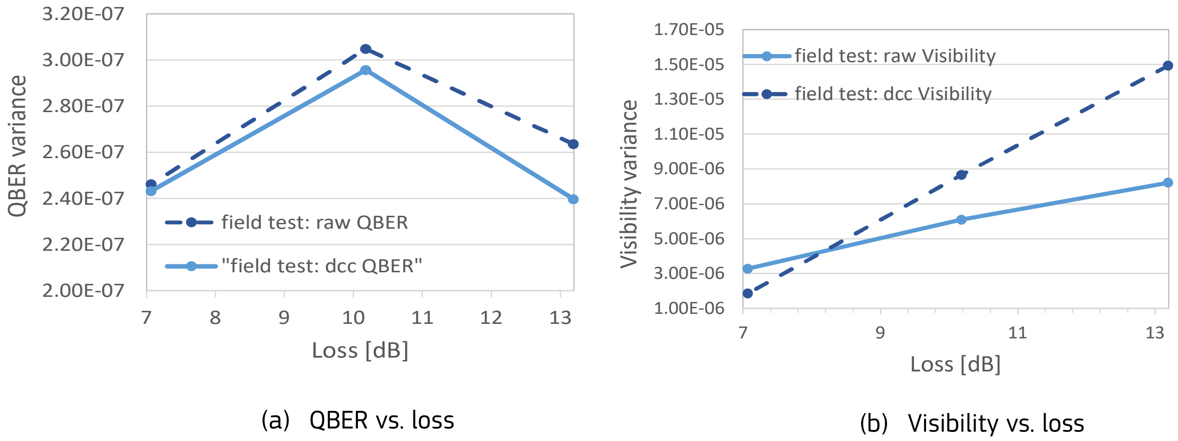


Figure 16: Dynamic performance (normalized moving average) of the quantum channel at 1310 nm with 13dB of attenuation (test on 28/5-1/6/2021)

The dynamic performance over a period of about 4 days is shown in Figure 15 and Figure 16. In Figure 16, each point represents an entry in the log provided by the command line interface (CLI) of the system. Given the variance of the entries, the normalized moving averages of the QBER, visibility and key rate are reported in Figure 16. The figure clearly shows that the variability in time of the QBER and visibility is limited, whereas the key rate can have oscillations of 100 kb/s above or below the mean value.

5.3.1.3 Time-averaged performance variations

To better quantify the time variation, the variances of QBER, visibility and key rate, averaged over multiple tests, are reported in Figure 17 (a) and (b), and Figure 18 respectively. The figures confirm that the QBER and the visibility have a limited variance, whereas the key rate suffers a high variance which is probably caused by the presence of the errors, leading to a high variation in the accumulation time (see Figure 15).



(a) QBER vs. loss

(b) Visibility vs. loss

Figure 17: Variance of QBER and visibility of the quantum channel for the field test at 1310 nm

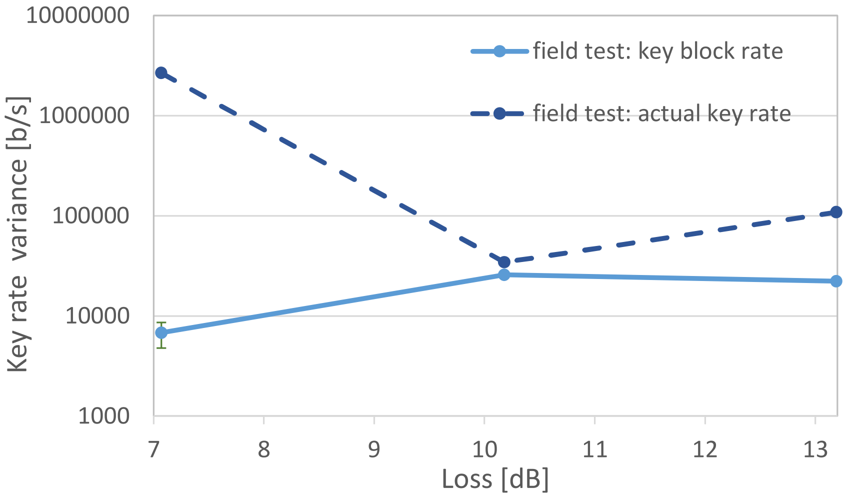


Figure 18: Variance of the key rate of the quantum channel for the field test at 1310 nm

5.3.1.4 Distribution and autocovariance of QBER and Visibility

The system has a good stability in time, e.g., the time-variation of the performance is limited, in the absence of changes of the external conditions. The variance of QBER and visibility in time is limited, as shown by the distribution of QBER and visibility reported in Figure 19, Figure 20, and Figure 21 for the field test at 1310 nm with 7, 10, and 13 dB attenuation, respectively.

Correcting for dark count improves the visibility and the QBER. A higher visibility is not otherwise correlated with better QBER.

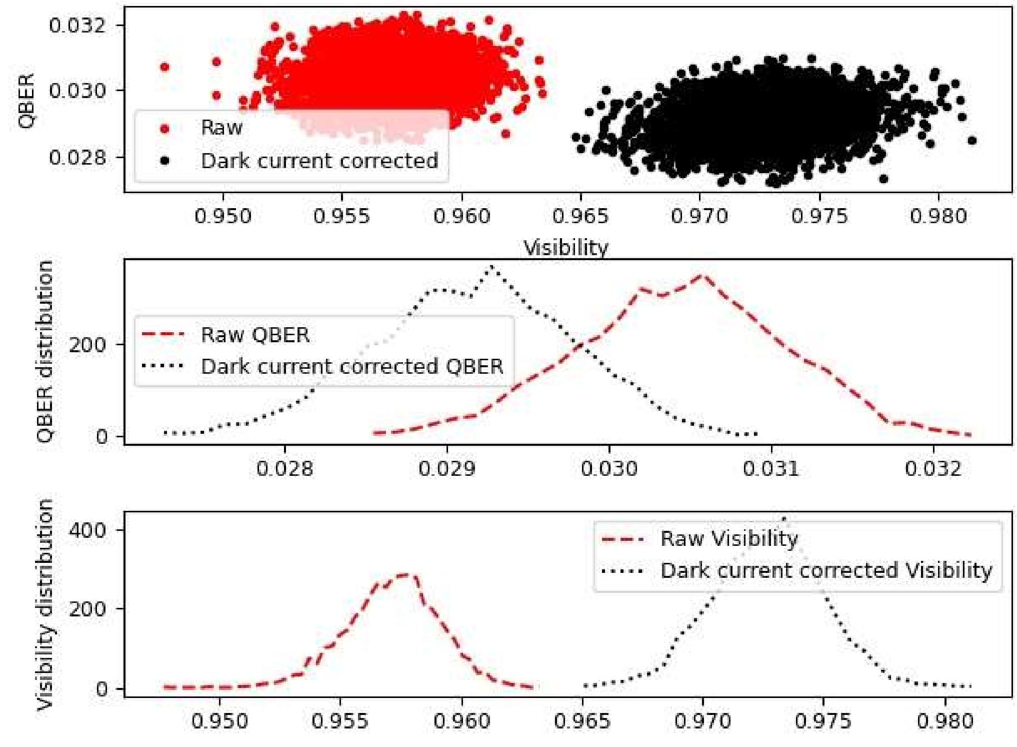


Figure 19: Distribution of QBER and visibility at 1310 nm with 7dB attenuation (test on 5-10/5/2021). The vertical axis in the bottom two plots (histograms) is the number of entries in the log file with a given value of QBER (centre figure) or visibility value (bottom figure)

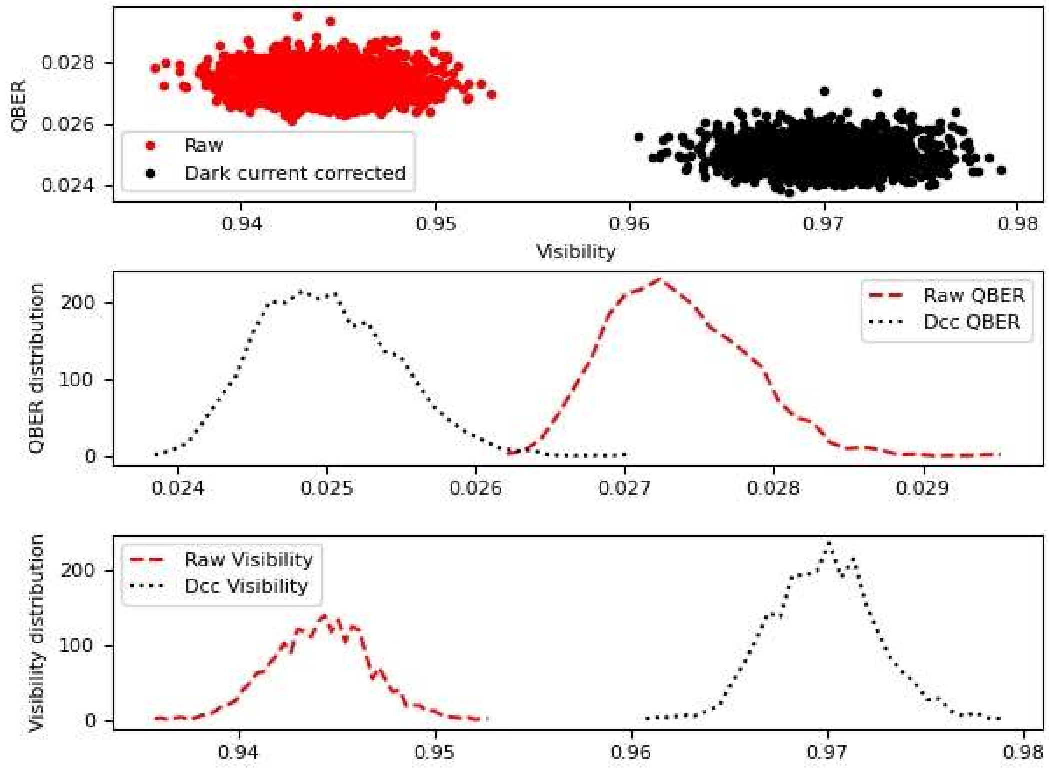


Figure 20: Distribution of QBER and visibility at 1310 nm with 10dB attenuation (test on 2-4/6/2021) The vertical axis in the bottom two plots (histograms) is the number of entries in the log file with a given value of QBER (centre figure) or visibility value (bottom figure

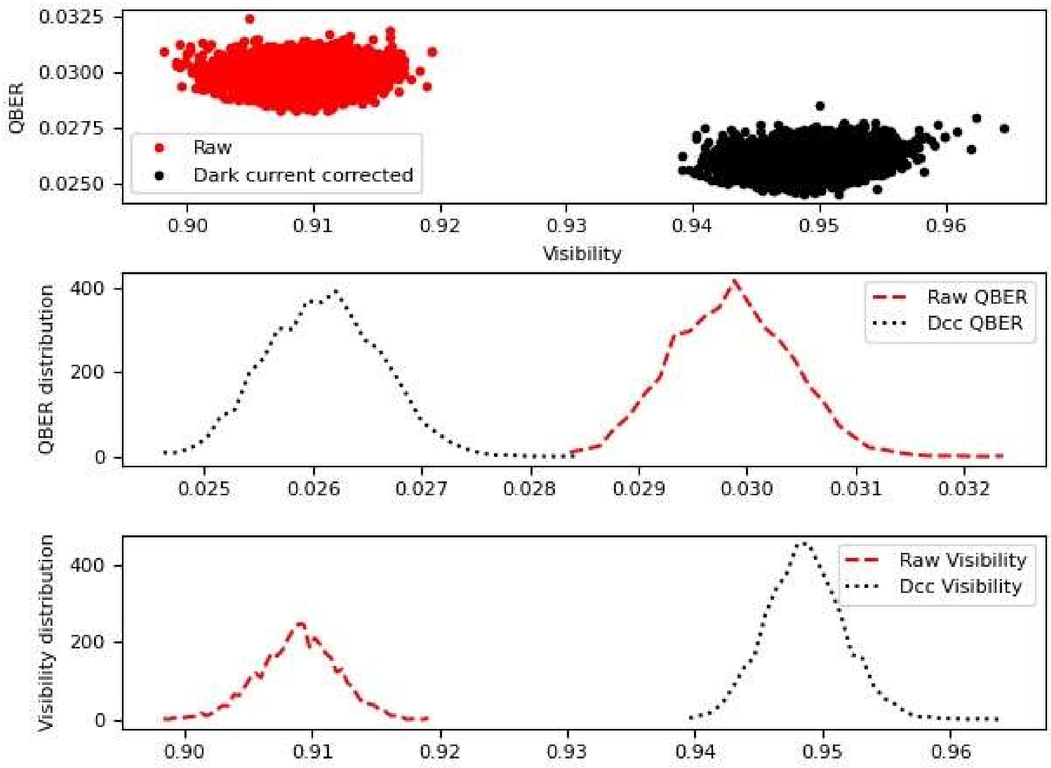


Figure 21: Distribution of QBER and visibility at 1310 nm with 13dB attenuation (test on 5/28-1/6/2021) The vertical axis in the bottom two plots (histograms) is the number of entries in the log file with a given value of QBER (centre figure) or visibility value (bottom figure

Also, the QBER and visibility performance periodically reported by the system (about every 100s) are not correlated in time as shown by the autocovariance plots reported in Figure 22, Figure 23, and Figure 24 for the field test at 1310 nm with 7, 10, and 13 dB attenuation, respectively. Since the autocovariance is concentrated at zero, there is no evidence for correlations on any particular time interval. In the case the autocovariance were not concentrated at zero, it may mean that the QKD system may not run in ideal conditions (e.g., for the presence of external light or for fibre connectors not tight enough that may introduce photons causing degradation and correlation of QBER and visibility).

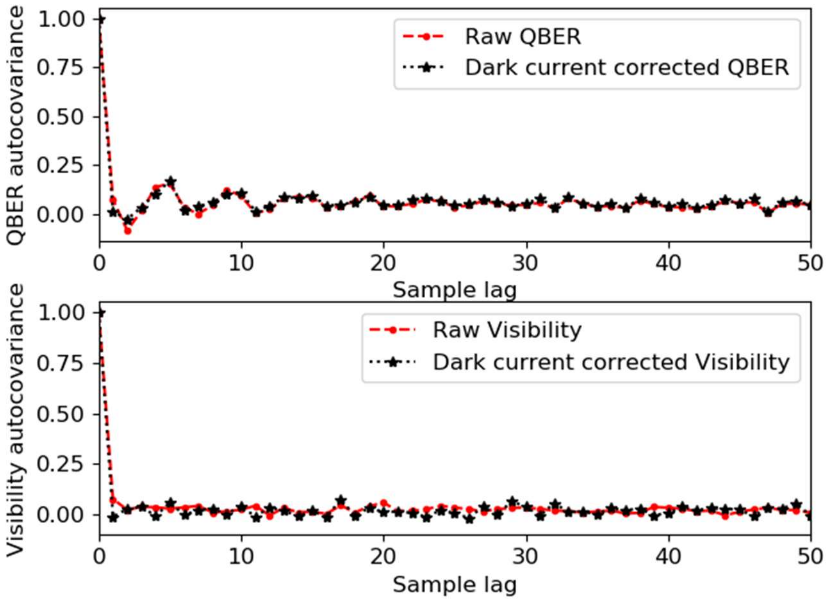


Figure 22: Autocovariance of QBER and visibility at 1310 nm with 7dB attenuation (test on 5-10/05/2021)

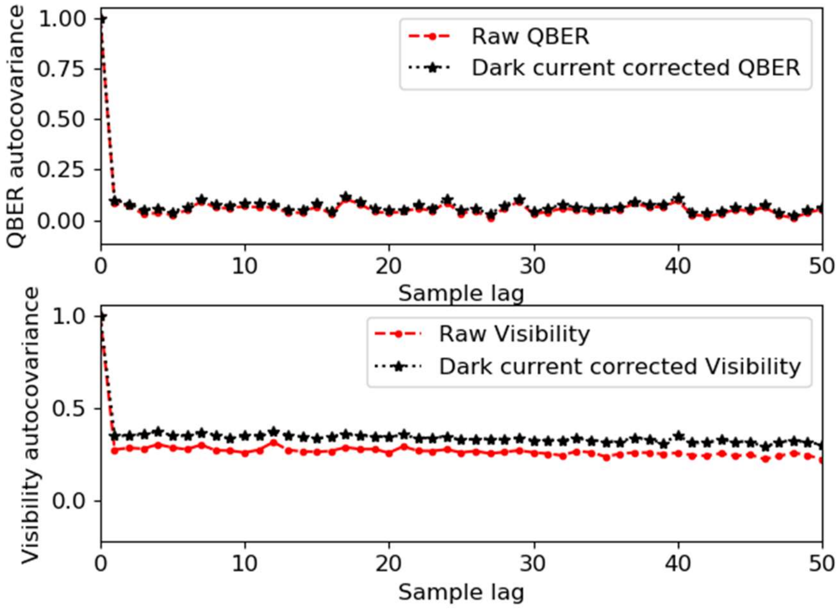


Figure 23: Autocovariance of QBER and visibility at 1310 nm with 10dB attenuation (test on 2-4/6/2021)

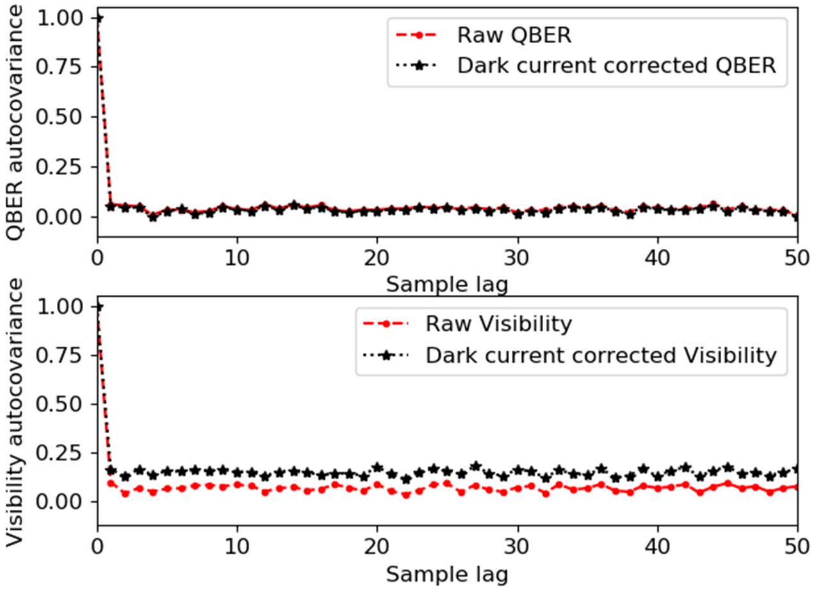
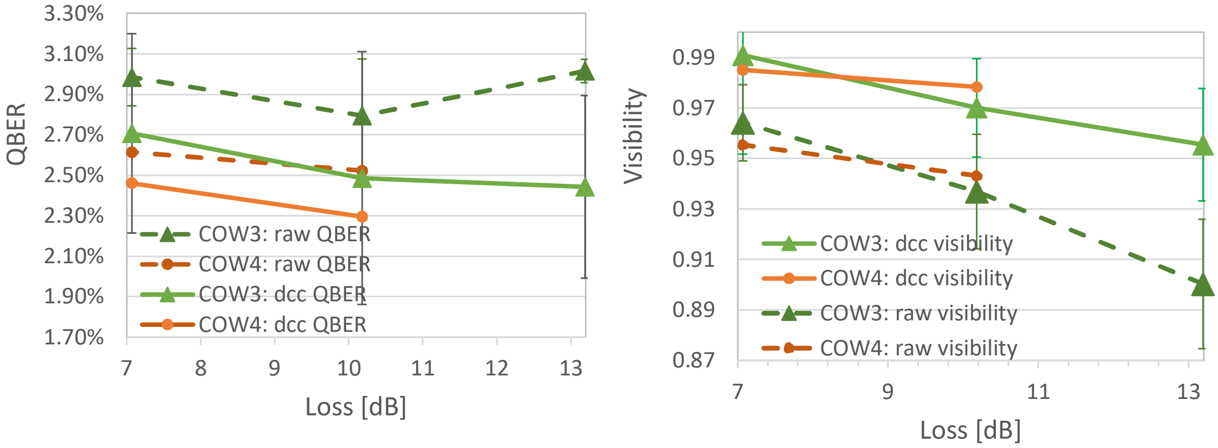


Figure 24: Autocovariance of QBER and visibility at 1310 nm with 13dB attenuation (test on 28/5-1/6/2021)

Instead, repetitions of the same test under the same conditions causes a rather high variability, leading to an ample confidence interval. This can be due to the changes in the connector interfaces on the quantum channel, but also to the optimal working point (e.g., optimal intensity modulator voltage, laser power, delay for synchronization) which is automatically found by the system. Small changes in the optimal working points or on the physical channel (e.g., cleanness of the connector interfaces) may lead to distinct performance.

5.3.2 COW3 vs. COW4: Quantum channel at 1310 nm

Let us compare the performance of the COW4 protocol with that of COW3, in the field test setting. For the quantum channel set at 1310 nm, the time-averaged performance of the QBER, visibility and key rate are shown in Figure 25 (a) and (b) and Figure 26, respectively. Due to technical and time constraints, the measurement at 13 dB loss was not taken. The measurements confirm the finding that COW4 maintains the same visibility of COW3, but the QBER at low loss is improved. The lower part of figure 26 compares the secret key rate with the system running COW4, to that with it running COW3. Also the secret key rate at 10 dB of additional loss is improved, whereas further tests may have been necessary to confirm the lower key rate at 7 dB.



(a) QBER vs. loss

(b) Visibility vs. loss

Figure 25: QBER and visibility of the quantum channel at 1310 nm for the field test with COW3 and COW4

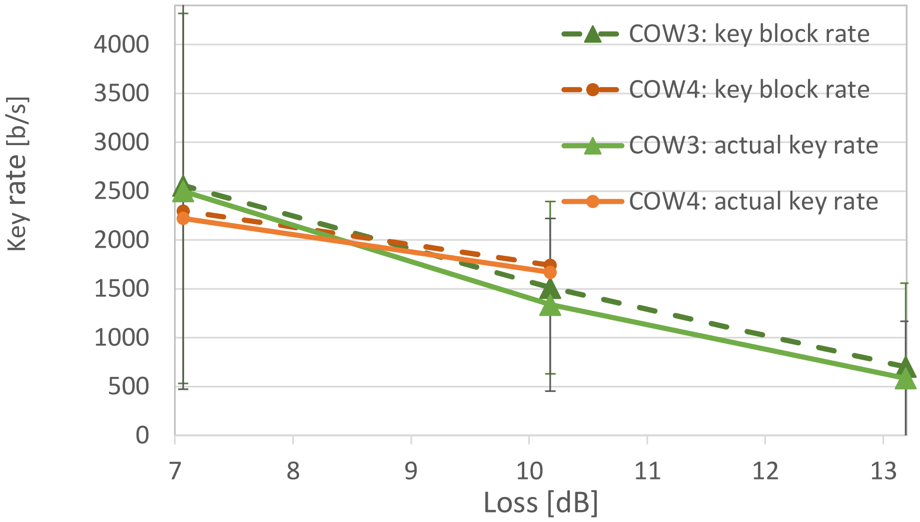


Figure 26: Key rate of the quantum channel at 1310 nm for the field test with COW3 and COW4

5.4 Critical Issues and Limitations experienced during the testing

5.4.1 Sensitivity to Temperature

The system is provided for typical use in data centres. From testing, it was noticed that temperature-related warnings (e.g., in the QKE host) were raised when the room temperature was around or above 21°C and in absence of forced ventilation. Best operating range in the room was for temperature below 21°C, with high fan speed.

5.4.2 Sensitivity to Light

The general recommendation is to install the QKD systems in server rooms. No specific indication of sensitivity to light was indicated by the manufacturers at the time of installation. However, it was noticed that excessive dark counts occur when light (even dim light) is present in the room or there are light reflections. The increase of dark counts augments the QBER and in some cases the visibility, to the point of causing a "stalling" of the key generation process (see Figure 27 bottom-right). In this case, the stalling of the key accumulation could occur statistically at any instant of the key accumulation (i.e., it was not only due to the race condition issue of the FPGA processes). Moreover the duration and frequency of the stalling was higher, reducing considerably the key rate especially during day time. By darkening the room hosting the QKD system, the performance especially at low attenuation improved significantly, avoiding the daily oscillation of performance caused by sunlight filtrating through the curtains.

Given the difficulty to control the room light in a measurable way, a quantitative assessment of the light on the performance was not carried out.

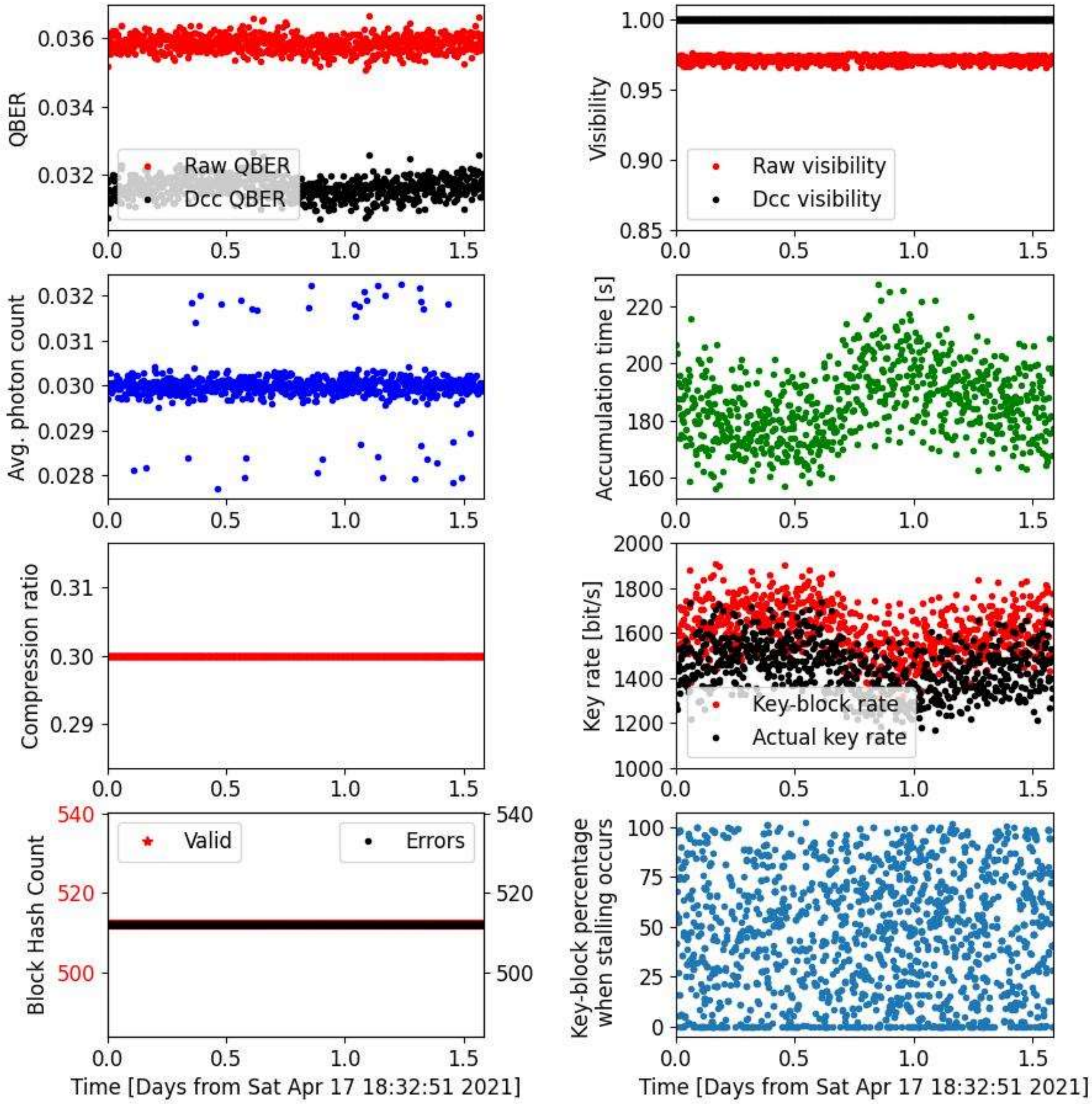


Figure 27: Performance of the system at 1310 nm with 7dB of attenuation. The errors and the variations of the accumulation time and key rate are visibly affected by the sunlight during the afternoon.

5.5 Security of the Protocol

According to [13] dated 2009, for the COW protocol no lower bound is known for the unconditional security, i.e., a proof of security "*without imposing any restriction on the computational resources or the manipulation techniques that are available to the eavesdropper acting on the signal*" was not (yet) known.

According to [16] published in 2020, the upper security bounds on the secret key rate of COW scales quadratically with the system's transmittance and thus "this approach does not seem to be appropriate for long-distance QKD transmissions".

In [17] published in December 2021, a zero-error attack against COW3 is presented, reducing the upper bound on the secret key rate of COW3 to more than an order of magnitude lower than previous upper bounds. The authors claim that this zero-error attack is optimal, as no other attack can reduce the maximum achievable distance in absence of errors. This new bound restrains significantly the maximum achievable distance for a secure key rate to values as low as 22 km. Please note that this bound is only exemplary, as the exact value would depend on the parameters of the QKD system, including the quality and attenuation of the fibres.

The work on the security of the COW3 protocol provides the most stringent bound against the zero-error attack [17]. To reduce the impact of the zero-error attack, the 4-state COW protocol (COW4) has been proposed in [13] along with additional performance metrics for detecting the presence of eavesdroppers. The theoretical discussion of the security of the COW protocols is beyond the scope of this report.

With the zero-error attack in [17], an eavesdropper Eve can intercept quantum signals without being detected. Such an attack exploits the fact that the transmission of vacuum pulses by Eve is not detected by Bob and allows her to break the entanglement-based channel. Indeed, if Eve injects one or more vacuum pulses, Bob will not be able to distinguish the vacuum sent by Alice from those sent by Eve and from the photon losses. Thus Bob may not be able to detect an eavesdropping, unless some other QKD performance parameter (such as the QBER) is monitored. In any case, occasional vacuum sent by Eve may pass undetected, permitting her to continue undisturbed the intercept-and-resend attack.

This weakness has been detected also on the IDQ system under test. When disconnecting the fibre carrying the quantum signals, the process of collecting the keys stalls. When re-connecting the fibre with the same or a different attenuation, most of the time the process of key collection and generation resumes after a few tens of seconds of "stalling" for optimizing and regulating the QKD system for resuming the key accumulation. No errors are generated due to the interruption of the transmission if it lasts few minutes (e.g., less than 3 minutes in COW3). As such, an eavesdropper could then resume the transmission without being detected. An example is given in Figure 28 and Figure 29, where the attenuation of the system at 1310 nm (in back-to-back configuration) was changed from 7 dB to 10 dB (at time 1 h approximately) and then to 13 dB (at time 4h approximately). The system did not report any error, only a brief period of stalling occurred during the change of attenuation (see plot 3 and 4 in Figure 28). The same behaviour occurred also in COW4 and even longer stalling durations were supported.

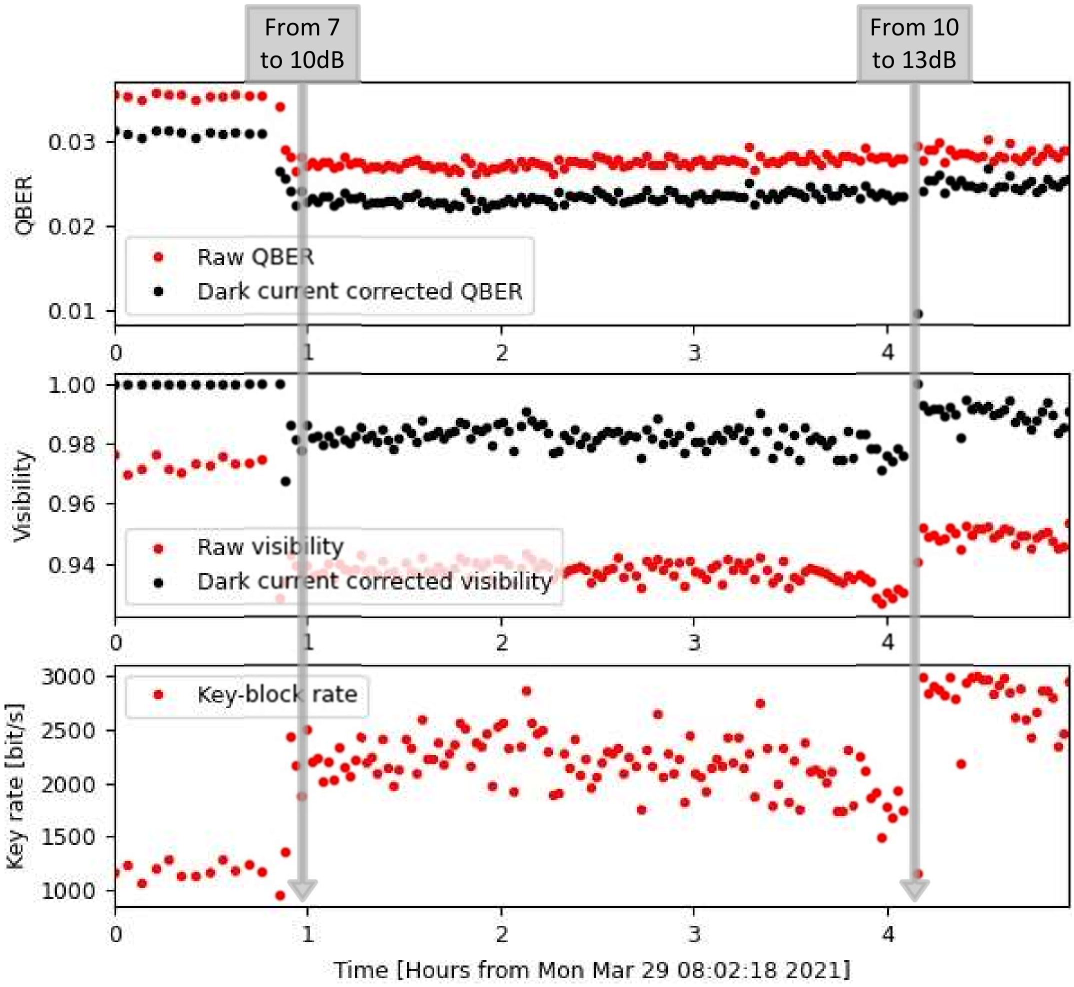


Figure 28: Performance in time when attenuation was changed from 7 to 10 (at hour 1) and then to 13dB (at around hour 4), without errors in the system (test on 29/3/2021)

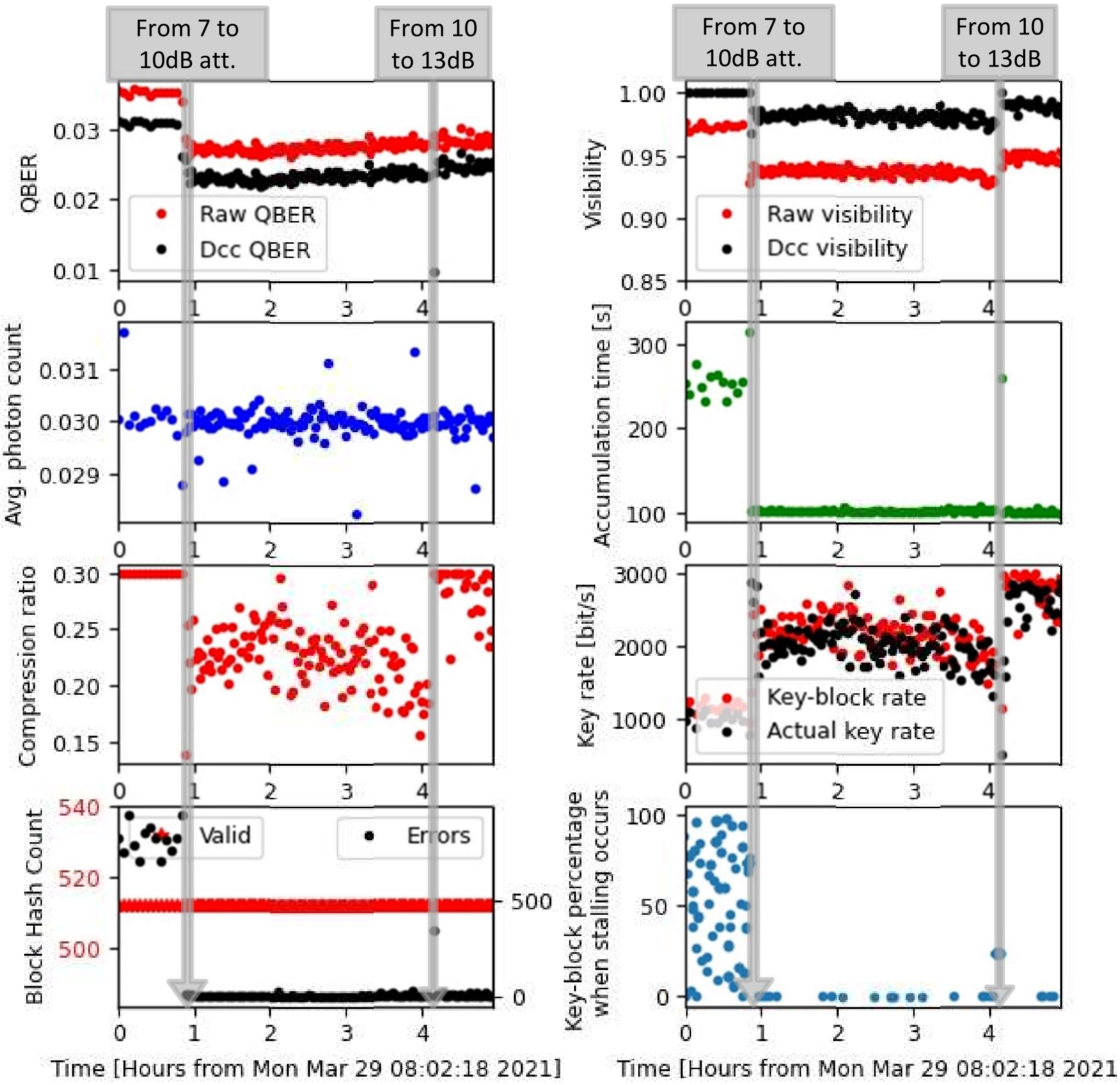


Figure 29: Additional performance in time when attenuation was changed from 7 to 10dB and to 13dB, without errors in the system (test on 29/3/2021)

With the upgrade of the system performed by IDQ in December 2021, a graphical interface for online monitoring of the key performance was provided. Users can set trigger alarms that can help to detect intrusions. In comparison, the command line interface (CLI) provides only indications of QBER and visibility.

However, an autonomous mechanism was not available for triggering alarms in case of anomalous behaviour that could be related to eavesdropping or other attacks. For instance, in the new release of the QKD system supporting COW4 the fibre carrying the quantum channel could be disconnected up to 16 minutes without alarms being triggered (system rebooting occurred after 16 minutes).

More importantly, for enhancing the security it is important to monitor other key performance parameters, as suggested also in [13]. Indeed, the zero-error attack in [17] is assessed from the gain of the key generation that is the number of “detection clicks” per signals transmitted by Alice. A monitoring of such performance, as well as of the attenuation, can help to detect any change in the quantum channel, which may be caused by malicious users. Such changes may be caused also by other non-malicious reasons which may require a prompt fix for a proper functioning of the system. It can also be objected that this defence could be implemented on a classical system using weak coherent states and conventional cryptography: there is no quantum advantage.

5.6 Quality of the quantum channel and stalling occurrences

Current performance of IDQ setup is affected by “stalling” events, i.e., temporary suspension of the key accumulation due to errors. This occurs when photons are not received (e.g., due to a temporary increase of the loss). Typically it occurs with higher probability when the connectors or the channel are not sufficiently clean, or in the presence of external factors (e.g., environment light). In general, in the tests at the JRC, the degree of care required with the quantum channel connections to achieve satisfactory performance was more than would be needed for a conventional fibre-optic network. In addition from the tests, it was evident that occurrence of stalling events is more frequent at the very beginning of the key generation cycle (at 0%) as shown in Figure 7 and Figure 30. This is due to the behaviour of the FPGA implementing the QKD protocol (i.e., due to race condition among different timers on parallel operations) and, according to IDQ response, it does not impact the final key rate.

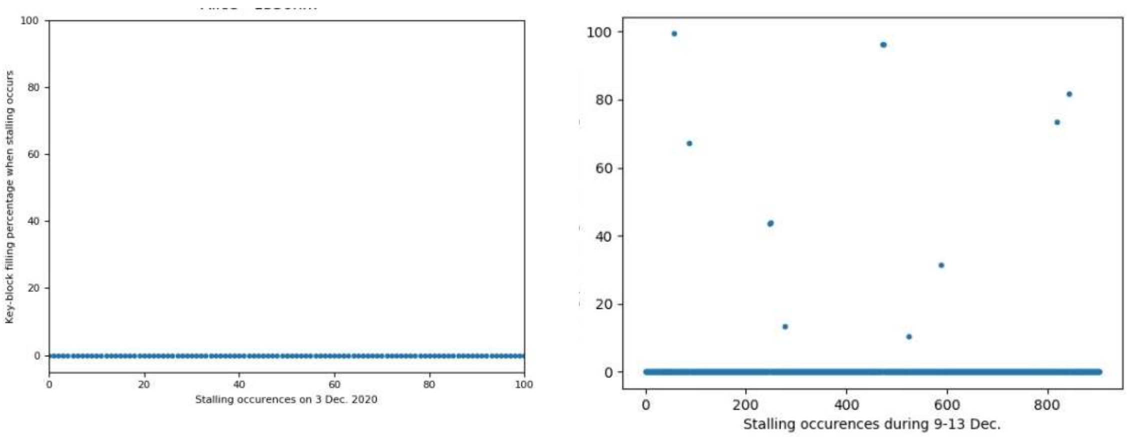


Figure 30: Stalling occurrences at different key-block filling percentage for the system at 1550 nm (left) and at 1310 nm (right)

5.7 Reliability of the Hardware

During the 19 month lease, the QKD equipment at 1550 nm experienced the following major failures:

- a failure of the intensity modulator, which required a repair after about 8 months of uninterrupted operations;
- endless loop performing “cooling down of the detector” during booting-up.

Other minor issues were experienced and solved thanks to the technical support of ID Quantique, by typically performing a complete reboot of the system, including a power off of the equipment.

While the testing of the QKD systems was aimed at testing the performance (a task that may have put the system under higher stress due to the changes of attenuation) and not at testing the reliability, the presence of multiple errors, warning and failures during the testing period indicated that:

- a constant monitoring of the system is important in order to promptly resolve the issues;
- automatic mechanisms for self-recovery and rebooting are important and may enable automatic solutions of some or most of the reliability issues;
- the mean time between failure (MTBF) needs to be properly assessed and evaluated before installing the systems in difficult to reach locations (e.g., satellite, inhospitable locations).

5.8 Management and Control Limitations

A comprehensive and integrated management and monitoring tool for the QKD and QNC system and for the encryptor should provide in real time:

- management of the equipment (i.e., QKD system and encryptors)
- online graphical monitoring the performance (i.e., of the quantum channel and of the encryptor)

- ability to raise alarms and warnings, display errors, and events.

As already mentioned, the quantum channel of IDQ system can be managed and monitored in textual mode via command line interface or via SNMP client. From the software release of December 2021, an online management interface was provided, allowing also the dynamic performance monitoring. However, it appeared that the events for alarms and warnings are to be set by the users.

The IDQ encryptors can be managed and monitored via the proprietary KEMS (Key Encapsulation Mechanism System) interface, which enables also the configuration of the system (e.g., IP addresses and setting such as refresh rate of the keys) and the visualization of the performance.

In addition to the previous requirements on the management interface, a controller able to interface both tools, providing online monitoring and dynamic performance control would be useful, making the system remotely manageable and configurable according to software-defined networking principles. For instance, based on the monitoring key rate, the key-change rate of the encryptor can be adjusted dynamically in order to ensure the maximum security (i.e., highest refresh rate) and reliability (e.g., storage of a set of keys) to avoid disruption in case of temporary failures or drop of key rate.

6 Conclusions

This report documented the installation and performance of the Cerberis^3 QKD system at JRC. The following main characteristics, strengths and shortcomings of the tested QKD system, which is representative of the state of the art, were found:

The QKD system can be easily **integrated with optical network equipment** (e.g. commercial system can use the ITU-T channels), but integration with deployed optical networks would be limited to short, unamplified links, such as in access network with point-to-point links. The reason is that quantum communication cannot be amplified and are limited in maximum reach (about 17 dB of loss for the system under test, corresponding to a typical distance of 85 km). In addition, other types of QKD protocols (e.g., multi-party QKD protocols based on entanglement) would be required for a network with multiple nodes exchanging keys.

The tested QKD systems provide a **secure key rate** (up to 3 kb/s in the measured system) significantly lower than the bit rate of optical communication (in the order of several hundreds of Gb/s per channel, with hundreds of channels carried in a fibre). Newer QKD systems from other vendors can reach higher rates in the order of hundreds of kb/s. Still, one-time pad (OTP) quantum communications would be limited to applications requiring only very low data rates. It is not yet at an adequate level of maturity for high rate optical communication.

Robustness and **reliability** of the tested apparatus (e.g., sensitivity to environmental conditions, robustness to degradation due to usage) would require technical improvements, to ensure the high quality of service required by optical networks and in future in satellites.

Stability of the tested system in time was good, but repeatability was rather poor due to the sensitivity of quantum channels to imperfections, making the troubleshooting and the rebooting procedure a tedious and time-consuming process (especially in the first release of the software). Careful cleaning of fibre ends at the connectors is mandatory and several attempts may be needed to achieve a good enough connection.

Security of QKD protocols is an area still open to research. Standardization can proceed only once the security proofs are consolidated and have the consensus of the whole scientific community. As such, the QKD protocol used in the tested equipment was recently demonstrated to be unsecure even for short distances. This example clearly highlights the lack of maturity for commercial or governmental deployment, in the area of QKD protocols and security demonstrations.

The tested system was found to not be able to detect possible **attacks** (e.g., man in the middle attack). Improvements especially in the monitoring of the performance are required for 1) detecting any performance degradation or change, which can be caused by an attacks, 2) raising alarms, and 3) aborting the communication when necessary. The inability to detect a possible attack pose at risk the infrastructure. To avoid that, certification of the equipment system must be pursued by the standardization bodies and vendors.

The available control and management interfaces provides a basic set of operations. **Additional functionalities**, the support of interfaces (e.g., standardized), the integration with controllers would be important features for network operators, to enable the intelligent control of the systems and the disaggregation of the network.

We recommend that coherent one-way (COW) protocols should not be used in operational EuroQCI until security weaknesses against zero-error and other send–resend attacks are better understood, including if the four-state version of COW adequately resolves the vulnerabilities.

We further recommend that QKD systems should be thoroughly tested for their ability to provide a continuous and reliable service when installed in realistic environments. Robustness against changes in ambient temperature and lighting should be verified.

References

[1] Grover, L. K., “A fast quantum mechanical algorithm for database search,” in proc. STOC96: ACM Symposium on Theory of Computing Philadelphia, Pennsylvania, USA, May 22 - 24, 1996.

[2] Shor, “P. “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer” SIAM Journal of Computing, 26, pp. 1484-1509, 1997.

[3] Sajeed, S., Chaiwongkhot, et al. “An approach for security evaluation and certification of a complete quantum communication system,” Scientific Reports, 11(1), 1-16, 2021.

[4] Van Assche, Gilles, “Quantum cryptography and secret-key distillation,” Cambridge University Press, 2006.

[5] U. Maurer, “Authentication theory and hypothesis testing,” IEEE Transactions on Information Theory, vol. 46, no. 4, pp. 1350–1356, July 2000.

[6] Piani, M., Mosca, M. and Neill., B. “Quantum random-number generators: Practical considerations and use cases,” 2021.

[7] Bernstein, Daniel J. “Introduction to post-quantum cryptography,” *Post-quantum cryptography*. Springer, Berlin, Heidelberg, 2009.

[8] Boyer, M, et al, “Tight bounds on quantum searching”, Fortschritte der Physik: Progress of Physics 46.4-5, pp. 493-505, 1998.

[9] Zalka, C., “Grover’s quantum searching algorithm is optimal,” Phys.Rev. A60, pp. 2746-2751, 1999.

[10] Constantin, J., Houlmann, R., Preyss, N., Walenta, N., Zbinden, H., Junod, P., & Burg, A. “An FPGA-based 4 Mbps secret key distillation engine for quantum key distribution systems,” Journal of Signal Processing Systems, 86(1), 1-15, 2017.

[11] Walenta, N., Burg, A., Caselunghe, D., Constantin, J., Gisin, N., Guinnard, O. et al. “A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing,” New Journal of Physics, 16(1), 013047, 2014.

[12] Stucki, D., Brunner, N., Gisin, N., Scarani, V., & Zbinden, H. (2005). Fast and simple one-way quantum key distribution. Applied Physics Letters, 87(19), 194108.

[13] Curty, M. “Foiling zero-error attack against coherent-one-way quantum key distribution,” Physical Review A, 104, 2021.

[14] Gisin, N., Ribordy, G., Zbinden, H., Stucki, D., Brunner, N., & Scarani, V. (2004). Towards practical and fast quantum cryptography. arXiv preprint quant-ph/0411022.

[15] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. “The security of practical quantum key distribution,” *Reviews of modern physics*, *81*(3), 1301, 2009.

[16] González-Payo, J., Trényi, R., Wang, W., and Curty, M. “Upper security bounds for coherent-one-way quantum key distribution,” *Physical Review Letters,* 125(26), 260510, 2020.

[17] Trényi, R., & Curty, M. “Zero-error attack against coherent-one-way quantum key distribution,” *New Journal of Physics,* 23(9), 093005, 2021.

List of abbreviations and definitions

COW	Coherent one-way protocol
COW3	Coherent one-way protocol with 3 states
COW4	Coherent one-way protocol with 4 states
AES	Advanced Encryption Standard
BER	Bit error ratio
COW	Coherent one-way protocol
COW3	Coherent one-way protocol with 3 states
COW4	Coherent one-way protocol with 4 states
dcc	Dark-count corrected
DSA	Digital Signature Algorithm
KEMS	Key Entity Management System
QBER	Quantum bit error ratio
QKC	Quantum key controller
QKD	Quantum key distribution
RSA	Cryptosystem named after authors, Ron Rivest, Adi Shamir, and Leonard Adelman
SDN	Software-defined network
SDO	Standard developing organisations
SHA	Secure Hash Algorithm

List of figures

List of tables

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct centres. You can find the address of the centre nearest you online (european-union.europa.eu/contact-eu/meet-us_en).

On the phone or in writing

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

— by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

— at the following standard number: +32 22999696,

— via the following form: european-union.europa.eu/contact-eu/write-us_en.

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website (european-union.europa.eu).

EU publications

You can view or order EU publications at op.europa.eu/en/publications. Multiple copies of free publications can be obtained by contacting Europe Direct or your local documentation centre (european-union.europa.eu/contact-eu/meet-us_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex (eur-lex.europa.eu).

Open data from the EU

The portal data.europa.eu provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.

Science for policy

The Joint Research Centre (JRC) provides independent, evidence-based knowledge and science, supporting EU policies to positively impact society

EU Science Hub
joint-research-centre.ec.europa.eu

@EU_ScienceHub

EU Science Hub - Joint Research Centre

EU Science, Research and Innovation

EU Science Hub

@eu_science

Publications Office
of the European Union