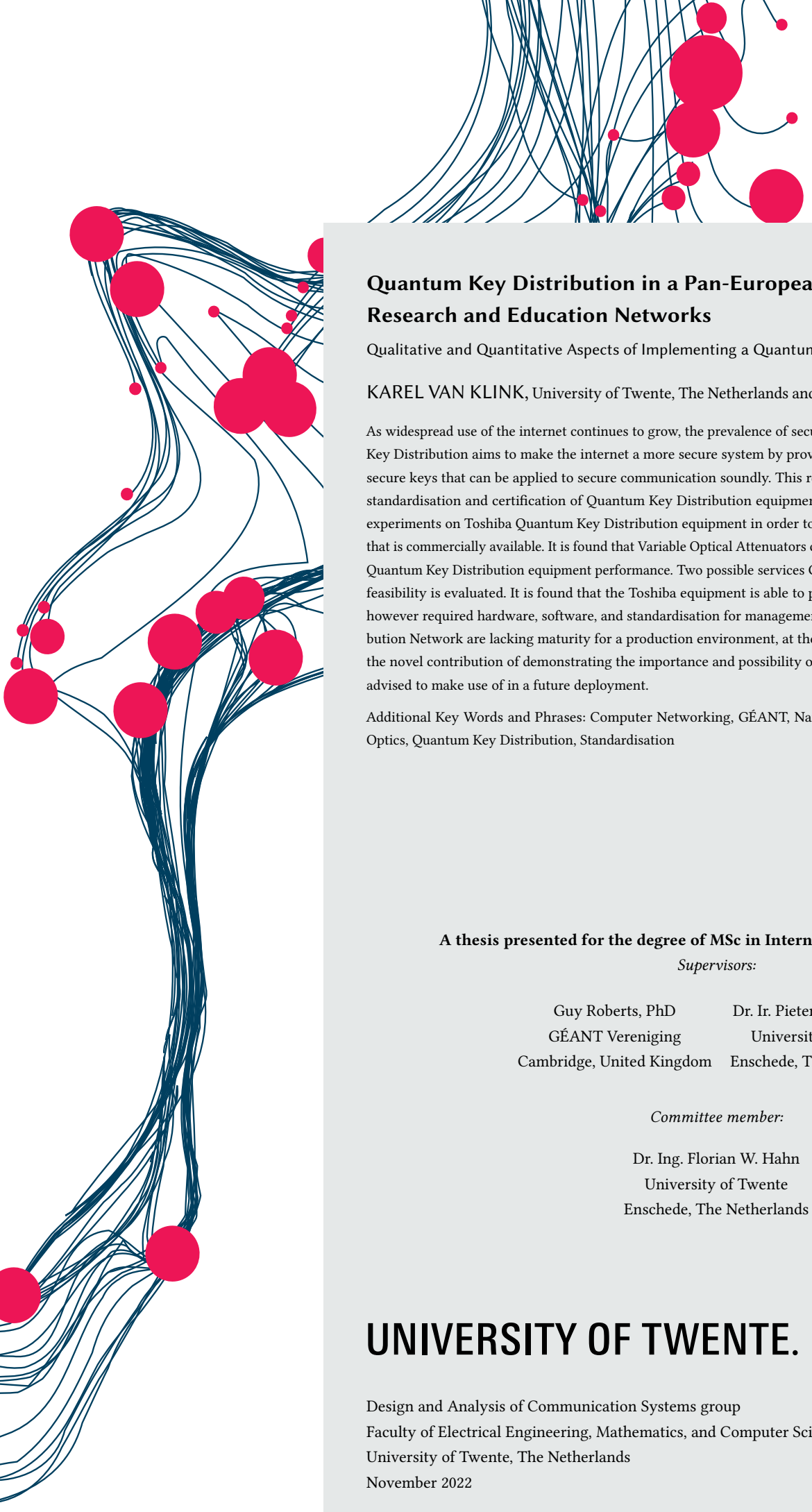


Quantum Key Distribution in a Pan-European Network of National Research and Education Networks

Qualitative and Quantitative Aspects of Implementing a Quantum Key Distribution Network

KAREL VAN KLINK, University of Twente, The Netherlands and GÉANT Vereniging, The Netherlands

As widespread use of the internet continues to grow, the prevalence of security threats it faces follows suit. Quantum Key Distribution aims to make the internet a more secure system by providing the possibility to generate perfectly secure keys that can be applied to secure communication soundly. This research investigates the state of the art in standardisation and certification of Quantum Key Distribution equipment, which goes hand in hand with a set of experiments on Toshiba Quantum Key Distribution equipment in order to investigate the performance of hardware that is commercially available. It is found that Variable Optical Attenuators cannot replicate dark fibre when measuring Quantum Key Distribution equipment performance. Two possible services GÉANT could offer are presented, and their feasibility is evaluated. It is found that the Toshiba equipment is able to perform adequately in a test environment, however required hardware, software, and standardisation for management and operation of a Quantum Key Distribution Network are lacking maturity for a production environment, at the moment of writing. This research makes the novel contribution of demonstrating the importance and possibility of multiplexing, something that is strongly advised to make use of in a future deployment.

Additional Key Words and Phrases: Computer Networking, GÉANT, National Research and Education Networks, Optics, Quantum Key Distribution, Standardisation

A thesis presented for the degree of MSc in Internet Science & Technology

Supervisors:

Guy Roberts, PhD
GÉANT Vereniging
Cambridge, United Kingdom

Dr. Ir. Pieter-Tjerk de Boer
University of Twente
Enschede, The Netherlands

Committee member:

Dr. Ing. Florian W. Hahn
University of Twente
Enschede, The Netherlands

UNIVERSITY OF TWENTE.

Design and Analysis of Communication Systems group
Faculty of Electrical Engineering, Mathematics, and Computer Science
University of Twente, The Netherlands
November 2022

ACRONYMS

AES Advanced Encryption Standard
ALS Automatic Laser Shutdown
API Application Programming Interface
ATCA Advanced Telecommunications Computing Architecture
AUX auxiliary
B92 Bennett 1992
BB84 Bennett-Brassard 1984
BBM92 Bennett-Brassard-Mermin 1992
C-band Conventional band (1530 nm to 1565 nm)
CI Confidence Interval
COW Coherent One-Way
CV-QKD Continuous Variable-QKD
DoS Denial of Service
DPS Differential Phase Shift
DV-QKD Discrete Variable-QKD
DWDM Dense Wavelength Division Multiplexing
ETSI European Telecommunications Standards Institute
EuroHPC European High Performance Computing
EuroQCI European Quantum Communication Infrastructure
FCAPS Fault, Configuration, Accounting, Performance, Security
GS Group Specification
HTTPS HTTP Secure
HUP Heisenberg Uncertainty Principle
IAM In-line Amplifier Module
IEC International Electrotechnical Commission
IEEE Institute of Electrical and Electronics Engineers
IRM In-line Raman Module
IRU Indefeasible right of use
ISG Industry Specification Group
ISO International Organisation for Standardisation
ITU International Telecommunication Union
ITU-T ITU Telecommunication Standardization Sector
JTC Joint Technical Committee
KM Key Manager
KMA Key Management Agent
KSA Key Supply Agent
MAN Metropolitan Area Network
MDI-QKD Measurement Device Independent QKD
MIB Management Information Base
MZ Mach-Zehnder
NGN Next-Generation Networking
NREN National Research and Education Network
O-band Original band (1260 nm to 1360 nm)
OC Operations Centre
OLS Optical Line System
OSC Optical Supervisory Channel
OSI Open Systems Interconnection
OTP One-Time Pad
PNS Photon Number Splitting
PoP Point of Presence
PQC Post-Quantum Cryptography
QBER Quantum Bit Error Rate
QCI Quantum Communication Infrastructure
QKD Quantum Key Distribution
QKDaaS QKD as a Service
QKDN Quantum Key Distribution Network
QoS Quality of Service
REST REpresentational State Transfer
ROADM Re-configurable Optical Add-Drop Multiplexer
RSA Rivest-Shamir-Adleman
SAE Secure Application Entity
SAML Security Assertion Markup Language
SARG04 Scarani-Acín-Ribordy-Gisin 2004
SD-QKD Software Defined QKD
SDN Software Defined Networking
SECOQC SEcure COmmunication based on Quantum Crytography
SG Study Group
SKR Secret Key Rate
SNDL Store Now Decrypt Later
SNMP Simple Network Management Protocol
SPDC Spontaneous Parametric Down-Conversion
TF-QKD Twin-Field QKD
TRL Technology Readiness Level
VM Virtual Machine
VOA Variable Optical Attenuator
VPN Virtual Private Network
WP Work Package

Contents

1 INTRODUCTION

1.1 Quantum Key Distribution

With recent developments in quantum computing threatening the security of the techniques that are currently used to transport data across the internet, a novel approach to securing the internet is paramount to its safety. Shor's algorithm has already been shown to be able to break cryptography methods based on integer factorisation [104]. These methods include the Rivest-Shamir-Adleman (RSA) suite, and both the finite field and elliptic curve Diffie-Hellman key exchange schemes [98]. Even with currently available quantum computing power being insufficient to perform these operations, the need for transitioning to Post-Quantum Cryptography (PQC) is already a concern for the present, with Store Now Decrypt Later (SNDL) attacks already possible by capturing large quantities of traffic [74].

With symmetric-key encryption provably secure against quantum computing attacks, this leaves the issue of key exchange itself. Quantum Key Distribution (QKD) is presented as a solution to this problem, that is proven to be unconditionally secure, if implemented properly [102]. Single photons with information contained within the quantum states that are exchanged, are used to distil key information resulting in unconditionally secure keys. Thanks to the no-cloning theorem, an eavesdropper can be detected through the application of theoretical limits on the used protocol [117]. An extended explanation of the operation of QKD and some of the used protocols is given in Section 2.5.

1.2 Services in GÉANT

GÉANT is an organisation based in Amsterdam and Cambridge that connects National Research and Education Networks (NRENs) throughout Europe and beyond. The services they offer do not only consist of connecting the NRENs themselves, but also includes offering additional value-added services on top of the network. Among these services there are eduroam, eduVPN, eduTEAMS, and other services in Trust & Identity, Network & Connectivity, Cloud, and Security [40]. This research will concern itself with the latter: security of the network.

In its current form, the GÉANT network is largely based on long-term Indefeasible right of use (IRU) agreements which ensure that GÉANT is in control of the optical fibre and equipment that is being used at transmission stations. The optical line systems currently in use are Infinera FlexILS Optical Line Systems (OLSes), which allow for disaggregation of both switching and multiplexing optical components in Points of Presence (PoPs). This allows GÉANT to both offer spectrum services to customers, and to easily replace transponders in the network as these are separate of the OLS. These transponders also include the possibility of using hardware-based encryption, if provided with symmetric keys.

Currently, GÉANT deploys no encryption through the OLSes on layers 1 and 2, nor on the routers on layer 3. Customers are expected to secure their own traffic at the source, and as such are reliant on asymmetric public key algorithms that are not quantum-safe. Because of this, GÉANT wants to investigate the possibility of applying QKD to the optical network.

1.3 QKD in GÉANT

GÉANT is investigating the use of Toshiba equipment to implement QKD, hence the practical aspects of the research will be specifically centred around Toshiba QKD hardware. The choice for Toshiba equipment was made, as they offer a highly mature off-the-shelf QKD solution, and their QKD research facilities are based within Cambridge, allowing for efficient collaboration and support. The goal of the experimental phase will be to investigate the performance of the equipment, when working in tandem with existing optical transmission hardware that is used in PoPs throughout the network at GÉANT.

The way that the GÉANT network is set up, all links pass through a series of optical amplifier stations before they reach their destination. These amplifier stations are situated around 75 km apart, and would ideally coincide with the hops a QKD link would take. The corresponding level of attenuation for these distances is taken into consideration when testing the equipment.

Two possible approaches exist for the integration of QKD in the network. The first is a security option that makes use of the encryption functionality of the transponders used in the network. These allow for hardware-based encryption on the Ethernet layer of all traffic passing through.

The second option that is to be investigated is the possibility of QKD as a Service (QKDaaS). The goal of such a system would be to provide any customers that make use of the GÉANT network to encrypt their traffic by using quantum keys that are generated by a Quantum Key Distribution Network (QKDN) service provided by GÉANT. This would allow for a higher degree of flexibility on the side of the customers of the network, as it will enable them to use quantum keys for any purpose they see fit.

1.4 Research Questions

Research questions that are to be answered in this research are as follows:

(1) What types of QKD solutions or services should GÉANT build?
   (a) What would be required to build a system where QKD is used to secure all internet traffic in a network using IEEE 802.1AE (MACsec) or IPSec?
   (b) What would be required to build a system where key distribution is offered as a service to other customers such as peering networks?
(2) How could GÉANT implement these services in their network?
(3) Which hardware and software solutions are required in order to maintain and monitor a QKD secured network, and which commercial components are currently ready for deployment in a carrier grade network?

(4) What is the expected Secret Key Rate of a QKD link in the GÉANT network?
   (a) When modelling the performance of the network, can a Variable Optical Attenuator (VOA) be used as a realistic substitute to approximate dark fibre?

Research Question 1, together with Research Question 1a and Research Question 1b seek to identify not only what these services could look like, but also the requirements and use cases GÉANT might have for these solutions.

Research Question 2 will focus on the practical aspect of implementing these solutions in the GÉANT network. This includes an investigation of the existing technology, commercially available equipment, its performance, and the current standardisation landscape.

Research Question 3 will be investigated following the approach presented in Section 3.1. In this section, a literature study is outlined where the Technology Readiness Level (TRL) of QKD hardware and software are evaluated.

Research Question 4 will be expanded upon in Section 3.2, where more in-depth questions to be answered are presented. This Research Question serves as an extension of the first two, where the expected performance of a solution is evaluated.

1.5 Outline

In the research carried out, work is initially performed to become acquainted with the existing GÉANT network, and the testing of QKD equipment that has already taken place within the organisation. Subsequently, background research is performed on the state of the art in implementing a QKDN, standardisation efforts by various institutions, and the QKD equipment that is currently commercially available. In parallel, a quantitative study is carried out to understand the performance of QKD equipment from Toshiba.

Section 2 provides a background on different approaches to QKD, their respective protocols, and the existing commercially available equipment and services for providing QKD. Different equipment vendors and their available products are compared, and an overview is given on the protocols that these products make use of. The section closes off with an overview of recent commercial deployments. Next, Section 3 provides an overview of the approach that is taken in this research, for both the literature study that is performed, and the quantitative analysis of the equipment from Toshiba. Section 4 follows with the literature study itself, where standardisation organisations are presented, with each their respective working groups that concern themselves with work related to QKD. Available standards are presented and examined on their differences, shortcomings, and future work. Then, Section 5 presents the methodology of the quantitative study that is performed on the equipment from Toshiba. Test runs are described, and the approach to evaluation of the results is given. The results from these tests are given in Section 6, where they are subsequently evaluated using statistical analysis. From these results, and from the earlier literature study, implementation of QKD and a QKDN in the GÉANT network is presented in Section 7. In Section 8 conclusions are drawn for the research questions presented in this section. The research closes off with a discussion in Section 9, where future work is also elaborated upon.

2 BACKGROUND

This section starts off with a discussion of GÉANT's requirements of a QKD system. These requirements are presented first, as it allows the research to be focused on the most relevant implementations of QKD technology. Next, an overview of commercially available QKD systems is given for a range of vendors. An overview of commonly used QKD protocols follows, after which practical implementations are discussed. The products mentioned in this section operate on different optical wavelengths. The frequency bands these products focus on are the Original band (O-band) and the Conventional band (C-band) [1].

2.1 GÉANT's Requirements

As an organisation that interconnects all of Europe's NRENs, there are various projects and stakeholders that are to be taken into account. Projects such as European Quantum Communication Infrastructure (EuroQCI) [38] and European High Performance Computing (EuroHPC) [37] play a key role in setting the objectives for quantum technology in the academic sphere in Europe. NRENs themselves, together with both academia and industry partners, have also taken matters into their own hands, and are actively researching the application of QKD in Europe in different projects. There exist consortia such as OpenQKD [89], Quapital [96], and CiViQ [18], and funding opportunities from the European Union [23, 24]. Numerous European NRENs are currently involved in building national Quantum Communication Infrastructure (QCI) networks, and it is likely that GÉANT will have a role in management and/or coordination of a European wide key distribution service.

Work on QKD in GÉANT started in Work Package (WP) 6 as a part of the GN4-3 project (GN4-3-WP6), and the team have performed a study in which it was found that NRENs are becoming more interested in implementing QKD [4]. Use cases from NRENs include government, military, and academic applications. A use case for GÉANT is supporting the NRENs in their efforts to implement QKD infrastructure. Supporting this infrastructure could include both supplying physical infrastructure where traffic between PoPs is quantum secured, or offering QKD as a service to the wider GÉANT community consisting of NRENs and other partners.

When implementing a QKD solution, cost is an important factor to take into account to ensure a solution that will suit the needs of the research community. When deploying a solution, one important feature for a vendor of QKD equipment is the possibility of multiplexing both quantum and data traffic on the same fibre link. This feature is needed as leasing a dedicated fibre link for QKD becomes very costly, very quickly. The average cost of fibre lease in the current GÉANT network is €0.19 per metre per year. This becomes a very substantial amount, especially when considering the fact that the current GÉANT network consists of 20 000 km of fibre, and is still increasing. The experimental phase of this analysis will therefore include an investigation into the performance of equipment when coexisting with data being transmitted over the same fibre. Allowing the QKD links to be established on a shared medium will greatly reduce the cost of implementation in the network. Moreover, as the ability to multiplex data with QKD traffic is quite novel, the performance of such a solution is unknown [114]. [6] presents a review of QKD links where data and QKD traffic are multiplexed. Experiments have been performed with QKD traffic in the C-band together with data [90, 112–114], and with QKD traffic in the O-band [114]. However, performance of QKD when combined with Infinera optical transmission equipment present in the GÉANT network is unknown. The need to understand the performance of QKD on the GÉANT optical transmission equipment is the main motivation for the work carried out in this thesis.

As previously mentioned in Section 1.3, the average link length for a single hop from one amplifier station to the next, is approximately 75 km. The level of attenuation that the optical signal is subject to will depend on the wavelength that a signal is transmitted at. Typically, this level of attenuation is 0.22 dB/km at 1550 nm and 0.33 dB/km at 1310 nm. 75 km would result in a level of attenuation of 16.5 dB and 24.75 dB, respectively. These numbers are based on the fact that the majority of the fibre that is in use in the network is G.652 single-mode fibre [54]. Equipment used for the purpose of QKD should therefore be able to withstand such levels of attenuation when operating.

For the SKR of a QKD link, the minimal rate required will largely depend on the expected consumption of keys. For the functioning of the system however, virtually any non-zero SKR is sufficient for operation. This is because of the fact that a QKD link will still produce key material when the key rate is relatively low. There is a lower limit to this however, as a low SKR will prevent proper operation of a QKDN. The required SKR for QKDaaS depends on the number of supported customers, where keys can also be buffered for future use. A higher SKR will allow for a higher rate of key consumption, which is advantageous.

2.2 Commercially Available QKD Systems

Currently, several systems are commercially available for performing QKD [21]. A brief comparison is made of all commercially available QKD hardware and services. First, QKD hardware from Toshiba, IDQuantique, Quintessence Labs, and QNu Labs are considered. QKD services are mentioned to help paint a clearer picture of the current state of the art, and are presented in Section 2.3.

Toshiba QKD Equipment. Toshiba offer two devices for QKD: a Multiplexed System and a Long Distance System [111]. An overview of their features is given in Table 1. The multiplexed system operates on a quantum channel in the O-band, which allows for multiplexing the traffic together with existing traffic on the C-band. The long distance system operates in the C-band and can not be multiplexed with traffic on the same fibre.

[1] The O-band is centred around 1310 nm, and the C-band is centred around 1550 nm

	Multiplexed System	Long Distance System
Advertised SKR	40 kbps at 10 dB loss	300 kbps at 10 dB loss
Maximum range	70 km of single-mode fibre	120 km of single-mode fibre
Fibres needed	one	two
Multiplexing	QKD on O-band with data on C-band possible	N/A
Used wavelength for QKD	1310 nm (O-band)	1550 nm (C-band)
Used protocol	T12 [82] (BB84 with decoy states and phase encoding)	
Security parameter	$\epsilon_{QKD} < 10^{-10}$	
Physical dimensions	3 U 19″ rack mounted	

Table 1. Overview of Toshiba equipment specifications [111]

IDQuantique QKD Equipment. IDQuantique offer nine "quantum-safe security products" [42]. Five devices for QKD, and four more that provide network encryption. This overview will only concern itself with the QKD equipment listed on the website. An overview of the QKD equipment is given in Tables 2 and 3. Table 2 contains information about the Cerberis product series, and Table 3 about the Clavis product line.

The Cerberis product line consists of three products. The Cerberis XG, XGR, and Cerberis^3. The XG model is geared towards telecommunication production environments, where it is used in combination with IDQuantique encryptors. The XGR model is advertised as a research platform for QKD, and is more suitable for research uses such as access to key data before post-processing. Cerberis^3 is similar to the XG, in the sense that it seeks to provide a complete package to a telecommunications company. The difference between the two products is that the former is placed in an Advanced Telecommunications Computing Architecture (ATCA) chassis [92], which allows for integration with other ATCA encryption equipment.

The Clavis product line consists of two products that are relevant to this research: the Clavis^3 and the Clavis^{300} QKD platforms. Whereas the Clavis^3 is aimed at research purposes and total control over system parameters, the Clavis^{300} is marketed as a solution to telecommunication companies that seek to quantum encrypt their existing traffic. The Clavis^3 model is placed onto a 19″ rack plate, and the Clavis^{300} model consists of an ATCA chassis that allows for installation of hardware encryptors in the very same chassis.

Quintessence Labs QKD Equipment. Quintessence Labs offer one QKD system: qOptica. Its properties are listed in Table 4. The system operates in the C-band and requires a dark fibre for QKD transmission.

QNu Labs QKD Equipment. QNu Labs offer different kinds of equipment based on quantum mechanical principles. Their Armos equipment offers QKD. An overview of its properties is given in Table 5.

2.3 Commercially Available QKD Services

In this subsection, two commercially available QKD services are reviewed: PhioTX and MagiQ.

PhioTX by QuantumXchange. QuantumXchange offer multiple subscriptions for QKD services: Trusted Xchange (TX), TX-C for Cloud, and TX-D for small office [95]. The TX subscription offers "out-of-band key delivery technology" that provides the end user with quantum cryptographic keys to use in their own equipment. The cloud variant of the subscription, TX-C, consists of an arbitrary amount of PhioTX nodes that deliver quantum cryptographic keys upon request. Keys are distributed across the network and fetched at two nodes wanting to exchange keys by making use of the European Telecommunications Standards Institute (ETSI) Group Specification (GS) QKD 014 key delivery API [33]. Next to this, they also offer TX-D for small business that provides Virtual Private Network (VPN) connections with quantum cryptographic keys. These keys are delivered in a similar fashion to the TX-C plan.

A comparison between PhioTX, MagiQ's QPN, and a self-hosted QKD system is presented in Table 6

MagiQ QPN. MagiQ offer one subscription product: QPN [84]. An overview of its features is presented in Table 6. QPN aims to provide a one-size-fits-all type of solution, where two QKD devices need to be installed at the two PoPs of a user, between which all traffic is encrypted using Ethernet encryptors.

2.4 Comparison of QKD Hardware

Give the situation described in Section 1.3 and the requirements listed in Section 2.1, it becomes apparent that a system capable of multiplexing both quantum and data signals onto a shared fibre is paramount to the cost-effective application of QKD in the GÉANT network.

Of the nine systems described in Section 2.2, six are able to operate on a QKD that is multiplexed together with data waves on a single fibre pair. These are the multiplexed system by Toshiba and the equipment manufactured by IDQuantique. Both the Toshiba multiplexed system and the IDQuantique Cerberis XG systems support multiplexing, are available in a 19″ rack mounted chassis, and are marketed as commercially available products that could be applied in a production environment.

A comparison between the experimental performance of the Toshiba equipment, and the advertised performance of the IDQuantique equipment will be made in Section 7.

	Cerberis XG QKD System	Cerberis XGR QKD Platform	Cerberis^3 QKD System
Advertised SKR	2 kbps at 12 dB loss		1.4 kbps at 12 dB loss
Maximum transmission loss	12 dB “standard”, 18 dB “premium”		
Fibres needed	one or two		
Multiplexing	QKD on O-band with data on C-band possible		
Used protocol	COW protocol [75]		
Security parameter	$\epsilon_{QKD} = 4 \cdot 10^{-9}$		
Physical dimensions	1 U 19″ rack mounted		6 U 19″ ATCA chassis

Table 2. Overview of IDQuantique Cerberis equipment specifications [42]

	Clavis^3 QKD Platform	Clavis^{300} Quantum Cryptography Platform
Advertised SKR	1.4 kbps at 12 dB loss	6 kbps at 12 dB loss
Maximum transmission loss	12 dB “standard”, 18 dB “premium”	18 dB “standard”, 24 dB “premium”
Fibres needed	one or two	
Multiplexing	WDM possible	
Used protocol	COW protocol [75]	
Security parameter	-	QBER <3 % at 10 dB loss
Physical dimensions	144 mm high (4 U 19″ rack equivalent)	6 U 19″ ATCA chassis

Table 3. Overview of IDQuantique Clavis equipment specifications [42]

	Quintessence Labs qOptica
Advertised SKR	1.9 kbps at 10 dB loss
Maximum transmission loss	10 dB
Fibres needed	two
Multiplexing	not possible
Used protocol	“coherent state CV-QKD”
Security parameter	QBER not listed
Physical dimensions	4 U 19″ rack mounted

Table 4. Overview of qOptica equipment specifications [97]

	QNu Labs Armos
Advertised SKR	*Unknown*
Fibres needed	two
Multiplexing	possible
Used protocol	DPS
Physical dimensions	2 U 19″ rack mounted

Table 5. Overview of QNu Labs’ Armos equipment specifications [94]

2.5 QKD Protocol Comparison

In general, QKD protocols can be divided into two categories: prepare and measure, and entanglement-based protocols. All QKD protocols are based on the Heisenberg Uncertainty Principle (HUP), which states that of a pair of conjugate properties, there exists an inverse relation between the accuracies of the known values of these properties. QKD generally makes use of the HUP through photon polarisation, where information is encoded in the polarisation of photons on multiple bases. Combined with the no-cloning theorem, which prevents arbitrary quantum states from being copied, it becomes impossible to circumvent the HUP [41].

In prepare and measure protocols, the system makes use of the fact that the properties of a particle will change after a measurement has taken place. This will allow for the detection of eavesdroppers, since the outcome of a measurement will change once it has already been observed. In entanglement-based protocols, two photons are linked such that they become entangled. When entangled, measurements performed on the one photon, will predict the outcome of a measurement on the entangled photon.

Comparisons of several QKD protocols have been presented in [25, 41, 88]. These survey papers generally discuss the different aspects of the Bennett-Brassard 1984 (BB84) protocol [12]. This protocol and multiple variants that followed that are beyond the scope of this research, as these are not implemented by the equipment mentioned in Section 2.2. Next to this, they also discuss the Coherent One-Way (COW) protocol [75], which is used in the IDQuantique equipment, also shown in Section 2.2. The Toshiba equipment makes use of the T12 protocol [82]. Finally, QNu Labs’ equipment makes use of the Differential Phase Shift (DPS) protocol [103], which is based on the Bennett 1992 (B92) protocol [25]. These protocols are explained further in the following subsections.

All of the aforementioned protocols are part of the family of Discrete Variable-QKD (DV-QKD). Here, the equipment makes use of a single-photon detector to register events. An alternative to this approach is Continuous Variable-QKD (CV-QKD). In this case, a continuous beam of photons is sent by the transmission equipment, and quantum information is encoded in properties such as phase modulation or amplitude.

A short introduction of the protocols used by the aforementioned equipment will be given: BB84, T12, DPS, and COW. All of these protocols are of the prepare and measure family of QKD protocols.

2.5.1 BB84 Protocol. The BB84 protocol as presented by Bennett and Brassard in [12] lays the groundwork for QKD as we know it today. `Alice` sends a random string of bits encoded into polarised photons to `Bob`. Encoding is performed through polarising photons in two different bases, and attaching either a `0` or `1` value to these states. A photon

	Self-hosted solution	QuantumXchange PhioTX	MagiQ QPN
Advertised SKR	varies	unknown	unknown
Security certification	varies	FIPS 140-2	none
OSI layer presence	Layer 2 and upwards possible	Layer 2	Layer 2
Used protocol	varies	unknown	BB84
Key delivery mechanism	ETSI QKD 004 or 014 [33, 34]	ETSI QKD 014	N/A
Initial investment	high	moderate	high
Custom hardware required	full hardware stack	encryptors	full hardware stack

Table 6. Comparison of different QKD solutions

polarised on the horizontal or 45° base are designated as a binary `0`, and the vertical or 135° bases are designated as a binary `1` [8].

Bob will randomly decide on the base they will use to polarise the received photon. This is done independently from Alice, and will either result in a correct reading, when the same base is chosen, or a random, incorrect output when the opposite base is chosen. `Alice` and `Bob` then determine, through a public channel, which photons were exchanged correctly, by sharing the basis on which these photons were transmitted.

As the original basis in which the photons are each sent is unknown, a potential eavesdropper Eve would - much like `Bob` - have to guess which basis to use when polarising the photon to observe its value. Because of this, there is a risk for Eve to re-transmit a photon to `Bob` in a different basis from what was originally sent by Alice. To test for eavesdropping, `Alice` and `Bob` can therefore share some of the secret bits in a public channel. The bits they both transmit and observe in the same basis should then always be equal, in the case where no significant eavesdropping has taken place. An example of a protocol run from [8] is given in Table 7.

2.5.2 T12 Protocol. The T12 as presented by Lucamarini *et al* in [82] operates in a similar fashion to the BB84 protocol. Quantum information is encoded in both intensity of the transmitted light pulses, and "another degree of freedom". This can either be polarisation (as is the case in BB84), or the relative phase from an asymmetric inferometer [82]. In the case of polarisation, the operation differs from BB84 in only one key detail. Where in BB84 `Alice` will choose bases at random (ie. $p_{rectilinear} = p_{diagonal}$), the probabilities are shifted in the case. With T12, we have $p_{rectilinear} \neq p_{diagonal}$. This gives a majority basis and a minority basis, which the T12 protocol uses to increase effective throughput. As presented by Lucamarini *et al.*: "(…) only 11.7 % of the detected counts are discarded, as opposed to 50 % in the BB84 protocol." [82] Because of this, the theoretical efficiency of T12 is 76.6 % higher than that of BB84. This theoretical increase was also confirmed in their experiments to be 73.5 % [82].

On top of the parameter optimisation, T12 also makes use of decoy states [79]. Decoy states are used to detect eavesdropping attacks, by having `Alice` prepare additional states purely for this purpose, as opposed to using states only for key generation as is the case with BB84. Decoy states vary from standard states only by means of their intensity. For these states, we have a certain gain Q_μ, a yield Y_n of an n-photon signal. We also have the Quantum Bit Error Rate (QBER) correlating to Q_μ, E_μ, and the QBER correlating to Y_n, e_n. The decoy state method proposed in [79] make use of the fact that the yields Q_μ and Y_n and their corresponding QBERs E_μ and e_n are linearly correlated to one another. This allows `Alice` and `Bob` to correlate observed QBER and yield to observed photon count. Based on this effect, they can produce an accurate range that should contain the observed QBER and yield for any amount of received photons per burst. This method also allows for detecting an eavesdropper with a high degree of accuracy.

2.5.3 DPS Protocol. Differential Phase Shift (DPS) QKD, presents a different approach to QKD from protocols based on BB84. It consists of a setup where photon pulses intentionally interfere with each other, in order to cause a state of superposition based on phase modulation. A diagram of such a setup is presented in Figure 1. "The security of this scheme is based on the fact that coherent states of light with an average photon number less than one are non-orthogonal when they have opposite phases" [45]. Since this setup relies on only a single measurement apparatus consisting of two detectors - which is half that of the required equipment for a receiving station using BB84 - DPS boasts a lower implementation complexity [43].

DPS is based on B92, a protocol that, in turn, is based on BB84. Where BB84 makes use of four, non-orthogonal states, B92 only uses two. Two sequential pulses are sent by Alice: one phase-modulated weak pulse, and a bright reference pulse. `Bob` then measures both pulses, combines them, and when `Alice` and `Bob` have used the same modulation this measurement is used for creating key material [45]. If `Bob` has selected the other basis, nothing is measured at all [88].

The DPS protocol operates in a similar fashion to B92. `Alice` sends a pulse train that is randomly phase-modulated by $\{0, \pi\}$. `Bob` uses a delayed Mach-Zehnder (MZ) interferometer to induce a time interval τ as displayed in Figure 1. Adjacent pulses that arrive interfere with each other, resulting in either one detector clicking, depending on the phase differences. Then, `Bob` shares with `Alice` at which times either one of the detectors clicked. From this information, combined with Alice's information on modulation, she can determine which detector must have clicked on Bob's end. From this, key material is generated, by making detector one correlate with binary `0` and detector 2 with binary `1` [45].

QUANTUM TRANSMISSION															
Alice's random bits	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Random sending bases	*D*	*R*	*D*	*R*	*R*	*R*	*R*	*R*	*D*	*D*	*R*	*D*	*D*	*D*	*R*
Photons `Alice` sends	⤢	↕	⤡	↔	↕	↕	↔	↔	⤡	⤢	↕	⤡	⤢	⤢	↕
Random receiving bases	*R*	*D*	*D*	*R*	*R*	*D*	*D*	*R*	*D*	*R*	*D*	*D*	*D*	*D*	*R*
Bits as received by `Bob`	1		1		1	0	0	0		1	1	1		0	1
PUBLIC DISCUSSION															
`Bob` reports bases of received bits	R		D		R	D	D	R		R	D	D		D	R
`Alice` says which bases were correct			OK		OK			OK				OK		OK	OK
Presumably shared information (if no eavesdrop)			1		1			0				1		0	1
`Bob` reveals some key bits at random					1									0	
`Alice` confirms them					OK									OK	
OUTCOME															
Remaining shared secret bits			1					0				1			1

Table 7. Example BB84 protocol run, originally from [8]. *D* and *R* denote diagonal and rectilinear bases, respectively.

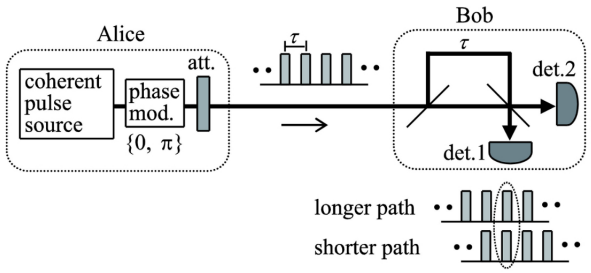


Fig. 1. DPS-QKD configuration from [43]. att: optical attenuator, τ: time interval of pulses.

One major advantage of DPS over standard BB84, is the fact that DPS is resilient against Photon Number Splitting (PNS) attacks without having to make use of decoy states. A proof of this property is presented in [44].

The equipment of QNu Labs described in Section 2.2 makes use of an adapted version of DPS, where the protocol relies in time-bin entanglement within a single pulse [103]. Time-bin qubits are formed by passing a short pulse of photons through an MZ interferometer. Depending on which arms of the interferometers each photon passes through, they will be in different time-bins. Creation of entangled time-bin qubits will occur when they are passed through a non-linear crystal and have Spontaneous Parametric Down-Conversion (SPDC) take place [85]. SPDC is a process that takes place when a photon with relatively high energy passes through a non-linear crystal. The photon may be split into a pair of photons, which are entangled [81]. This conversion rate is relatively low, at an efficiency of 4×10^{-6} [11].

2.5.4 COW Protocol. The COW protocol, is introduced by researchers at IDQuantique to use in their QKD equipment [107]. With the COW protocol, information is not stored in polarisation as with BB84 and its derivatives, but in time. Weak pulses are generated in specific time bins, which represent different bit values. `Alice` starts by encoding data in these timeslots into pairs of pulses. In case of a `1`, the first pulse will be attenuated, and the second one will not. For a `0`, the attenuation of the two pulses is the opposite. Some empty space is then left between the encoded pulses for the decoy pulses. The rate of decoy states can be controlled, in order to adjust to the required percentage of decoy pulses. For a decoy state, both transmitted pulses are not attenuated. The signal received by `Bob` is shifted by the time difference between two pulses. This will eliminate the decoy pulses, and allow `Bob` to extract the encoded bits from Alice's data transmission [75]. Similar to BB84, a public phase follows where some bits are revealed in a public channel and the final sifted key is created.

2.6 Quantum Bit Error Rate

When measuring the performance of a QKD link, there are two main factors that are taken into account: the SKR and the Quantum Bit Error Rate (QBER). The QBER serves as a means of efficiency to indicate the performance of an algorithm, and the equipment used. In the case of the BB84 protocol, the QBER is calculated as the ratio of received bits where `Bob` had selected the correct base to perform its measurement in. This is displayed in Table 7, where the QBER can be read as the ratio of bits that are not marked as OK in the row "Alice says which bases were correct".

Next to indicating efficiency, QBER is also used for the detection of eavesdropping in QKD protocols. For example, in BB84 the transmission bases are chosen at random. If an eavesdropper (Eve) tries to intercept states, there is a 50 % chance they will pick the correct base for intercepting the photon that `Alice` intended to send to Bob. In this case, Eve is able to successfully replicate the state of the photon and forward it to Bob. However, when Eve picks the opposite base from Alice, Eve is unable to forward a state to `Bob` where they can predict the outcome of a correct measurement. On average, an intercept-resend attack will therefore result in a QBER of 25 % [93].

2.7 Recent Commercial Deployments

Multiple QKD secured networks have already been tested in practical environments. A one-way QKD system has been demonstrated in [118],

where it was shown that "actively compensated QKD systems are suitable for practical applications". Chapuran *et al.* demonstrate QKD in the O-band multiplexed with data channels in the C-band [14]. Practical solutions to QKD have been shown to be effective in a number of places, including: a six-node network in Vienna, Austria [91], a five-node network with a trusted relay node in Heifei, China [17], a ring network consisting of three nodes in Madrid, Spain [77], a four-node star topology network in Durban, South-Africa [87], a five-node network with one central router in Wuhu, China [115], a mesh network consisting of six nodes in Tokyo, Japan [100], and a three-node ring network in Geneva, Switzerland [108]. More recently, an expansive approach was put into practice in Heifei, China, with 46 nodes in a network topology where nodes would reside in one of three sub networks [16].

In the aforementioned implementations, six made use of the BB84 protocol, most of which incorporated some form of decoy states ([118], Heifei, China [17], Madrid, Spain [77, 116], Durban, South Africa [87], Wuhu, China [115], Heifei, China [16]). On top of that, [14] made use of B92 - a protocol based on BB84 that uses only two non-orthogonal states in one system and "a full suite of protocols" in another. The network in Vienna from [91] compared performance of a multitude of protocols, including COW, T12, and a CV-QKD protocol. [100] in Tokyo, Japan made use of a combination of BB84 with decoy states, Bennett-Brassard-Mermin 1992 (BBM92) [9], and Scarani-Acín-Ribordy-Gisin 2004 (SARG04) [101]. The network in Geneva, Switzerland made use of the SARG04 protocol [108]. SARG04 is a protocol introduced to combat PNS attacks, where SARG04 differs from BB84 in the post-processing stage. BBM92 is a protocol similar to SARG04 which makes use of two non-orthogonal quantum states [105].

Twin-Field QKD. Another technique that has shown much promise in early testbeds [15, 78] is the Twin-Field QKD (TF-QKD) method [83]. At the moment of writing, TF-QKD is not yet available in any commercial systems, yet it is included for the sake of completeness since it poses a great potential for future products. It consists of a different scheme than other QKD solutions, where pairs of phase-randomised optical fields are generated by both `Alice` and Bob. These fields are then combined at a central measuring station in the middle of the link, which theoretically allow for taking repeater-less QKD beyond distances of 500 km. However, this is yet to be shown in a practical environment. There is an ongoing field trial with prototype TF-QKD equipment from Toshiba being tested by GÉANT between Frankfurt and Kehl, but no results have been published at the time of writing.

2.8 Scattering Effects in Fibre

When transmitting photons through an optical medium, this unavoidably introduces attenuation. This attenuation is caused by different phenomena, including material absorption and scattering effects [22]. Next to this absorption effect, there are multiple scattering effects that take place. One of these is the effect of Raman scattering [114]. Raman scattering is an effect where a photon can re-radiate in all directions, and in some cases, the photon loses some of its energy. As a result, the wavelength of the photon is lower. For data waves, this is a relatively small issue, as data is transmitted at a high photon rate. However, this poses a potential issue for QKD transmissions, as these rely on single-photon detection. Photons generated through the mechanism of Raman scattering of the high-intensity optical data signal can appear as noise at the QKD receiver, effectively harming performance of the QKD channel. The scale of this effect is investigated, as will be explained in Section 5.

3 APPROACH

This section is an adaptation of the work presented in the preliminary course Research Topics.

The approach to the research questions presented in Section 1 is presented as twofold. First, a literature study is performed on the applicability of the two use cases of QKD for GÉANT. Second, experiments are performed on the performance of a QKD system in a practical lab environment. This will give valuable insight into the practical aspects of implementing the QKD systems investigated in the literary study.

3.1 Literature Study

In order to get a clear view on the possibilities for QKD in the GÉANT network, a literature study is performed on the two use-cases, as presented in the next two sections. The viability of both approaches in the existing network of GÉANT is evaluated, but a practical design and implementation of such a solution is beyond the scope of this research.

Secure DWDM with QKD. The first use-case makes use of QKD in the GÉANT network to encrypt traffic at one of the following layers:

- Layer 1-2: hardware data encryption on the Dense Wavelength Division Multiplexing (DWDM) transponders according to IEEE 802.1AE
- Layer 2-3: IP/MPLS with IPSec

This use-case would consist of designing a solution that will deliver this service in the GÉANT network. Questions to be answered are (1) how to build a trusted node, and (2) how to manage key chains over multiple hops. This approach will allow for all traffic flowing through the relevant layer of the GÉANT network to be encrypted using quantum keys.

Quantum Key distribution service in GÉANT. The second use-case is one where GÉANT offers QKD as a service to their community and/or peering networks. Users can fetch and send keys from QKD equipment located in their GÉANT PoP. Subsequently, this will consist of answering the question of what would be required to implement such a system in the GÉANT network. A broad description of the architecture is to be made, and questions to be answered are:

(1) How can keys be exchanged between service providers and/or users in a secure way?
(2) What standards currently exist that are relevant to this solution?
(3) What hardware is required?
(4) What software solutions are required?

Operation and Maintenance. Beyond the literary study on what services GÉANT could provide, a recommendation is to be made on to operation and maintenance of a QKD service. This acts as an extension to the previous section, as it forms an integral part to the success of the QKD system. Questions that are to be answered include:

(1) What is required to certify a system secured by QKD meets standards?
(2) How can the GÉANT Operations Centre (OC) check that the QKD systems are operating correctly and that keys are being correctly exchanged?
(3) What alarms are available to monitor both systems, what alarm Application Programming Interfaces (APIs) are available? How would the OC respond to these alarms?
(4) Is any configuration management system needed to set up QKD exchange?

3.2 Experiments

For the experimental part, research is performed with a QKD testbed in the GÉANT Cambridge lab. The Toshiba QKD system is integrated with Infinera DWDM equipment. From this, the performance and behaviour of the Toshiba QKD system can be understood when operating in tandem with the Infinera system. The research focuses on the stability of the system when operating at the edge of the performance envelope. These experiments are performed in order to get a clear understanding of what will prove to be the challenges when implementing a QKD system in a real-life scenario.

The Toshiba QKD is set up such that it can exchange keys between two back-to-back boxes: `Alice` and `Bob`. The Infinera FlexILS equipment is set up to send data, multiplexed with the quantum channel carrying the keys. Two Virtual Machines (VMs) with sufficient bandwidth are set up to transfer data between the hosts. Software following the ETSI GS QKD 014 key delivery API is then used to transfer keys between each QKD box and their respective Virtual Machine (VM).

The Toshiba QKD equipment is configured to demonstrate successful key exchange and test the maximum key exchange rates. Data is plotted for key exchange rate against fibre attenuation. Test parameters consist of SKR, and key error rate. Then, the Toshiba QKD system is set up to transfer keys over the same fibre as Infinera's DWDM channel with data, and maximum possible key exchange rates are measured with one or more wavelengths of data present. SKR is plotted once again against fibre length and number of wavelengths present in the system. All parameters are tested again as per the previous test setup. All dataflows are demonstrated to be correctly encrypted through a qualitative analysis.

These experiments are designed to approach a realistic simulation of a production environment, including the optical equipment that it is to be used with in tandem. Questions to be answered from these experiments are the following, these relate to the question of what would be the hardware requirements of a QKD solution.

(1) What length of fibre is the equipment able to sustain, while still successfully exchanging key material?
(2) To what degree do foreign data waves have an influence on the performance of the system?

(3) How well does the equipment integrate with an existing production environment of optical equipment?

Experimental results are ultimately compared to the results presented in [99] and [90].

4 STANDARDISATION LITERATURE SURVEY

The following section presents a literature study of the standardisation work that has been performed by various bodies that govern such standards. First, an overview of these organisations is given, which is followed by their existing working groups in the fields relevant to QKD. Then, available standards are presented for various aspects of implementing, maintaining, and monitoring QKDNs. A summary is given of the work that has already been performed, and the section is closed off with an overview of future work that is to be performed by standardisation entities.

[13] and [80] give a comprehensive survey of QKD and QKDN standardisation at large. Both present a list of standardisation bodies, and their current work. This paper however seeks to build on their work by presenting an overview of standards relevant to QKDN from various organisations, including a summary of their contents.

4.1 Overview of Organisations

Different organisations exist for the standardisation of QKD and QKDN interoperability. Many countries both in- and outside of Europe have their own respective bodies for standardisation, and these are brought together under different umbrella organisations that are relevant for this research.

ETSI. The European Telecommunications Standards Institute (ETSI) is a European organisation that is concerned with standardisation efforts in the fields of "telecommunications, broadcasting, and other electronic communications networks and services" [20].

ETSI ISG on QKD. The committee within ETSI that work on documents related to QKD is the Industry Specification Group (ISG) on QKD [19]. The working group focuses only on work related directly to QKD.

ITU-T. The International Telecommunication Union (ITU) is part of the United Nations. It consists of three sectors, one of which is the ITU Telecommunication Standardization Sector (ITU-T). It releases standards in different categories, ranging from "Audiovisual and multimedia systems" to "Global information infrastructure" [46].

ITU-T SG 13. Within the ITU, one of the Study Groups (SGs) that work on recommendations related to QKDN is SG 13: "Future networks, cloud computing, and trusted network infrastructure" [47]. Work from this SG is mostly geared towards the development of Next-Generation Networkings (NGNs) and Software Defined Networkings (SDNs), from an architectural point of view. Section 4.3 will contain work from this SG, namely the Y-series recommendations on design and architecture of various aspects of QKD and QKDN.

ITU-T SG 17. A second SG from the ITU, number 17, presents recommendations that are concerned with the technical and practical aspects of QKD [48]. SG 17: "Security", have published security recommendations that are widely used such as X.509 and X.1141 - public key certificates and Security Assertion Markup Language (SAML) [52, 64]. Recommendations relevant to QKD and QKDN written by SG 17 are presented in Section 4.3, and are all in the X-series.

ISO. Founded in 1946, the International Organisation for Standardisation (ISO) gathers national standards bodies under a global umbrella that develops standardisation works in "almost all aspects of technology and manufacturing" consisting of 167 members each representing their own country [1].

ISO/IEC JTC 1 SC 27. The ISO performs work in committees, one of these is the Joint Technical Committee (JTC) 1 on Information Technology, with sub-committee 27 on Information security, cybersecurity, and privacy protection working on standardisation related to QKD [49].

4.2 ETSI Standards

ETSI have published a set of standards and recommendations regarding the practical application of QKD. At the time of writing, ETSI have 15 work items. Of these 15, 11 currently have a status as publication, 2 are in a drafting stage, and 2 have been stopped. This research will evaluate 7 out of the 11 published standards, which are relevant to the implementation and operation of a QKDN. This includes use cases, key delivery APIs, security specifications, and

ETSI GS QKD 003 contains "Components and Internal Interfaces" [30]. The document is scoped to contain preparatory work into the definition of interfaces between components of QKD, and the components a QKD consists of. As these components are widely discussed in the following documents, GS QKD 003 has been left out of scope.

ETSI GS QKD 005 describes security proofs of QKD. As these do not relate to the application of QKD directly, this standard is left outside the scope of this research [27].

ETSI GS QKD 007 is a vocabulary of terms related to QKD [31].

ETSI GS QKD 011 sets requirements for optical components in a QKD module [29]. These requirements are purely for specification of measurement procedures in a QKD implementation over optical fibre. Since this only relates to the implementation of optical components themselves, this standard is outside the scope of this research.

4.2.1 ETSI GS QKD 002. ETSI GS QKD 002 contains an overview of use cases that can benefit from implementing QKD [28]. Besides these use cases, the scope of the document also includes development of certification of QKD systems. As the importance of QKD is illustrated, it is noted that for proper functioning of a QKD system there are requirements to be met on both the hardware and software side. To ensure proper security, it should be possible to evaluate the operation of equipment based on established criteria.

The document lists categories of work that is to be performed, and refers to following ETSI documents that will address these subjects. These will be presented in the following subsections. One of the categories that is listed is "QKD; Use Cases" [28], which is contained in this

document. Application scenarios follow, where four of the layers out of the Open Systems Interconnection (OSI) model are listed: the data link layer, network layer, transport layer, and the application layer. On all four of these, an overview is given of the roles that QKD can play in securing each of these layers. From these four layers, different use cases are presented. This research will highlight two of these, as they overlap with the two use-cases presented in Research Question 1.

First, use case 2 describes an "Enterprise Metropolitan Area Network" [28]. This overlaps with the solution listed in Research Question 1a. The use case describes the encryption of all traffic between locations of a Metropolitan Area Network (MAN), however in the case of GÉANT this would span across all PoPs in the network. Encryption of all traffic traversing the network is fulfilled by having Ethernet encryption equipment use quantum keys to encrypt all traffic on the data link layer by using security schemes such as MACSec.

Second, there is use case 4: "Backbone Protection" which overlaps with the solution listed in Research Question 1b [28]. Keys are distributed through existing optical links, where a quantum channel is allocated among data channels by making use of a Re-configurable Optical Add-Drop Multiplexer (ROADM). The use case notes that quantum keys can be deployed for various goals, such as validating transmission authenticity, of encryption of some messages that are transmitted across the links. The exact application of the quantum keys is then left up to the NRENs and other involved parties that will be making use of this QKDaaS.

For both aforementioned use cases, these will serve a guiding role in the description of how to apply QKD to the GÉANT network in Section 7.

4.2.2 ETSI GS QKD 004. ETSI GS QKD 004 presents an application interface for QKD [34]. This interface resides between a Key Manager (KM) and a cryptographic application. It is noted that manufacturers can build upon this document with higher level applications as they see fit, something that is already done in ETSI GS QKD 014 [33].

The document presents various diagrams that depict a systematic overview of a QKD link, including the applications that are to consume the generated keys. Based on these diagrams, links are identified, between which the interaction of key delivery should be taking place.

An API specification in introduced, first listing all functions, and then a series of sequence diagrams that describe the functioning of the API. In these diagrams it is shown that the document not only specifies interactions between the KM and an application, but also among the applications themselves. The specification includes support for application discovery in a QKDN, a process where equipment in the QKDN will search for a QKD node that is both reachable by the other application, and meets Quality of Service (QoS) specifications.

One of the appendices of the document outlines the relationship between this API and the one described in GS 014. This will be discussed in Section 4.2.5.

4.2.3 ETSI GS QKD 008. ETSI GS QKD 008 is a document containing a "QKD Module Security Specification" [26]. It is scoped to contain the necessary requirements for a QKD module to be properly responsive to hacking attempts of a QKD module. This is noted to include physical protection of a device, which should be achieved through implementing tampering sensors and circuits, among other measures.

The contents of the document start off with functional security requirements, which are "derived from (…) high-level functional security objectives" [26]. These generally are related to proper operation of a QKD link, such as implementing a correct protocol, preventing unauthorised access, and detecting errors.

From these functional objectives, a list of module specifications is presented in order to fulfil these objectives. QKD modules are defined to be hybrid modules, in the sense that it is a module that incorporates both specialised hardware and software. It is stated that the security of a module is to be specified. Physical ports and interfaces are defined, where it is prescribed that a QKD should have a data input, output, control input, and a status output interface.

In a subsequent section roles, authentication, and services are defined. A QKD module is to support at least a user role, and that of a "Cryptographic Officer" [26]. Limits are imposed on the lower boundary of security in authentication and authorisation of these roles. Then, services are defined. It is listed to support the following functions: show status, show the module's version number, perform self-tests, perform approved security function, zeroise, bypass capability, and external software loading. Zeroisation is the practice of erasing all cryptographic information contained within a QKD module.

Security standards are listed for software, the operational environment, and the physical security of a QKD module. The requirements on physical security are of special interest in this document, as this definition had not been made before in other standardisation literature. Exhaustive requirements are listed, including restrictions on ventilation slits and tamper detection. Self-tests for the equipment are listed in a following section, where it is stated that a QKD module must be able to perform tests on proper operation, integrity of the module, and tests on the source of entropy for generating randomness. The document closes off with a set of best practices for QKD module vendors, on proper design, deployment, and operation.

The document has multiple appendices attached to it. The first appendix is a summary of documentation requirements, that serves as a checklist for proper testing on the security of a QKD module. This checklist includes checks on module specification, software, hardware, and operational requirements. The second appendix consist of a QKD module security policy, that is supposed to be included in any documentation provided by a vendor. Required clauses of such a policy are outlined, including policies for identification & access, access control, physical security, and an attack mitigation security policy. An appendix follows with recommended practices for software development, which is included for informational purposes.

4.2.4 ETSI GS QKD 012. ETSI GS QKD 012 contains a description of the resources required for the implementation of a QKD link in an optical network infrastructure [32]. Tasks that should be performed by the QKD modules at `Alice` and `Bob` are listed, and the three channels for communication are set out to consist of a quantum channel for key material, a synchronisation channel, and a distillation channel. The quantum channel is used for the transmission of quantum states, in which the key material is encoded. The synchronisation channel is used to provide clock synchronisation between `Alice` and `Bob`, phase reference compensation, and polarization drift compensation. The distillation channel is a classical channel used to send information between `Alice` and `Bob`, for purposes related to post-processing and sifting of key material.

The document presents two different QKD architectures. One implementation is based on a dedicated quantum channel, where the quantum channel and possibly the synchronisation channels are on a dedicated link. The distillation and classical channels reside on separate optical links, resulting in a system that requires at least two or three links to be available for the functioning of the system. In the second implementation, the quantum channel is multiplexed with the synchronisation and distillation channels for operation on a separate optical link. When the classical channel is also multiplexed into this link, the document speaks of a "fully multiplexed architecture" [32]. In this architecture, only two or even one optical link is required for operation, respectively.

The document closes off with a section dedicated to the parameters that are exchanged between a QKD operator and a network operator. E.g., availability of an optical channel, level of attenuation across the link, and the wavelength of the used channels.

4.2.5 ETSI GS QKD 014. ETSI GS QKD 014 describes a key delivery API that allows for external applications and equipment to make use of the generated quantum keys from a QKD link [33]. This API is implemented by any and all KMs. The entity that fetches quantum keys is referred to as a Secure Application Entity (SAE). These Secure Application Entities overlap with the applications displayed in Figure 2.

SAEs are able to fetch keys, but it is left up to these entities themselves on how they notify their counterpart on what key to fetch from their corresponding KM. The document prescribes the functioning of the API, where it is possible to fetch quantum key material, get the current status of 'their' KM, and fetch a list of all available key IDs that are known to another SAE. Expected data formats are also specified, such that SAEs are able to implement API functionality.

The document includes an appendix where a comparison is made between this API, and the one described in GS QKD 004 presented in Section 4.2.2. Where the latter is implementation agnostic, the one presented in the current document is implemented as a REST API exclusively, built on top of the HTTP Secure (HTTPS). "One can consider that the present document is an easy implementation of ETSI GS QKD 004" [33]. Where GS QKD 004 will provide more flexibility in the API calls that are possible, GS QKD 014 bears a lower implementation cost.

4.2.6 ETSI GS QKD 015. ETSI GS QKD 015 defines a control interface for SDN [35]. The scope of the document contains a definition of interfaces for integration of SDN in a QKDN, abstraction models and workflows for SDN-enabled QKD nodes, and resource discovery of QKD nodes.

The document includes a description of the capabilities of a Software Defined QKD (SD-QKD) node, and from this a series of sequence diagrams and workflows follows. These sequence diagrams include application registration to a SDN, and the creation of both a physical and a virtual QKD link between SD-QKD nodes. Both security and protocol considerations are presented, but their implementational details are left to further standardisation work.

4.2.7 ETSI GS QKD 018. ETSI GS QKD 018 describes an "Orchestration Interface for Software Defined Networkings" [36]. This work is a continuation of what is presented in GS QKD 015, and describes the requirements of an SDN orchestration controller of a QKDN. Where GS QKD 015 serves to connect SD-QKD nodes to an SD-QKD controller, GS QKD 018 provides a connection from this SD-QKD controller to an overarching SDN orchestrator, that also orchestrates the SDN controller of the corresponding optical transport network.

Parameters are described for an SDN orchestration interface, considering parameters of network topology for nodes, links, network status, inventory, service status, and service provisioning. Making use of these parameters, sequence diagrams follow that describe service requests and service provisioning. Once again, security and protocol considerations are given for interoperability of the controller with other existing SDN orchestration interfaces.

4.3 ITU-T Standards

The ITU-T provides multiple standards that deal with either QKD or QKDN. There are two series of standards where publications are made, namely X.1700-X.1729, and Y.3800-Y.3999. X.1700-X.1729 is the allocated range of recommendations for quantum communication, Y.3800-Y.3900 for QKDN.

The range of ITU-T X.1702-X.1709 is allocated for "quantum random number generator", which is beyond the scope of this research [58]. ITU-T X.1715 and ITU-T Y.3808 are concerned with integration of a QKDN with a secure storage network, as this is not integral to the operation of a QKDN, these standards are left beyond the scope of this paper [68, 72].

4.3.1 ITU-T Y.3800. Recommendation ITU-T Y.3800 "Overview on networks supporting quantum key distribution" serves as a recommendation that gives an overview on the basic functioning of QKD, and possible approaches to realising a QKDN [57]. It is a first in a series of QKDN recommendations, that are noted for future work. The scope of the recommendation is an overview of QKD technology, the network capabilities required for supporting QKD, and a basic conceptual structure for QKDNs.

First, an overview of QKD technology is given in clause 6. The basic elements of a QKD link are introduced, and an explanation is given on the difference between the quantum and classical channels. For the guaranteed information theoretical security (IT-security) property of QKD, it is noted that further assumptions are required for practical implementations of QKD modules. QKD modules are defined as what is also referred to as `Alice` and `Bob` in literature.

Second, QKDN is presented, together with how they should relate to (existing) user networks. Four options are presented for realising a QKDN:

- Optical switching or splitting
- Trusted relaying
- Measurement-assisted relaying
- Fully quantum networking

With optical switching or splitting, QKD link traffic is shared between multiple nodes, in order to form keys between different users as demand changes over time. Trusted relaying is a method where links are extended by means of introducing trusted QKD nodes along a path that is also quantum secured. Keys are forwarded along the path, allowing for long chains of QKD nodes that span large distances. Measurement-assisted relaying can be realised through two methods: Measurement Device Independent QKD (MDI-QKD), and TF-QKD. TF-QKD is explained in Section 2, and MDI-QKD works in a similar fashion, in the sense that both techniques rely on having an intermediate node along a quantum link that only consists of a single-photon source, that need not be fully secured since no actual key information is known to the intermediary node. Fully quantum networking is listed as a secure alternative to the three aforementioned methods, since the network only consists of quantum channels between nodes. This allows for entangled states to be transferred across an arbitrarily large and complex network. The possibility of using a fully quantum network however relies on the availability of technology such as quantum repeaters, which are not yet available in practice.

As measurement-assisted relaying extends the functional distance of a single QKD link, it is topologically regarded as a single link, the inner workings of which are beyond the scope of Y.3800. For this reason, the standard focuses on trusted relaying as a method of forming a QKDN.

Y.3800 presents ten design considerations for a QKDN: security, scalability, stability, efficiency, application-oriented, robustness, ability of integration, interoperability, ability of migration, and manageability. From these design considerations, a plethora of QKDN capabilities follow. These capabilities bring the ten design considerations into practice, but further standardisation is left to further recommendations and standards. Eg. "The QKDN has network control and management capabilities" [57], which logically follows from the design consideration of manageability, does not impose any restrictions on how this should be realised.

In the clause 8, conceptual structures and basic functions are presented of a QKDN. It is noted that "it is an essential assumption for the QKDN that the QKD node is a trusted node" [57]. The four-layer structure for a QKDN is introduced, as it will also appear in numerous other publications. At the top, a service layer that resides in the user network. Below this, three layers that together make up the QKDN. As a top layer, the QKDN control layer where QKDN controllers reside, which control the lower two layers: the key management layer, and the quantum layer. The key management layer provides generated keys to the end users, and manages the relay links in the network. The quantum layer consists of physical hardware that performs key exchange. The diagram from Y.3800 is also shown in Figure 2. A demarcation boundary is shown in the diagram, between the user network and the QKDN. The boundary symbolises the interaction between the two networks that run in parallel, and is also the focal point of most standardisation. This is where applications that fetch their keys, and where security and functional requirements are specified. This interface between the two networks should be very clearly standardised, as this is the border where two different worlds of vendors converge.

Clause 8 further continues in describing the different layers in a QKDN, and the basic functions such as key management, QKDN control, and QKDN management. The recommendation closes of with a short clause on security considerations, where it is noted that specifics are beyond the scope of the recommendation.

4.3.2 ITU-T Y.3801. The ITU-T has published supplementary recommendations that build upon Y.3800 for fleshing out the various aspects of QKDN that are introduced there.

ITU-T recommendation Y.3801 focuses on "Functional requirements for quantum key distribution networks" [59]. Specifically, it stipulates the functional requirements of: the quantum layer, the key management layer, the QKDN control layer, and QKDN management layer. These requirements are supplemented with recommendations on what support these four actors in a QKDN should support to aid interoperability. Security considerations are shared, but are left outside the scope of this recommendation.

4.3.3 ITU-T Y.3802. ITU-T recommendation Y.3802 introduces a "functional architecture" of QKDN [65]. Functional elements and architectural configurations of QKDN are presented. The scope of the recommendation includes the following aspects.

- "Functional architecture model;
- Functional elements and reference points;
- Architectural configurations;
- Basic operational procedures." [65]

First, the functional architectural model is presented in Figure 1 in [65]. This is a more in-depth version of the one presented in Y.3800, shown in Figure 2. The presented diagram prescribes functional elements of QKDN. The recommendation then continues to give functional elements of QKDN, divided per layer in the network. Second, reference points are given that allow for referring to specific parts of a QKDN.

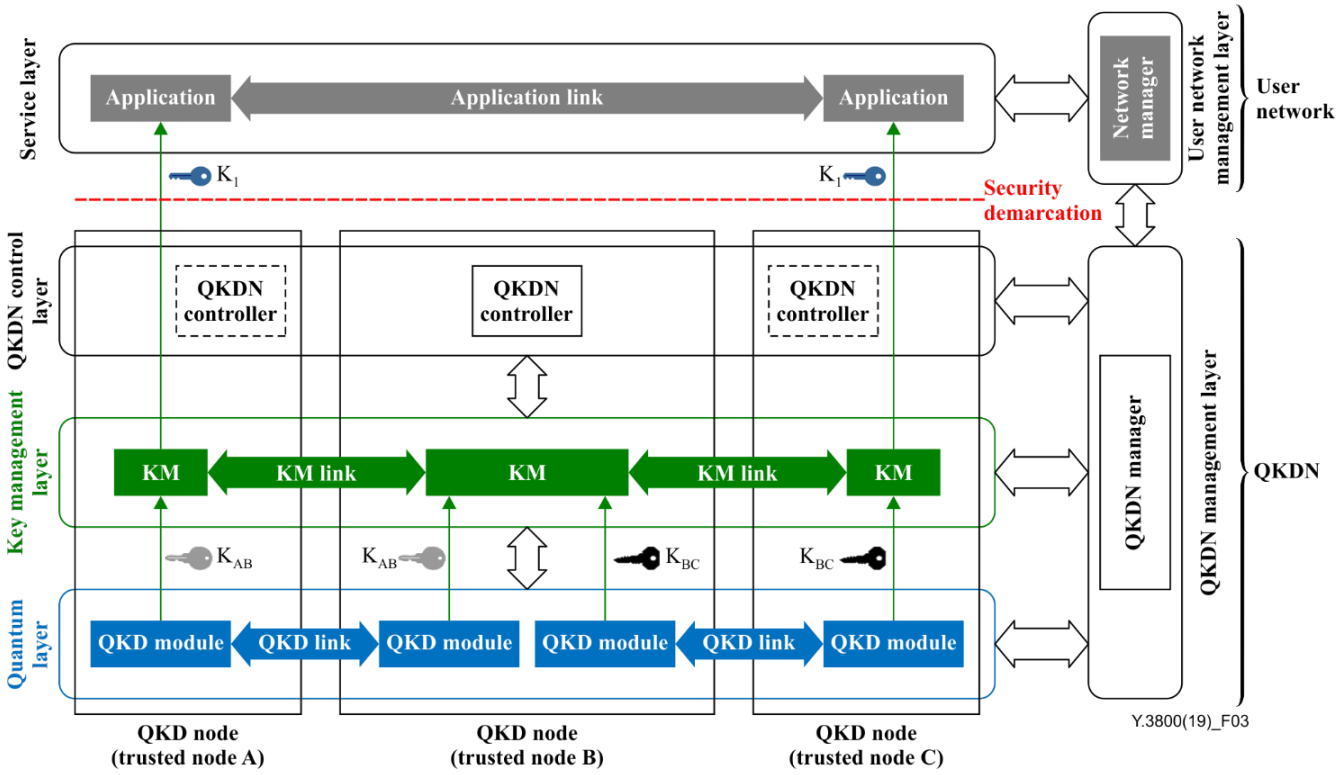


Fig. 2. QKDN diagram from [57] that shows the structures of a QKDN and a user network. Note the security demarcation between the two.

One of particular interest is Ak, which is the reference point connecting applications to the key supply function of a Key Supply Agent (KSA). The KSA is part of the KM, and is the party any application would interact with when fetching keys from QKDN. Ak is the connection that crosses the security demarcation line shown in Figure 2.

Multiple architectural possibilities for QKDN are presented: distributed QKDN, centralised QKDN, centralised QKDN with hierarchical QKD nodes, and centralised QKDN with centralised key relay. In distributed QKDN, each node is wholly self-reliant, and can freely interact with any other QKD node that is also self-reliant. Centralised QKDN stands opposite of this approach, where all nodes rely on one single QKDN controller. Relating this to the ten design considerations of QKDN mentioned in Y.3800, the centralised approach is more efficient and manageable, yet less scalable and has a lower ability of migration. The third configuration - centralised QKDN with hierarchical QKD nodes - introduces three kinds of QKD nodes that seek to address the lower degree of scalability: QKDN user nodes, QKDN access nodes, and QKDN relay nodes. A QKDN user node only provides the functionality necessary for a user to fetch and use keys. A QKDN access node and QKDN relay node both serve the purpose of key relay between apps that utilise quantum keys. Their difference lies in their topological location in a network. Both access and relay nodes are part of a network that stands separately from the user nodes, only access nodes stand at the edge of this network. Relay nodes solely relay quantum traffic throughout this network. The fourth configuration is a variation on the centralised approach presented earlier. Here, all key relay functions of the KMs are centralised into a KM that is part of the QKDN controller that stands at the hierarchical head of the network. This simplifies functionality of the local KMs at each node, reducing network complexity at the cost of reduced scalability.

Then, clause 10 provides sequence diagrams for operational procedures in a QKDN. These include service provisioning, key generation, key request and supply, key relay, and key relay rerouting. If translated into industry standards, this should allow for equipment to become (almost) vendor-agnostic. The recommendation closes off with time synchronisation and security considerations. Much like earlier recommendations in this same series, the importance of both is stressed, but their details outside the scope of the recommendation.

4.3.4 ITU-T Y.3803. ITU-T recommendation Y.3803 is concerned with key management of a QKDN [62]. The recommendation's scope is noted to include "an overview of key management in a (…) QKDN; functional elements of key management; operations of key management; and key formats" [62]. Diagrams from Y.3800 and Y.3802 are presented to illustrate the point of using KMs. Y.3803 however, introduces the distinction between a Key Supply Agent, and a Key Management Agent (KMA). The KMA concerns itself with key storage, relay, and life cycle management. This is in line with requirements introduced in Y.3801. The KMA interfaces with other KMAs in QKD modules. The KSA is situated between the KMA and a cryptographic application. The KSA provides

key supply, and combination functionality in accordance with ITU-T recommendation X.1714 that is introduced in Section 4.3.12.

A KMA and KSA each have their own link according to the recommendation, but it is also noted that this would most likely will be the same link in practice. However, this allows for the possibility of having a node act as a relay station only, ie. by having only a KMA link and not a KSA link. Once again, the security demarcation also shown in Figure 2 is referred to as a demarcation of responsibilities. Only the KSA links will cross this demarcation, and once keys are handed over, their security becomes the responsibility of the recipient application on how they utilise it.

A schematic is presented that contains a reference model for key management within a KM, and how these are to be supplied to cryptographic applications. It depicts flow of keys, for both from a KSA to an applications, but also between KMAs for key relay. Keys are combined when they cross over to another KMA, and recovered by making use of an XOR operation that allows for having a key cross over from one side to the other across a link that spans multiple QKD relay nodes. A clause follows, that specifies the functionality of a KMA with regard to acquiring, authenticating, and storing keys.

Key relay between KMAs is described, including different specific protocols that should be used to attain this goal. These include using One-Time Pad (OTP), and Advanced Encryption Standard (AES). Key supply from KSAs to cryptographic applications is also dictated. Once again, X.1714 is referenced on how a key is to be generated, yet specifics for delivery are left beyond the scope of this recommendation. Only metadata for a KSA key is stipulated. Rerouting of key relay between KMAs is then presented, and four different cases where rerouting is to take place are presented. These are: manual, fixed rate, data-traffic adaptive, and scheduled. A key relay route can be set manually, be based on the key generation rates of one or more QKD links, be adaptive to the traffic that had recently flowed through key relay links, or be scheduled depending on predicted conditions such as key consumption or key generation rate. A reference is made to Y.3804, which is also presented in this section. Key life cycle management is then presented, one of the requirements presented in Y.3801. The responsibility of life cycle management lies with the QKDN manager.

Clause 9 of Y.3803 presents different approaches to key relay methods, which chiefly differ in the order of operations that are performed on the key material that is relayed. The recommendation closes of with a table containing metadata fields, with a description of each field and whether it is mandatory or optional.

4.3.5 ITU-T Y.3804. ITU-T recommendation Y.3804 stipulates "control and management" of a QKDN [61]. It is noted that the scope of the recommendation includes the functional elements of a QKDN, and functions and procedures of control, management and orchestration in a QKDN. A figure is presented that contains the functional architecture, which was already presented in Y.3802. In this version however, the QKDN controller and QKDN management have been highlighted as they are relevant to the work presented in Y.3804.

The QKDN control layer is introduced to realise proper operation of the QKDN as a whole. The QKDN control layer controls the quantum, and key management layers. This is achieved through communication control messages with the KMs, and QKD modules. The following functions are listed for the QKDN controller: routing, configuration, policy-based, access, and session control. In the subsequent clauses, functionality of each aspect is described in more detail. The routing control function manages a routing table for key relay functionality. This includes both creating new routes, and rerouting key relay paths. Different rerouting methods are already given in Y.8303. The configuration control function prescribes that the QKDN controller must be able to control and reconfigure QKD links and KM links if any sort of alarm is raised. These alarms could be raised in case of a failed link, or when an eavesdropping attack it detected through an increase in QBER. Policy-based control ensures that the QKDN controller is able to adhere to imposed QoS requirements. The access control function verifies that functional components of a QKDN are legitimate nodes in the QKDN. This includes issuing certificates for functional components, bookkeeping of these components, and performing authentication between the QKDN controller and any functional component using these issued certificates. The session control function is meant to support KMAs and KSAs with key delivery, and to ensure that this delivery is performed conform the imposed QoS standards utilising the policy-based control function.

The recommendation continues to list common management functions, which are formulated to fulfil requirements presented in Y.3801. These form a comprehensive description of functional requirements of a QKDN controller. The requirements are based on Fault, Configuration, Accounting, Performance, Security (FCAPS) requirements presented in ITU-T M.3400 and Y.3111 [51, 55]. These functional requirements are complimented with procedures of control, management, and orchestration of QKDN. These procedures are all described in step-by-step lists, which are also visualised in sequence diagrams.

4.3.6 ITU-T Y.3805. ITU-T recommendation Y.3805 is concerned with "Software-defined networking control" [67]. It specifies requirements and a functional architecture of a SDN controller and operational procedures of SDN control for a QKDN. The requirements that are listed form an extension of the ones that are mentioned in Y.3801, and introduce the existence of an SDN controller, that interfaces with the service, QKDN management, key management, and the quantum layers.

With the basic functional requirements described, the recommendation moves on to alternative, hierarchical models of an SDN controllers in a QKDN. These are to be deployed in large-scale QKDNs, or in cases where "only a single SDN controller is unsuitable for overall control in QKDNs" [67]. Then, basic operational procedures are given, through flow diagrams which are complemented with step-by-step descriptions

of how certain processes concerning SDN should take place in a QKDN. These procedures include key request, relay, and monitoring of different nodes in the QKDN.

4.3.7 ITU-T Y.3806. ITU-T recommendation Y.3806 contains requirements for QoS assurance [66]. The scope of this recommendation is noted to contain both high-level and functional requirements of QoS in QKDN. Once again the aforementioned link Ak mentioned in Section 4.3.3 is given special attention, as it is noted to be the main point of interest for QoS information towards another party that interacts with the QKDN. High-level requirements of QoS assurance are given, based on the requirements related to QoS from Y.3801 [59]. Subsequently, functional requirements are presented that stipulate QoS requirements for QKDN regarding planning, monitoring, service optimisation, service provisioning, and service protection. The recommendation closes off with security considerations that are to be adhered to, and references to existing ITU-T standards X.1710, Y.3801, Y.3802, Y.2701, and Y.3101 [53, 56, 59, 63, 65]

4.3.8 ITU-T Y.3807. ITU-T recommendation Y.3807 closely ties in with the work presented in Y.3806, as this recommendation presents "Quality of service parameters" [69]. The scope of this recommendation contains descriptions of QoS and network performance (NP) on QKDN, QoS parameters, a classification of performance concerns, and supporting factors of network performance.

The very same security demarcation as presented in Figure 2 plays an important role once again. Here, it represents the boundary between QoS on the user network side, and NP on the side of the QKDN. This recommendation only focuses on the former, and NP is left beyond the scope of this document. A distinction between QoS and NP is given, where it is stated that QoS focuses on service attributes, and user network-observable effects. Because of this, only the procedures relative to this boundary are relevant for QoS aspects of QKDN. These procedures take place in the KM and quantum layers, and across the link Ak from Section 4.3.3. They consist of key requests and key supply from the KSA, and notifications between cryptographic applications.

From these procedures, the QoS parameters follow. Throughput, KSA-key response delay, KSA-key response delay variation, KSA-key delivery error ratio, KSA-key delivery loss ratio, and availability are presented in the recommendation. As part of availability, service restoration time is also presented.

Privacy, security, and integrity aspects of QoS in QKDN are mentioned, but left beyond the scope of the recommendation.

4.3.9 ITU-T Y.3809. ITU-T recommendation Y.3809 "describes roles, a role-based model, and service scenarios in (…) QKDN from different deployment and operation perspectives" [70].

First, the roles are presented which consist of: security application service user, security application service provider, QKDN provider, QKDN management provider, and user network provider. A diagram is given on how these different roles interact, and by which means. Interactions via these interfaces are listed in a table.

From these roles, different models are presented that provide different role-based service scenarios of QKDN. An important remark is made: "This clause does not identify, in an exhaustive manner, all role-based models and service scenarios of a QKDN" [70]. The models are of varying levels of complexity, also containing examples where there can be multiple QKDN providers, and multiple QKDN management providers.

An implementation description is also provided as appendix, in order to guide the process of adopting the conceptual structures and roles of QKDN and user networks.

4.3.10 ITU-T X.1710. ITU-T recommendation X.1710 describes a "security framework for quantum key distribution networks" [63]. The scope of this recommendation is to provide a global overview of security in QKDN, from which following standards can follow in the series. This includes security aspects, threats, requirements, and measures. The recommendation only provides a security framework for QKDNs, security analyses of QKD protocols are beyond its scope.

The diagram showcasing the functional elements of a QKDN from Y.3800 is once again referenced. These functional elements each have their own security aspects, and from this diagram the relations between the elements is given, including the types of information that is transmitted between these elements. From these relations, an overview of security threats follows. Attack surfaces are identified in QKD, KM, control, and management links. Three kinds of threat are distinguished: intentional, administrative, and accidental.

Only intentional security threats lie within the scope of this recommendation. Within this category, the threats that are identified consist of: spoofing, eavesdropping, deletion or corruption, repudiation, and Denial of Service (DoS). As mentioned before this recommendation only considers the QKDN security framework, which puts security threats such as side-channel attacks outside the scope of this document.

Security threats are presented for all types of links within the QKDN, and outward to the user network, from which follow security requirements and measures to combat these threats. Detailed specification of the requirements is noted to be out of scope, but the recommendation does list categorical approaches per threat, which consist of authentication, access control, confidentiality, integrity, availability, and accountability. For all approaches, requirements are listed on how these are to be achieved.

4.3.11 ITU-T X.1712. ITU-T recommendation X.1712 is a description of key management in QKDNs [71]. This recommendation is concerned with security threats, requirements, and measures for key management in a QKDN. Security threats mentioned in this recommendation, are an extension of the ones from ITU-T X.1710 described in Section 4.3.10. Once again a diagram is shown representing all attack surfaces of a QKDN, however in this recommendation, a KM has been expanded into

a KSA and a KMA to display the two different links that exist between these different components.

The security requirements and measures introduced in ITU-T X.1710, are described more extensively in ITU-T X.1712 for each of the five categorical approaches per threat. The security measures listed are of a quite concrete nature, providing examples on how to approach these measures in a practical environment.

4.3.12 ITU-T X.1714. ITU-T recommendation X.1714 contains information about "key combination and confidential key supply for quantum key distribution networks" [60]. The recommendation specifies requirements for both the security of key combination and key supply between QKDN and applications. The recommendation notes that it focuses on two topics in particular:

- "the security of the combination of keys exchanged through a QKDN and keys exchanged through other key exchange methods;
- the security of the key supply from a QKDN to cryptographic applications." [60]

Key combination is argued to be a valuable feature of a QKDN, since it allows for a higher degree of proven security when used properly. As is noted: "The key resulting from an appropriate key combination can be secure as long as one of the keys used as inputs for this combination remains secure [10, 39]" [60] This would contribute towards making the adoption of a QKDN more feasible from a security point of view, with keys that are more likely to be provably secure. The recommendation lists security requirements for key combination methods, and for key supply between QKDNs and cryptographic applications in the user network. The requirements for key combination form a clear set of rules a system should adhere to. The requirements listed for key supply however are quite broad and few.

4.4 ISO/IEC Standards

Standardisation efforts produced by the International Organisation for Standardisation (ISO) are in close collaboration with the International Electrotechnical Commission (IEC). These standards however are not available to the public in their full form when still in drafting, and therefore this research will only briefly evaluate their general scope.

4.4.1 ISO/IEC DIS 23837-1. ISO/IEC DIS 23837-1 specifies a general overview of security requirements that are to be met in both QKD equipment and optical networking equipment [49]. This largely overlaps with the objectives set out in ETSI GS QKD 008, containing a QKD module security specification.

4.4.2 ISO/IEC DIS 23837-2. ISO/IEC DIS 23837-2 forms a set of evaluation activities that are meant to perform testing procedures on QKD equipment [50]. Once again there exists an overlap with existing work from ETSI, in this case with ETSI GS QKD 011.

4.5 Summary

In this section, a summary is given of the standardisation efforts that have been undertaken by the organisations listed in Section 4.1.

4.5.1 ETSI Group Standards. The Group Specifications produced by ETSI are comparably practical in nature. The presented work provides clear and concrete examples of requirements that are to be implemented in QKD modules, to ensure proper and secure operation. Their series of GSes start off with an overview of use cases, and the goals that QKD is supposed to achieve in GS QKD 002. Two of the presented use cases can be applied to the two proposed solutions from Research Question 1. GS QKD 008 is an extensive standard that presents security requirements that are to be implemented in QKD equipment. This document serves as a clear guideline on what QKD node certification could look like, and how it is recommended to be implemented by equipment vendors. For the implementation of a QKD link, GS QKD 012 describes the resources that are required to achieve this goal from a purely optical equipment standpoint. This serves as a step-up to the GS QKD 015 and GS QKD 018 where SDN and orchestration interfaces are presented, respectively. These list large amounts of parameters that are to be exchanged between QKD and optical equipment in order to support mechanics such as provisioning and monitoring. This leaves two more standards that are closely related; GS QKD 004 and GS QKD 014. Both present APIs for fetching quantum key material, but each take a different approach. GS QKD 004 is meant to provide vendors with a high degree of flexibility by presenting an implementation-independent description. GS QKD 014 on the other hand is meant as an API that is relatively easy to implement, at the cost of a higher degree of overhead due to the fact that it is a fully-fledged REST API built on top of HTTPS.

4.5.2 ITU-T Recommendations. Overall, the work that has been presented by the ITU-T in the series of recommendations ranging from Y.3800 to Y.3809 together form a clear set of requirements that are to be fulfilled for achieving a QKDN solution. Various aspects of QKD and QKDN are covered across the different recommendations. Next to these functional requirements - presented in Y.3800 and Y.3801 - there are also recommendations for the architectural implementation. Y.3802 provides the overview for general architecture, including basic operational procedures. The next recommendation in the series, Y.3803, stipulates functional requirements for the management of keys, which is handled in the two Key Managers. Y.3804 covers control and management, to be taken care of in the QKDN controller, for which different possible architectures are presented. Once again, functional requirements from Y.3801 are elaborated on, in the context of management of a QKDN. Recommendation Y.3805 extends the work presented in Y.3804, where an alternative form of control of the network is achieved through Software Defined Networking. Requirements for adhering to Quality of Service policies are given in Y.3806, such that a QKDN can perform as expected from other parties relying on the keys generated by the

network. These requirements are extended in Y.3807, where QoS parameters are introduced that allow for setting performance levels that a network should attain. Y.3808 contains requirements for integrating with a secure storage network, which is left beyond the scope of this study. Y.3809 then concludes the current range of recommendations with a description of roles and service scenarios in both deployment and operational perspectives. This last recommendation is more of a managerial perspective than an implementational one.

From the relevant recommendations in the series X.1710-X.1729 - currently consisting of X.1710, X.1712, X.1714, and X.1715 - a comprehensive set of system requirements follows, that describe various methods on securing a QKDN. X.1710 gives an overview of the general requirements that are to be met with respect to security in a QKDN, and give a framework for categorising various security threats that might pose against proper operation of such a network. The requirements for internal management of quantum generated keys is addressed in X.1712, where an overview is given of security threats, requirements, and measures to be taken in a QKDN. These measures are already of a relatively practical nature, compared to the more abstract requirements from X.1710. Recommendation X.1714 then closes off the series, and contains requirements on both key combination and key supply to a user network. The requirements for key delivery however, are still quite generic.

4.6 Future Work

For this research, this section on future work will constrain itself to the work that is needed in standardisation in order to be able to implement a QKDN in an optical network. Where other survey papers have remarked that work is to be performed in standardisation of fields such as CV-QKD and QKDN in free-space networks, these lie outside the scope of the paper [13, 80].

The work that is currently performed by both ETSI and the ITU-T serve as a strong basis for future harmonising standards, that will dictate the interoperability of QKD equipment, and their security. Recommendations published by the ITU-T currently give an overview of the possibilities with both QKD and QKDN, in particular in the recommendations in the series Y.3800 to Y.3809. These recommendations lay the groundwork for architectural approaches to QKDN, and the various aspects of maintenance of such a network. However, these publications are still of a conceptual nature, giving vendors little to hold on to in terms of implementation of equipment. The recommendations currently published in the range of X.1710 to X.1714 provide managerial requirements, security threats and use cases for a QKDN, that can be applied when designing and implementing a quantum secure solution.

The ETSI GS QKD series of documents present more practical aspects that focus on the operation of QKD equipment. This includes documents such as ETSI GS QKD 008, where security requirements are defined for QKD equipment. ETSI GS QKD 012 presents different approaches for integration of QKD with optical equipment, where the added value of multiplexing both quantum and data traffic onto the same fibre is shown.

The largest gap that is to be bridged, is the fact that the work produced by both the ITU-T and ETSI are either recommendations or specifications. Neither have the status of standards yet, which is needed for vendors to reach a consensus on the requirements that QKD related equipment needs to fulfil. Especially for key fetching APIs such as ETSI GS QKD 004 and GS QKD 014, which would allow for interoperability between QKD equipment and applications that seek to make use of generated quantum keys. Especially the API presented in ETSI GS QKD 014 has become the de facto standard for fetching quantum key material from QKD equipment, despite the fact that this document is still a Group Specification and not a European standard. This includes the QKD equipment from Toshiba used in this research. The same holds for the work presented in ETSI GSes QKD 015 and 016 for the integration of QKD in an SDN. YANG files are presented as examples of a possible implementation, but no industry standard exists yet. Further configuration of optical equipment to co-exist with QKD equipment should also be possible through a standardised API. ETSI GS QKD 012 already presents a relevant list of parameters for configuration. The Toshiba QKD equipment offers for remote monitoring which will be discussed in Section 7.4, however this is not implemented following any of the aforementioned standards. If this were the case, interoperability with equipment from other vendors would increase.

In the field of certification ETSI GS QKD 008, ITU-T X.1712, and especially ISO/IEC IS 23837 will form an important set of criteria for QKD to adhere to, in order to certify correct operation of the equipment in a secure manner. When this ISO standard is fully published and comes available to the national standardisation institutes, it will allow for certification of QKD equipment that ensures secure operation. As more techniques become commercially available however, the certification will have to keep up with these developments.

5 METHODOLOGY OF EXPERIMENTS

In this section, the experiments performed with the Toshiba equipment are presented. Research has been performed on the QKD testbed in the GÉANT Cambridge lab over a period of two months. The QKD equipment is integrated with Infinera DWDM equipment in order to gain an insight into the interoperability of the two systems. These experiments are performed with the objective of gaining a clear understanding of what will prove to be the challenges when implementing a QKD system in real-life. Part of the experiments is to investigate the performance of the system once the quantum channel and data channel coexist on the same fibre. In order to achieve this, the Toshiba QKD equipment's auxiliary (AUX) port is used to multiplex data and quantum traffic into the same fibre. The AUX port provides built-in wave-division multiplexing of the data and quantum signals.

5.1 Preparation

The first round of testing required calibrating the system and the initial setup, such that initial levels of attenuation are known. Insertion loss of the QKD boxes has been measured. There are two fibre spools that are used in various experimental setups. Both spools have a length of 50 km. Attenuation of the spools is measured in order to determine the total insertion loss between the QKD boxes. In the experimental set ups where transponders and optical amplifiers are present, built-in power measurement in these components are used to measure the level of attenuation of the system. Otherwise, experimental results only consider relative attenuation induced by the VOAs. This allows for investigation of the relative influence of attenuation on both SKR and QBER.

As the level of insertion loss of the setup will vary each time the optical wiring is reconnected, it may differ between each experimental setup. For this reason, a measurement of total loss is performed prior to testing for each experimental setup. Small variations in attenuation can be caused by various external influences deteriorating the quality of a connection, such as dust particles gathering on plugs.

5.2 Taking Measurements

When measuring the performance of the setup, both SKR and QBER are measured over a period of time. The measurement data is generated by the Toshiba equipment as an average over an entire block of measurements. These blocks are based on the principle of privacy amplification. This privacy amplification process takes place when detection events are converted into secret keys. This procedure is performed in order to limit the knowledge of a potential eavesdropper based on the bits that are made public by Bob. In part this privacy amplification process is based on finite size effects, where a higher degree of privacy amplification will correlate to a higher degree of security of the generated key material [76].

In order to attain a certain level of security, a set 'block size' is chosen to perform privacy amplification on. Because of this, the system will wait for a sufficient amount of key material to arrive, before outputting quantum keys. SKR and QBER readings are therefore still representative of the system, as they are taken as average over the total time it takes to generate one block of key material. As a result, a higher level of attenuation - which will cause fewer photon detection events to occur - will correlate with the system to take a longer amount of time before a collection of keys is generated.

5.3 Fixed Attenuation

Initial testing is performed with a setup that does not include any data traffic on the AUX ports, and where the fibre between the QKD boxes only includes a fixed attenuator in both directions. This is done in order to verify correct operation of the system. This setup is identical to the one given in Figure 3a, where only the attenuators at label C have been replaced with fixed attenuators.

5.4 Variable Optical Attenuators

Once initial testing is performed, and a baseline measurement made, the fixed attenuators are replaced with VOAs. A diagram of this testbed is given in Figure 3a. The attenuation is varied from the lowest value prescribed in the operation manual of the Toshiba equipment that is 3 dB, up to the point where the system will fail to properly perform key exchange. Attenuation is raised in increments of 1 dB, and 10 readings are gathered after the system has aligned and initialised. Readings consist of SKR and QBER. The average SKR and QBER of these 10 readings are each plotted against attenuation.

5.5 Adding Fibre Spools

After the testing with VOAs, both fibre spools are added to the setup, which results in the diagram shown in Figure 3b. In both directions, the fibre spool is directly attached to the transmitting equipment, with the VOA attached to the spool. This is done in order to maximise the effect of Raman scattering from introduced data waves in the C-band. Again, 10 readings of SKR and QBER are averaged, and added to the results. The goal of having both the tests with and without the fibre spools part of the system is to answer Research Question 4a.

5.6 Adding Multiple Auxiliary Data Waves

Once the system consists of fibre spools combined with the VOAs, the AUX ports on the QKD boxes are connected to the Infinera optical equipment. First, both sides are connected to a Infinera FlexILS OLS that introduces a data channel at a single wavelength. This is done because the setup of this testbed is less complicated than having multiple data waves present, which allows for gathering initial results more quickly. Second, ROADMs are connected in between of the OLSes and the QKD equipment on both sides in order to introduce data waves at higher power levels. The choice for Infinera equipment is made, since this

equipment is used in the GÉANT production network, of which this experimental environment is an approximation. A system diagram of both these setups are presented in Figures 3c and 3d.

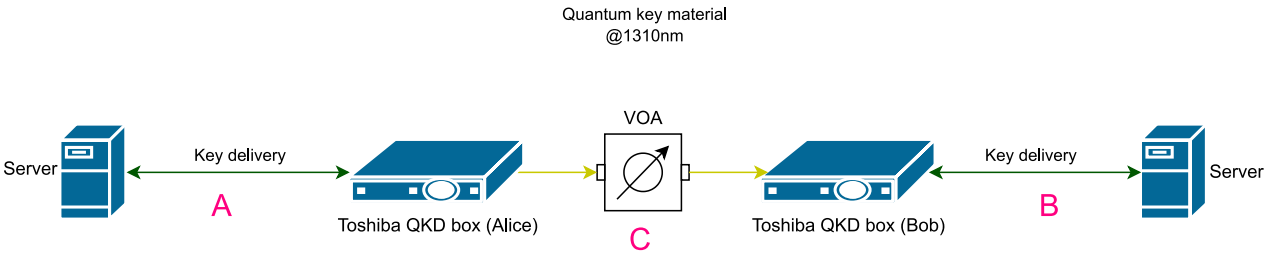
SKR and QBER are plotted against different levels of attenuation and against different power levels of the data channels. These SKRs and QBERs are averaged over 10 measurements.

5.7 Verification

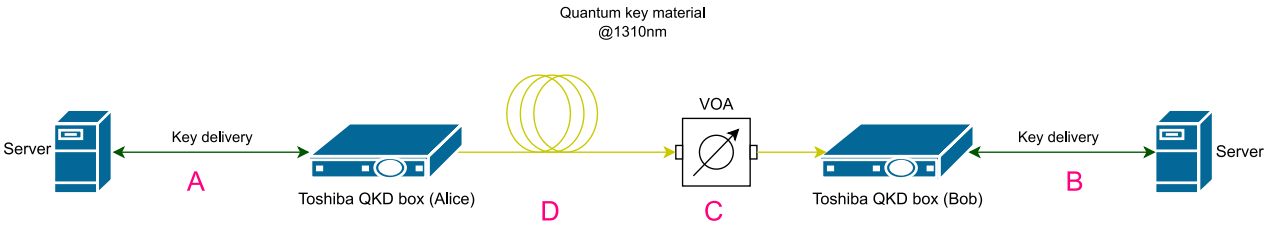
A statistical analysis is also performed on the data gathered. Performing this analysis gives an insight into the dependency of SKR and QBER on variables such as attenuation and the total power level of data waves that co-exist on the same fibre.

5.8 Comparisons

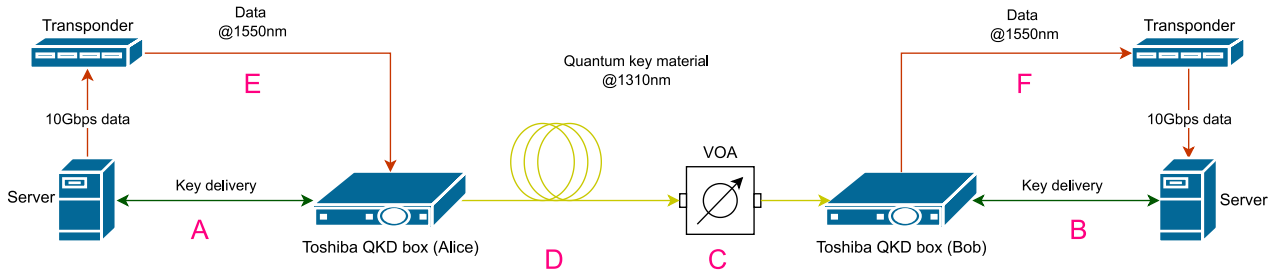
In order to get better insight into the state of the art in QKD equipment performance, a comparison will be made between the results of the Toshiba equipment, and results gathered in [99] and [90]. The first is a lab report that presents performance of QNu Labs equipment, the second contains experimental results of a lab setup investigated by Toshiba researchers.



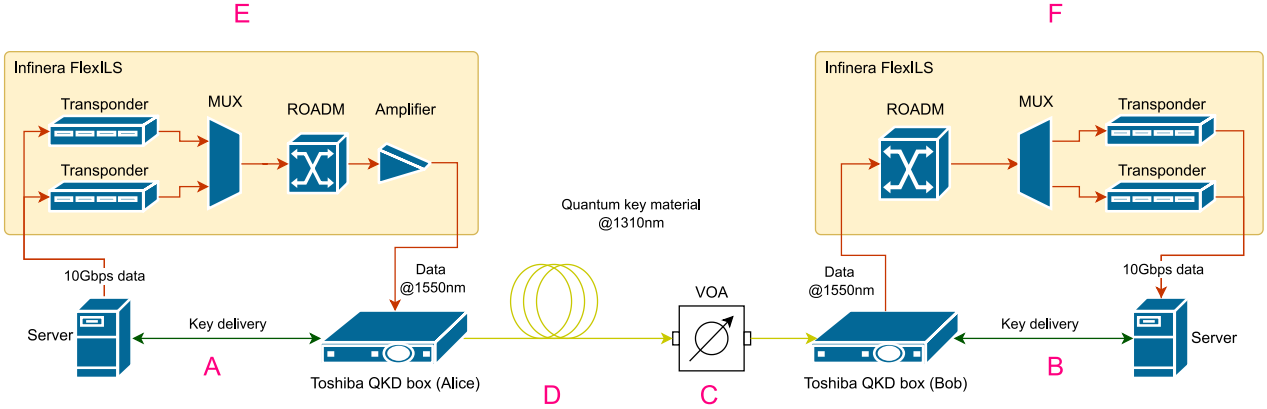
(a) Test setup where key exchange is labelled A and B, and attenuation is introduced by the VOAs at label C.



(b) Test setup where key exchange is labelled A and B, and attenuation is introduced by the VOAs at label C and fibre spools at label D.



(c) Test setup where key exchange is labelled A and B, and attenuation is introduced by the VOAs at label C and fibre spools at label D. Data is introduced through transponders labelled E and F.



(d) Test setup where key exchange is labelled A and B, and attenuation is introduced by the VOAs at label C and fibre spools at label D. Data is introduced through transponders labelled E and F. Data from two transponders is multiplexed together on both sides, passed through a ROADM, and amplified.

Fig. 3. Overview of Toshiba equipment setups. Green arrows indicate flow of quantum keys, orange arrows indicate flow of data, and yellow arrows indicate a mix of both quantum keys and data.

6 EXPERIMENTAL RESULTS

In this section, the results of experiments described in Section 5 are presented. First, a base-line reading is performed where the insertion loss of the QKD boxes in the current experimental setup is measured to be 1.42 dB through a single box.

6.1 Fixed attenuation

The system is set up as shown in Figure 3a, where the VOA at label C is replaced with a fixed attenuator. With a fixed attenuator of 10 dB, the system on average achieved a bit-rate of 1 020 600 bit s^{-1}, at a QBER of 3.2 %. The ten readings gathered are found in Table B.1-1.

6.2 Variable Optical Attenuators

With the system set up as shown in Figure 3a, measurements were made of the performance of the system when varying the attenuation of the VOAs between 3 dB to 24 dB. The upper limit of 24 dB was found to be the point, after which the system would no longer successfully align and was unable to perform QKD. The average values of bit-rate, QBER, and duration per level of attenuation are given in Table 8. The duration is measured as the time it takes for the system to present ten readings. The results are plotted as bit-rate and QBER against attenuation in Figures 4 and 5, respectively.

VOA Attenuation (dB)	SKR (bps)	QBER	Duration
3	2 817 000	3.31 %	0:01:15
4	2 829 000	3.22 %	0:01:12
5	2 771 000	3.26 %	0:01:12
6	1 899 000	3.27 %	0:01:49
7	1 842 000	3.21 %	0:01:53
8	1 368 000	3.28 %	0:02:26
9	1 086 000	3.40 %	0:03:00
10	985 000	3.38 %	0:03:24
11	677 000	3.26 %	0:04:48
12	558 000	3.28 %	0:05:50
13	502 000	3.42 %	0:06:22
14	338 000	3.42 %	0:08:51
15	283 000	3.39 %	0:11:13
16	250 000	3.42 %	0:12:25
17	175 000	3.46 %	0:17:40
18	154 000	3.55 %	0:19:40
19	120 000	3.60 %	0:24:28
20	84 000	3.60 %	0:35:03
21	64 000	3.71 %	0:44:27
22	48 000	3.93 %	0:54:19
23	35 000	4.01 %	1:10:28
24	27 000	4.15 %	1:29:35

Table 8. Average values of bit-rate, QBER, and elapsed time at different levels of attenuation induced by VOAs.

6.3 VOA and Fibre Spools

In the system setup shown in Figure 3b, fibre spools were introduced to induce additional attenuation. These spools are connected directly to the transmitting equipment, with the VOAs connected after the spools in both directions. The spool connecting `Alice` to `Bob` is found to have a level of attenuation of 13.1 dB, and the spool in the opposite direction a level of 10.6 dB. These spools will be referred to as spools 1 and 2, respectively. The levels of attenuation are measured using the built-in measuring equipment in the transponders present at labels E and F shown in Figure 3c. These were already connected, but not used in the current setup.

Once again, the VOAs that are part of the setup were varied from 1 dB up to the upper limit where the system would no longer initialise, which was found to be 12 dB. At this point, the system was found to

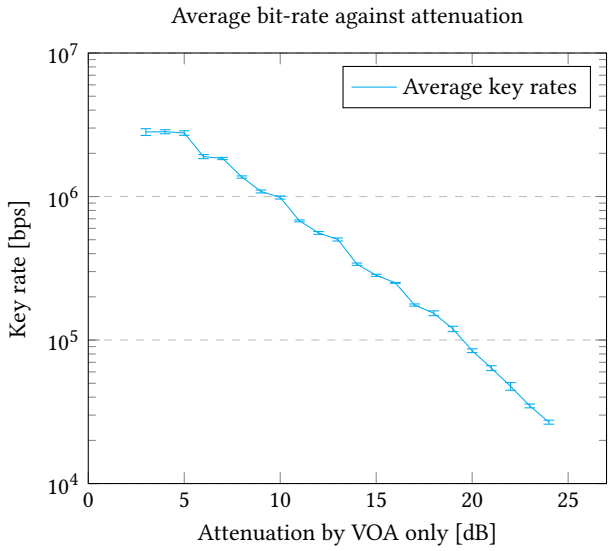


Fig. 4. Graph displaying the relation between SKR and attenuation induced by VOAs with no fibre spools present.

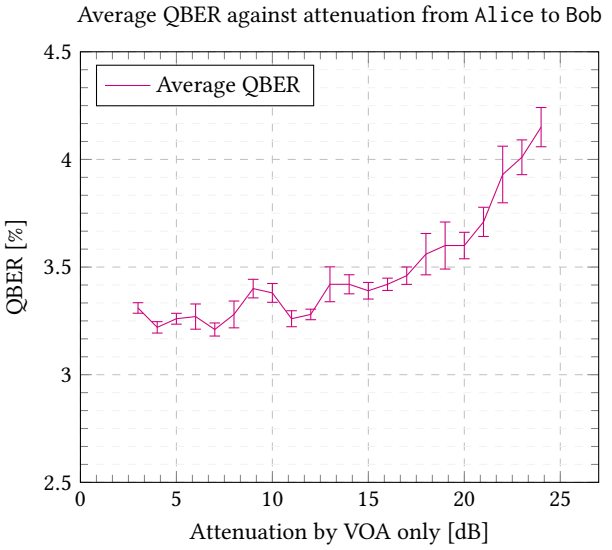


Fig. 5. Graph displaying the relation between QBER and attenuation induced by VOAs with no fibre spools present.

fall out of alignment numerous times. With the VOAs set to 13 dB, the system would no longer initialise successfully. The average values of SKR, QBER, and elapsed time can be found in Table 9. These values are plotted in Figures 6 and 7. As mentioned before, the attenuation of the system including the fibre spool, but excluding the VOA was measured to be 13.1 dB in the direction from Alice to Bob. As such, the aforementioned table and graphs all cover a range from 14.1 dB to 25.1 dB. All readings can be found in Appendix B.3.

During testing, two anomalies arose both when the VOAs were set to a level of 7 dB, resulting in total attenuation at 20.1 dB. As can also be seen in Table B.3-7, the time between readings output by the system varied significantly, compared to the other readings in this setup. Where readings would be output in a relatively consistent manner with other levels of attenuation, in this case the time between readings would vary between 24:06 and 2:01:53. No obvious reason was found for this to occur.

Attenuation (dB) Alice to Bob	SKR (bps)	QBER	Duration
14.1	43 700	4.13 %	1:03:05
15.1	34 800	4.32 %	1:09:25
16.1	24 600	4.27 %	1:46:31
17.1	20 500	4.68 %	1:48:55
18.1	13 300	4.63 %	2:46:20
19.1	8700	4.96 %	3:31:25
20.1	6500	5.29 %	9:40:05
21.1	3500	5.83 %	5:34:34
22.1	1800	6.43 %	6:02:29
23.1	300	6.89 %	15:01:32
24.1	0	8.03 %	10:54:38
25.1	0	8.88 %	10:13:35

Table 9. Average values of bit-rate, QBER, and elapsed time at different levels of attenuation induced by VOAs, in combination with two 50 km fibre spools.

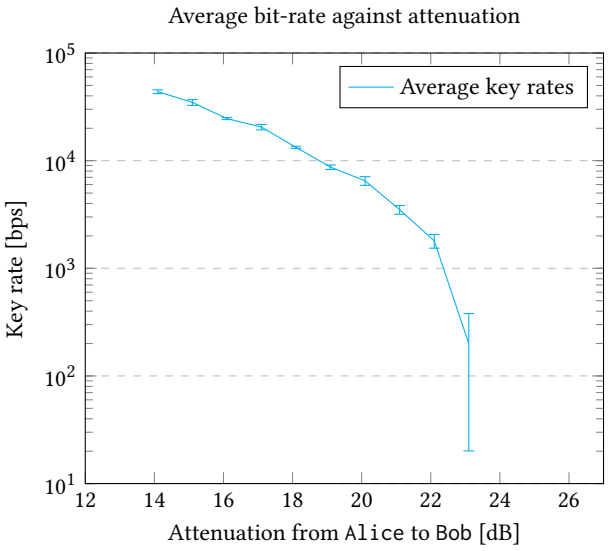


Fig. 6. Graph displaying the relation between SKR and attenuation induced by VOAs and fibre spools. (24.1 dB and 25.1 dB are missing, since a SKR of 0 cannot be displayed on a logarithmic scale.)

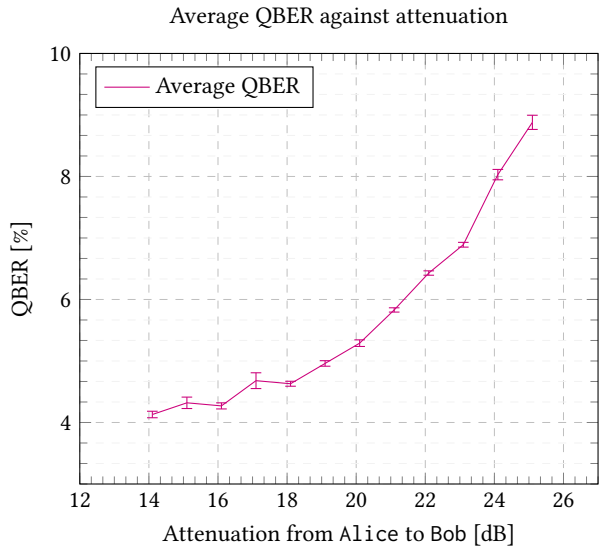


Fig. 7. Graph displaying the relation between QBER and attenuation induced by VOAs and fibre spools.

6.4 VOA, Fibre Spools, and Data

Moving on to the system setup in Figure 3c, a single wave of data is introduced onto the shared medium between the two QKD boxes. A set of baseline readings without an optical data wavelength at 1550 nm wave was gathered, data was transmitted at 0 dBm, and at +3 dBm. The average values can be found in Table 10. These three runs are combined into a single graph for SKR and QBER, which are found in Figures 8 and 9, respectively.

The fibre spools were connected arbitrarily during the construction of the setup, and the net attenuation from Alice to Bob was accounted for when performing a measurement of the attenuation of the setup excluding the VOAs. Spool 2 was connected in the direction from Alice to Bob, and spool 1 in the opposite direction. As a result, the attenuation of the entire system, excluding the set value of the VOA, was found to be 10.6 dB in the direction from Alice to Bob. The level of attenuation in the tables and graphs therefore ranges from 11.6 dB to 21.6 dB. With the VOAs set to 12 dB, the system would no longer successfully initialise. All readings from this test setup can be found in Appendix B.4.

6.5 VOA, Fibre Spools, and More Data

Finally, testing is performed in the test setup described in Figure 3d. Here, data is introduced on the shared medium through the AUX port on the QKD boxes at multiple wavelengths. Due to time constraints on the lease of the Toshiba equipment, the choice was made to perform testing at fewer levels of attenuation, to allow for testing at more power levels for the introduced data waves.

Attenuation (dB) from Alice to Bob	SKR (bps)	QBER	Duration
	No AUX data		
11.6	85 300	3.71 %	0:37:08
12.6	73 500	3.72 %	0:44:05
13.6	56 600	3.84 %	0:55:54
14.6	40 400	4.08 %	1:35:14
15.6	33 000	4.13 %	1:25:37
16.6	23 600	4.33 %	1:23:43
17.6	17 100	4.49 %	2:24:00
18.6	13 000	4.73 %	2:47:34
19.6	8000	4.92 %	4:23:05
20.6	6000	5.43 %	4:25:32
21.6	2500	5.97 %	6:54:10
	AUX data wave at 0 dBm		
11.6	86 000	3.71 %	0:37:20
12.6	74 300	3.73 %	0:44:04
13.6	56 900	3.82 %	0:55:56
14.6	35 500	3.97 %	1:24:26
15.6	31 100	4.27 %	1:25:15
16.6	23 900	4.34 %	1:47:09
17.6	18 200	4.48 %	2:14:30
18.6	12 900	4.77 %	2:47:37
19.6	8500	5.18 %	3:32:53
20.6	5500	5.61 %	4:43:56
21.6	2900	5.88 %	6:55:02
	AUX data wave at +3 dBm		
11.6	105 300	3.76 %	0:40:01
12.6	74 200	3.86 %	0:40:56
13.6	54 800	3.89 %	0:56:51
14.6	35 900	4.01 %	1:23:02
15.6	31 800	4.21 %	2:19:56
16.6	21 000	4.27 %	2:12:09
17.6	16 700	4.57 %	2:24:23
18.6	12 300	4.80 %	3:00:03
19.6	8200	5.24 %	3:46:12
20.6	5700	5.49 %	4:25:39
21.6	2100	6.34 %	6:00:05

Table 10. Average values of bit-rate, QBER, and elapsed time at different levels of attenuation induced by VOAs, in combination with two 50 km fibre spools.

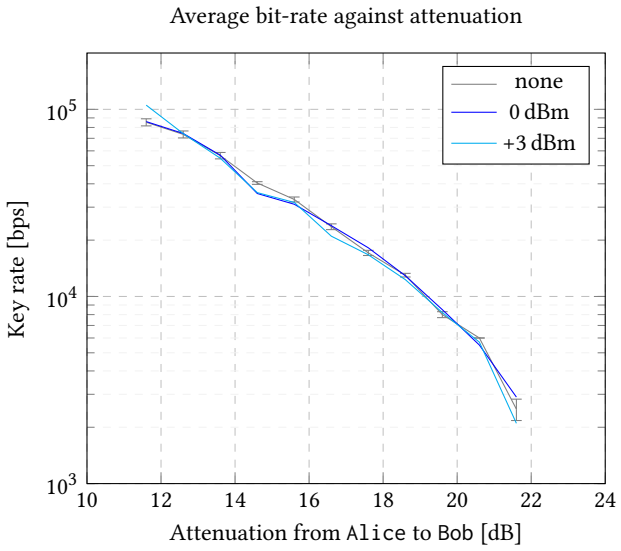


Fig. 8. Graph displaying the relation between SKR and attenuation induced by VOAs and fibre spools, including varying levels of data transmitted onto the shared medium.

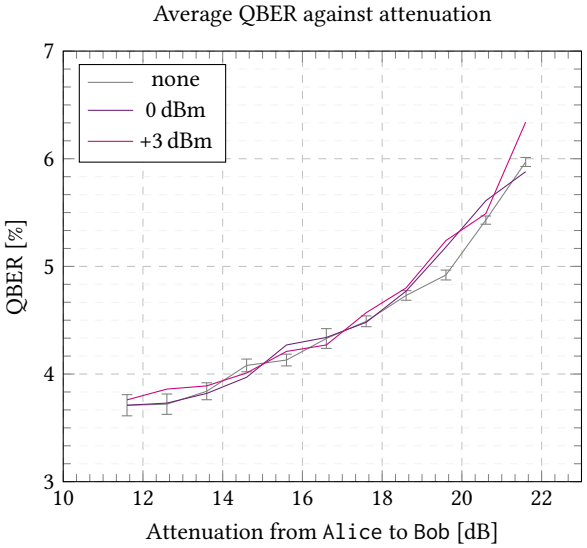


Fig. 9. Graph displaying the relation between QBER and attenuation induced by VOAs and fibre spools, including varying levels of data transmitted onto the shared medium.

To be able to perform testing with data transmitted at multiple wavelengths, ROADMs were added to the test setup such that the data waves are multiplexed together. The Infinera equipment needs to be able to communicate configuration data for proper operation, which is done on a separate channel outside of the C-band, this is known as the Optical Supervisory Channel (OSC). For the Toshiba equipment to perform optimally, passband filters are present in the equipment that filter out all traffic outside of the C-band. This blocks the Infinera OSC and required the ROADMs to be set to submarine cable mode, which disables the use of this OSC. Appendix A contains two spectrum readings where the presence of the OSC is made apparent.

Figure 10 displays the two optical data waves at which the data channels are transmitted. These readings are taken with the optical power meter that is built into the ROADM on the side of Alice.

The VOAs were set to four different levels of attenuation. Attenuation of the system excluding the VOAs was measured to be 13.5 dB from Alice to Bob, as this direction incorporated spool 1. The upper limit for the VOAs was found to be 10 dB, at higher power levels for the data waves. Above this levels of attenuation, the data wave at the receiving end was too weak to be detected by the optical equipment, and was shut down by the Automatic Laser Shutdown (ALS) feature when a fibre is suspected to be cut. When testing at lower levels of transmission power, the data wave was shut down by the equipment. Due to the aforementioned time constraints, further tests were carried out at a

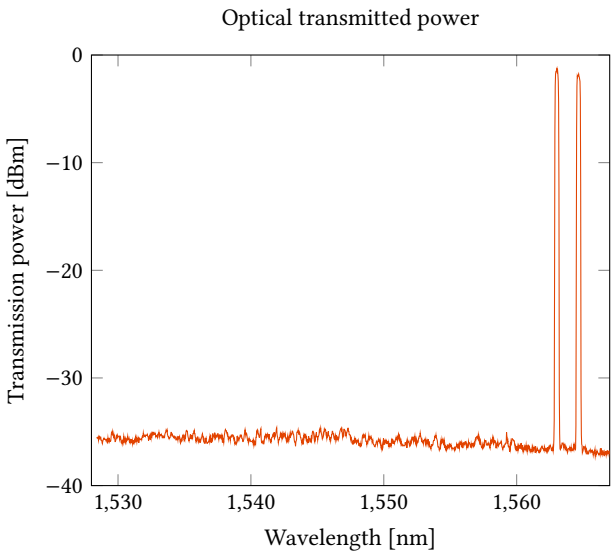


Fig. 10. Graph that displays the two transmitted optical data waves, centred around 1563.0 nm and 1564.6 nm. The graph displays the entire C-band.

maximum level of attenuation at 9 dB instead, such that a comparison can still be made between the tests carried out at different transmission power levels. The highest total optical transmit power level onto the fibre during this experiment was +17.8 dBm being the net optical power for the two wavelengths, which was the highest power level the optical equipment was able to output in the setup used. This is equivalent to 80 wavelengths each of −1.5 dBm, a typical power level for a fully operational C-band system.

Table 11 contains the average values of SKR, QBER, and total duration. All readings can be found in Appendix B.5. These runs are combined into two graphs, one for comparing SKRs, and one for comparing QBERs, these can be found in Figures 11 and 12, respectively. As stated in the operation manual of the equipment, the highest allowed optical power received at `Bob` may not exceed −6 dBm, beyond which point communication with `Alice` is not guaranteed by the manufacturer. The system was able to perform past this limit in the following experiments, but it should be noted that performance may become less predictable, as the system is operating out of the power bounds set by the manufacturer. In the tables and figures that display SKR and QBER, readings that took place beyond this threshold are in bold or circled, respectively.

As can be seen in Table 11, there are only two levels of attenuation on which testing was performed when the total power of the data waves was set to +17.8 dBm. This was caused due to the fact that testing the system at the high level of power from the data waves, rendered the system unusable. This will be elaborated upon in Section 8. All measurements can be found in Appendix B.5.

6.6 Evaluation

In order to ensure statistically significant results, a small analysis is performed on the data gathered from the experimental phase of this

Attenuation (dB) from `Alice` to `Bob`	SKR (bps)	QBER	Duration
	AUX data wave at −1 dBm		
14.5	81 500	3.85 %	0:38:48
17.5	37 300	3.96 %	1:21:14
20.5	15 800	4.57 %	2:30:50
22.5	7200	5.27 %	4:01:44
	AUX data wave at +6 dBm		
14.5	68 000	4.06 %	0:42:53
17.5	34 200	4.33 %	1:17:21
20.5	12 900	4.89 %	2:33:15
22.5	7000	5.34 %	3:59:11
	AUX data wave at +9 dBm		
14.5	**70 000**	**4.21 %**	**0:38:39**
17.5	29 800	4.64 %	1:15:45
20.5	14 700	4.96 %	2:17:10
23.5	3500	5.92 %	5:01:45
	AUX data wave at +12 dBm		
14.5	**66 000**	**4.44 %**	**0:37:48**
17.5	**26 200**	**4.89 %**	**1:16:12**
20.5	11 500	5.18 %	2:34:21
23.5	2400	6.17 %	4:58:48
	AUX data wave at +15 dBm		
14.5	**56 800**	**4.93 %**	**0:37:38**
17.5	**24 700**	**5.19 %**	**1:16:24**
20.5	**8600**	**5.70 %**	**2:31:20**
23.5	1300	6.73 %	5:03:44
	AUX data wave at +17.8 dBm		
14.5	**49 800**	**5.48 %**	**0:36:33**
24.5	0	8.12 %	6:20:46

Table 11. Average values of bit-rate, QBER, and elapsed time at different levels of attenuation induced by VOAs, in combination with two 50 km fibre spools. Two data waves are introduced on the AUX channel various power levels.

research. The figures presented in this section all include error bars, which are calculated as the 95 % Confidence Intervals (CIs). These are calculated based on the data points presented in Appendix B. When looking at these error bars, it allows for predictions to be made on the influence of external factors such as attenuation on the operation of a QKD link.

First, the impact of attenuation alone on SKR and QBER is elaborated upon. As can be seen in Figures 4, 6, 8 and 11, SKR decreases as attenuation increases. This behaviour is expected, and helps confirm that the equipment was operating properly. Figures 5, 7, 9 and 12 showcase the influence of attenuation on the QBER. Here it is also shown that, as attenuation increases, the QBER follows in an upward trend.

Second, the influence of one or more foreign data waves on the SKR and QBER is highlighted. When looking at Figures 8 and 9, it is shown that the introduction of a data wave at 0 dBm or +3 dBm does not significantly influence the SKR or QBER. In both graphs, data points largely fall within the CIs shown for the case where there is no auxiliary data present.

Third, the graphs in Figures 11 and 12 display the influence of the introduction of data waves at higher levels of power, more representative

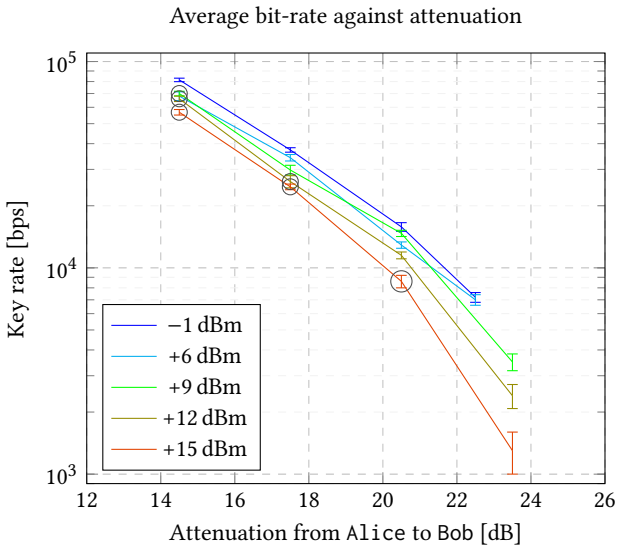


Fig. 11. Graph displaying the relation between SKR and attenuation induced by VOAs and fibre spools, including varying levels of data transmitted onto the shared medium. (17.8 dB is missing, since a SKR of 0 cannot be displayed on a logarithmic scale.)

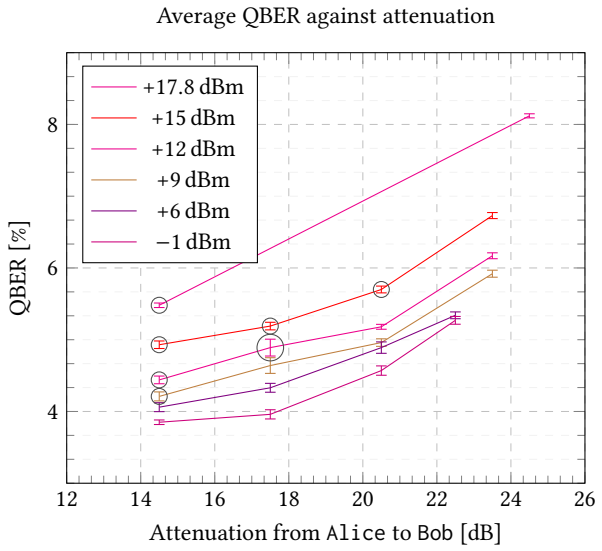


Fig. 12. Graph displaying the relation between QBER and attenuation induced by VOAs and fibre spools, including varying levels of data transmitted onto the shared medium.

of a real-world situation that is expected to be present in a PoP. Here, it becomes apparent that data waves at higher power levels do indeed impose a performance impact on SKR and QBER, as the 95 % CIs are mutually exclusive for most power levels, apart from a few exceptions where two data power levels will overlap at certain levels of attenuation. Especially in the case where total data wave power is set to +17.8 dBm, a large influence is illustrated.

Considering the test setup where multiple data waves are present, an estimate can be made on the performance of SKR and QBER as the level of data transmitted increases. For every +3 dBm increase in optical transmission power, SKR goes down by approximately 15 % and QBER goes up by 6 %.

From the results, it becomes apparent that a VOA is not able to replicate the effects of the use of a fibre spool on SKR and QBER. Comparing the results between Tables 8 and 9, the use of a fibre spool will on average decrease SKR by 93 % and increase QBER by 46 % at a comparable level of attenuation.

6.7 Comparison

The experimental results are compared to achieved results in related work, both with equipment from QNu Labs, and with an experimental lab setup by Toshiba where performance of QKD traffic is multiplexed together with data channels onto a shared fibre.

6.7.1 QNu Labs Equipment. With the results gathered from the experiments, a comparison can be made with the results presented in [99] where QNu Labs equipment was investigated. Different levels of attenuation were tested with various lengths of fibre spools, and impact of DWDM data was investigated. It was found that the system would sustain levels of attenuation up to approximately 21 dB, at a QBER of 4.5 % on average. This is comparable to the SKR performance seen of the Toshiba equipment, at a similar level of attenuation and a lower QBER. However, the SKR of the QNu Labs equipment was significantly lower than that measured with the Toshiba equipment, as it was found to be approximately 5000 bps for attenuation levels between 2.8 dB and 21 dB. Maximum SKR achieved is noted to be 15 000 bps, much lower than the 2 800 000 bps listed in Table 8.

6.7.2 Toshiba Labs Experimental Setup. Comparing the experimental results from this section to the results presented in [90], the achieved performance of both setups is quite similar. Patel *et al.* were able to achieve a SKR of 2 380 000 bps, and a maximum fibre length of 70 km. This SKR was achieved over a fibre length of 35 km, which corresponds to a level of attenuation of 7.7 dB at 1550 nm. Such performance was not achieved in this research. However, in [90] the setup was able to sustain a data wave launch power of +5 dBm as opposed to the +17.8 dBm presented in Table 11. The maximum achieved fibre length of 70 km corresponds to a level of attenuation of 23.1 dB at 1310 nm, which is comparable to the 23.5 dB at 1310 nm presented in Table 11.

7 IMPLEMENTING QKD SERVICES

This section presents an overview of what is needed for GÉANT to build a QKD solution it its network. First, general requirements are presented that would allow QKD links to be established in the network. From this, two subsections will follow that each present the implementation of the two service types presented in Research Question 1, and provide answers to the questions raised in Section 3. This overview also includes requirements for maintenance and monitoring, to provide an answer to Research Question 3. This research focuses on the hardware challenges when building QKD services in the GÉANT network. The existence of proprietary software stacks built by individual QKD equipment vendors is acknowledged, however these stacks were not tested. Without an agreed set of standards to test the software stack against, and without a clearly defined use-case for QKDaaS, evaluation of the proprietary software stacks is left beyond the scope of this research. The work that is needed to address this challenge is covered in Section 9.

7.1 Establishing Operational QKD

Establishing a QKDN will involve creating QKD links between all PoPs in the network, such that keys can be exchanged throughout the entire network. First, the implementation of a single QKD link is presented.

7.1.1 Establishing a QKD Link. For the purposes of implementation of a QKD link, this overview focuses on Toshiba equipment. This is due to the fact that Toshiba equipment has been investigated in a lab environment in Section 5, and the performance of the equipment has been quantified, when combined with optical transmission equipment used in GÉANT PoPs. The network in GÉANT at the moment of writing consists of 230 spans of fibre that are lit using Infinera FlexILS equipment. The average measured attenuation for each link has been collected in a histogram that can be found in Figures 13 and 14. Note that for the implementation of QKD, only half of these spans will need to be used, as each link will consist of two fibres. One for transmitting and one for receiving data from the other PoP.

In order to be able to use at least 90 % of the links in the network with QKD capabilities would require sustaining a level of attenuation at 33 dB multiplexed together with data channels at multiple wavelengths which add up to a total launch power of up to +20 dBm if the entire C-band is filled. Multiplexing of the quantum and classical channels should be performed in accordance to ETSI GS QKD 012. When multiplexing however, the Toshiba equipment filters out light outside the C-band, which includes the OSC of the Infinera transmission equipment that is currently deployed in the GÉANT network. To be able to keep making use of this channel, it would be required for Toshiba to modify their optical multiplexer to create a bespoke filter for GÉANT that passes the OSC. This is presented in ETSI GS QKD 012 by means of communicating network parameters - such as synchronisation channel wavelength - between the QKD and the optical transmission equipment.

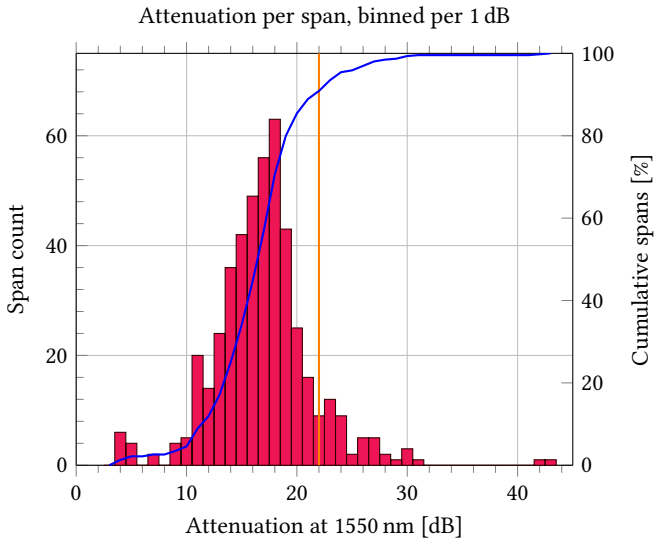


Fig. 13. Histogram of the amount of fibre spans, binned per 1 dB against attenuation of the link span at 1550 nm. On the left y-axis there is absolute span count which corresponds to the bar graph in red. On the right y-axis, the cumulative percentage of spans, marked with the blue line. The link spans left of the orange line can be used by long rage QKD equipment that operates in the C-band.

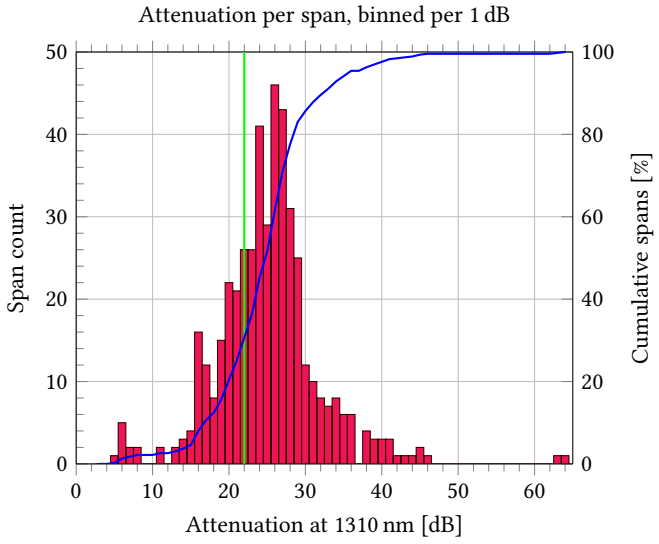


Fig. 14. Same as Figure 13, but with estimated attenuation at 1310 nm. On the link spans left of the green line, it is expected that quantum and data waves can be multiplexed on the same fibre.

In the case where GÉANT buys a dedicated fibre for the quantum channel and this is lit using Toshiba's 1550 nm equipment, Figure 13 shows that it is expected that 90 % of spans have an attenuation that will allow quantum keys to be carried. In the case of short links, GÉANT could multiplex data and quantum keys on the same fibre. Data is then transmitted in the C-band, and QKD is performed in the O-band at 1310 nm. According to Figure 14 this will only work for around 37 % of GÉANT fibre spans. For the 10 % of links that are too long for even dedicated fibre, there are two possible solutions: re-design the system

with shorter link spans such that attenuation is lower, or to wait for the next generation of QKD technology that is possibly able to sustain the higher level of attenuation on the link spans.

For the installation of the QKD equipment itself, little to no additional hardware is required. Every set of QKD equipment to be installed on one end of a link span consists of the QKD transmission equipment itself, and a 'control unit'. In total these add up to a required rack space of 3 U on each end of the link. Both of these will need to be provided with power, and two Ethernet connections must be available. One for the delivery of quantum keys, and one separate connection for management and monitoring.

All required software for QKD operation itself is provided by Toshiba, and is integrated into the control units that are present on both sides of a link. Further software solutions required for utilisation of the quantum keys or operation and maintenance will be discussed in the following subsections.

7.1.2 Establishing a QKDN. For the implementation of a fully-fledged QKDN that offers QKDaaS, ITU-T recommendation Y.3802 provides an overview of the components that are required. Four layers are defined, each with their own requirements: the quantum layer, key management layer, QKDN control layer, and the QKDN management layer. A functional architecture from Y.3802 is shown in Figure 15. To ensure that properly secure equipment is deployed in the network, certification must be available that verifies that the QKD equipment is indeed safe to use in a production environment. As is discussed in Section 4.6, such certification does not exist at the moment of writing, with standards such as ISO/IEC IS 23837 currently under development. Once available however, this certification is paramount to the security of the QKDN.

The Quantum Layer. The fundamental layer, as shown in the diagram in Figure 15, is the quantum layer where the key material is exchanged between QKD modules. Establishing such a layer is described in the previous section. However, this quantum layer will have to communicate with the management layer. This is accomplished though the management interfaces that connect to the control units supplied with the Toshiba equipment. These management interfaces require that security certificates are installed, to ensure that only authorised users are able to fetch keys from the equipment.

Key Management Layer. Directly interfacing with the quantum layer, is the key management layer. This layer is responsible for the relay of keys across multiple hops in a QKD link. Software for this purpose is not yet available for a production environment. A solution such as AIT QKD R10 contains protocols for forwarding quantum keys across a single QKD link, a routing protocol for the QKDN control layer, and a transport layer protocol that enables quantum keys to traverse a QKDN [86]. However, this software is indicated to be incomplete, and is missing required functionality such as IPSec. On top of this, parts of the protocols listed above are not yet fully implemented and therefore cannot be used in a production environment. From the work that presents these protocols as part of the European SEcure COmmunication based on Quantum Crytography (SECOQC) effort, it is stated that "it must be stressed that the SECOQC approach allows complete interoperability in the trusted repeater regime but is not directly transferable to switched or mixed networks" [91]. Similar approaches to SD-QKD have been demonstrated, but this has only been in lab environments [3, 109]. A ready-made software solution therefore does not exist yet.

QKDN Control Layer. As prescribed in recommendation Y.3804 presented by the ITU-T on control and management of QKDN, it becomes clear what work needs to be performed in the QKDN control layer [61]. As already described in Section 4.3.5, the QKDN control layer will have to be able to fulfil the task of routing, configuration, access, and session control. For the Layer 2 encryption solution in the GÉANT network however, little routing will have to be performed. Because of the fact that keys are to be used at the far ends of each QKD link, and to be used within the PoP where the link terminates only, keys will only have to be forwarded across a series of link spans. This is not the case for QKDaaS, as keys will need to be routed and forwarded across a QKDN. Management of access to quantum keys will depend on the service that is offered, and will therefore be presented in later subsections.

QKDN Management Layer. The QKDN management layer is used for the monitoring of the system as a whole. In the case of a link going down, the network should be able to make use of quantum keys that have been forwarded along an alternative route. This would help guarantee continuous operation of the QKDN. The management layer will therefore have to support re-routing of key material, and be able to discover routes across the QKDN that are operational based on available monitoring data. This management layer is made a distinctly separate layer, since routing will have to be performed by a piece of software that is not bound to compatibility with a single equipment vendor. It should be possible for equipment of multiple vendors to co-exist on a QKDN without a loss of functionality.

The Service Layer. The upper layer of the architecture consists of the service layer, of which the exact implementation will depend on the service that is to be offered by GÉANT. As such, the two different approaches to a service layer will be presented in the separate subsections that follow. For both of the services, this is software that will have to be developed by GÉANT. This is because of the fact that both services will require features that are highly specific to the GÉANT network and the way it operates.

7.1.3 Implementation Cost of a QKDN. It is estimated that at current commercial prices the cost of enabling the entire GÉANT network with QKD will cost in the tens of millions of Euros. Even without the labour cost of installing this equipment at all relevant PoPs in the network, the total price tag will already add up to a substantial portion of what has been spent on the entire GÉANT network in total. Because of this, it

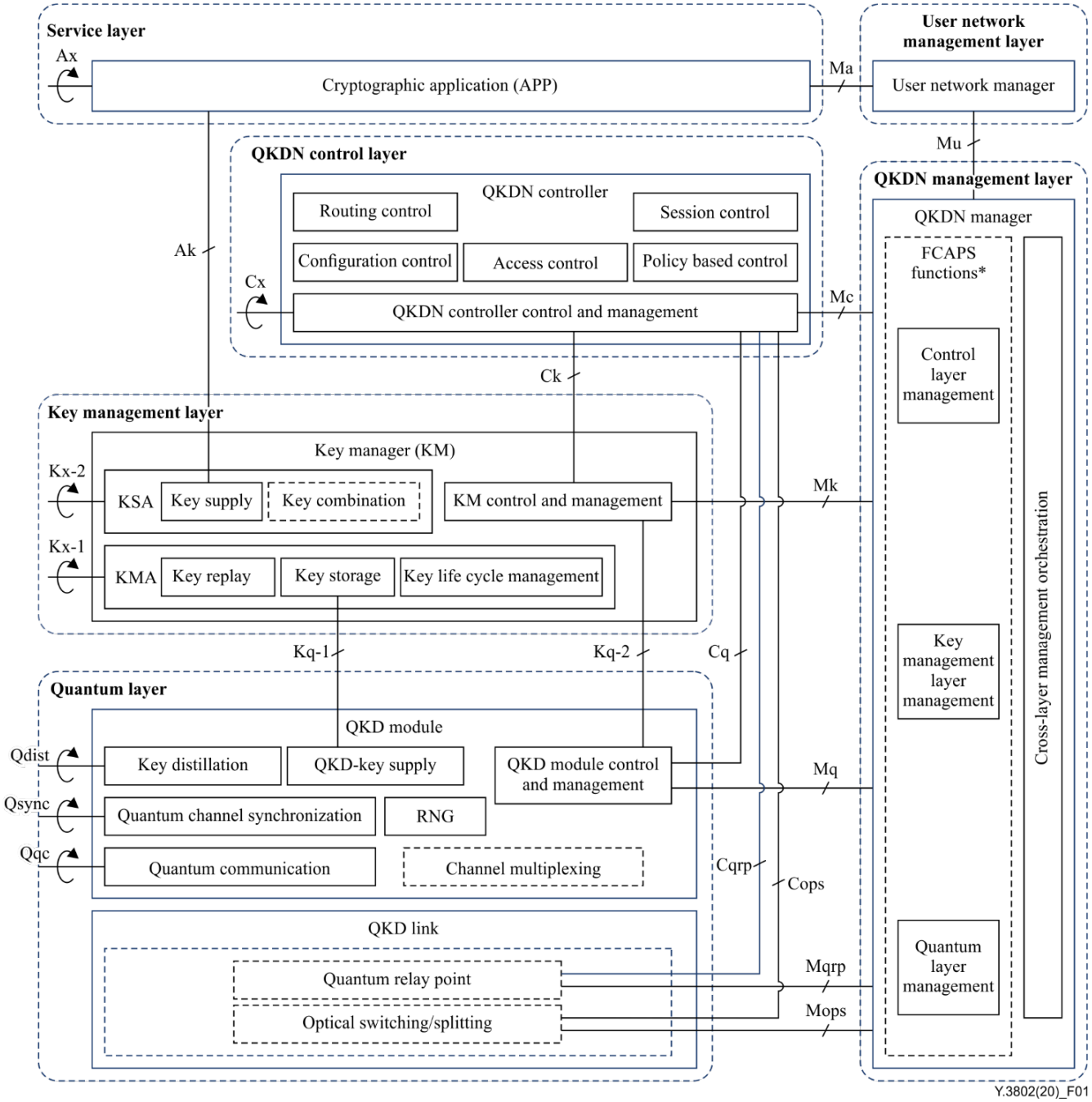


Fig. 15. Diagram from ITU-T Y.3802 that shows a functional architecture of QKDN [65].

will be necessary to prioritise the implementation of a QKDN in the GÉANT network. For example, an initial deployment on the western ring - consisting of the PoPs London 1 and 2, Amsterdam, Frankfurt, Geneva 1 and 2, and Paris - would focus investment on the part of the network that sees the greatest amount of traffic and therefore be best returns on investment. In this case there are 53 link spans that need to be covered, which would reduce the cost to be one quarter of the cost of covering the entire GÉANT network.

There is also an important difference in cost when considering to multiplex data channels and quantum key channels onto the same fibre. If QKD were to be implemented on the western ring alone, this would already add up to a significant cost in dark fibre IRU leases alone. At a total length of 3462 km, the total cost of ownership of the 15 link spans adds up to over €6 000 000. This cost could be reduced by making use of equipment that allows for multiplexing of quantum traffic onto an otherwise unused piece of spectrum.

Object	Value
TOSHIBA-QKD-MIB::qkdOperStatus	INTEGER: qkdOperational(1)
TOSHIBA-QKD-MIB::qkdServerToQkdUnitStatus	INTEGER: ok(1)
TOSHIBA-QKD-MIB::qkdClassicalChannelStatus	INTEGER: ok(1)
TOSHIBA-QKD-MIB::qkdKeyDeliveryLinkStatus	INTEGER: ok(1)
TOSHIBA-QKD-MIB::qkdClassicalRxPowerStatus	INTEGER: ok(1)
TOSHIBA-QKD-MIB::qkdSecureBitRate	Gauge32: 2861000
TOSHIBA-QKD-MIB::qkdQuantumBitErrorRate	Gauge32: 315

Table 12. Example output of Toshiba equipment on its Simple Network Management Protocol (SNMP) interface when operating on a QKD link.

In the GÉANT network, two types of optical amplifiers are used. Both In-line Amplifier Modules (IAMs) and In-line Raman Modules (IRMs) are deployed at amplifier stations along links. As the IRM based amplifiers utilise Raman pumps to increase the power level of data waves on the fibre after data and quantum key waves are multiplexed together, this has the unavoidable side-effect of destroying the quantum states that are sent on the quantum channel. This is due to the fact that amplification takes place after data wavelengths are multiplexed with the quantum key traffic, which conflicts with the no-cloning theorem as presented in Section 2.5 [2]. In the IAMs, the amplification of the photons takes place before they are multiplexed with quantum key traffic onto the shared medium, which prevents unwanted amplification of quantum key photons [110]. With the way that the amplifier stations in the GÉANT network are built, this introduces an additional cost for implementation. 168 IRMs would need replacing with IAMs in amplifier stations. This increases the total cost of implementation by approximately one third of a million Euros.

Subsequent work will have to be performed on where in the GÉANT network the demand for quantum key services is the highest, this is beyond the scope of this research.

7.2 Encryption of Layer 2 Traffic

Implementation of a solution that encrypts all Ethernet traffic in the GÉANT network will follow a similar approach to the one presented as use case number 2 in ETSI GS QKD 002 [28]. If implementing the solution presented in Research Question 1a, relatively little new optical transmission equipment is required. The ROADMs that are currently in use in the GÉANT network already support the use of cryptographic keys for hardware-based Ethernet encryption.

However, software support in the optical transmission equipment is lacking at the moment of writing. Infinera are currently working on the implementation of the API from ETSI GS QKD 014, which would make the use of quantum keys possible with all G30 model transponders in the GÉANT network. Collaboration with Infinera is possible, as they are keen to test a potential solution in a production environment. Actual support for this however, is currently unavailable.

7.3 Quantum Keys as a Service

In order to be able to offer QKDaaS in a QKDN to GÉANT's customers, much more work is needed compared to the encryption of Layer 2 traffic. As customers can request keys at each PoP, key material will have to be propagated across the entire network. This poses a significant increase in complexity of required routing protocols that will have to be in place.

Fetching of keys at PoPs will be the responsibility of the customer, and is readily possible when making use of the ETSI GS QKD 014. The API will however have to be rate-limited, in order to prevent one or a few customers from fetching all available keys at a higher rate than the rate at they replenish. This would effectively result in a DoS of the QKDN. The rate at which customers are able to fetch keys is also directly influenced by the SKR of a corresponding link. As such, the required performance of the system depends on the expected demand for QKDaaS on a link.

For access management of the QKDN, customers will have to be whitelisted in order to prevent malicious access to quantum keys. This adds an administrative burden on the provisioning of the service.

7.4 Operation and Maintenance

The following section seeks to answer Research Question 3. For this, the implementation of sufficient maintenance and monitoring capabilities will be restricted to Toshiba equipment. First, the requirements for maintenance of the equipment is presented. Second, monitoring is addressed.

Toshiba Equipment Maintenance. For the maintenance and servicing of the equipment by Toshiba, a service contract will be in place. Under this maintenance agreement, all parts and labour are included for repairs. For these repairs to be performed, equipment will either have to be returned to Toshiba, or a field engineer could be deployed for on-site repairs. This does not cover malicious or accidental damage to the units, for which additional costs would be incurred as this falls outside of such a maintenance agreement. GÉANT will therefore have to pay for a maintenance fee, and GÉANT will have to ensure that Toshiba perform an annual health check of all equipment.

To be able to remotely sense health of the equipment, VPN connections to all control units will have to be put into place. This will also allow for the remote deployment of software security updates that might be necessary, for properly secure operation of the equipment. This will

increase the complexity of the implementation however, since amplifier stations do not provide internet access at the time of writing.

Monitoring a QKDN. For the monitoring of the proposed QKDN, various tools and protocols exist for the sections of the network outside the quantum realm. However for monitoring of the quantum layer, software solutions will have to be developed to be able to keep an insight in the current performance of the QKDN.

Toshiba equipment comes provided with an Simple Network Management Protocol (SNMP) interface that allows for polling equipment statistics. These include current SKR, QBER, and operational status of the key delivery and quantum links between equipment. In accordance with ETSI GS QKD 008, the equipment is able to clearly indicate that it is operating in "approved mode" [26]. This is achieved with a provided SNMP Management Information Base (MIB) provided with the equipment. Incorporating these SNMP metrics and notifications into the existing dashboard used by the GÉANT OC will allow for proper monitoring of the equipment on the quantum layer of the QKDN. An example of the output by the SNMP interface is given in Table 12.

For example, when monitoring the QBER to detect eavesdropping attempts, this is to be detected by the QKD equipment itself. In accordance with ITU-T recommendation Y.3803, the equipment must inform either the KMs or the QKDN controller directly [62]. These alerts are to be monitored by the OC.

At the higher layers in the QKDN, monitoring requirements and capabilities will depend on the offered service. When encrypting Layer 2 traffic, it should be adequate to monitor the QKD equipment by making use of the aforementioned SNMP interface, and periodically sending `ping` requests to the associated control units to ensure that all QKD links are live. For the monitoring of the keys that are in use, the Infinera transponders will have to be monitored to make sure that the key rotation time is sufficiently low, and that they are able to fetch new keys from the adjacent QKD equipment in a PoP. For the QKDN solution that offers QKDaaS, more monitoring and logging information will have to be available to the GÉANT OC. E.g., key replenishment and request rates at the PoPs, and the logging key consumption by customers such that they can be throttled if needed. Monitoring software for the latter case would have to be developed, as this does not readily exist as an existing software product.

7.5 Feasibility with Toshiba Equipment

In order to gain insight into the feasibility of implementing QKD in the GÉANT network, a comparison is made between the experimental results from Table 11 and the data in the histogram from Figure 14. It was found that the equipment is able to sustain a level of attenuation of up to 23.5 dB when combined with a total launch power of +15 dBm for the present data wavelengths. Comparing this to the histogram, 23 dB of attenuation covers 36.3 % of the link spans in the GÉANT network.

If QKD were to be offered on the western ring only, as part of an initial deployment, 32.1 % of the links could be used instead. Figures 17 and 18 contains pair of histograms that display the expected attenuation for all link spans in the western ring, similar to the ones presented in Figures 13 and 14.

The outlier that is shown at 65 dB of attenuation is a submarine link between Amsterdam and London. It is unlikely that any QKD equipment will be able to bridge this attenuation any time in the next years. For this reason, to close the western ring other solutions such as satellite based QKD would need to be investigated, or the network is operated in a topology where the western ring is not closed. The latter requires forwarding of keys across multiple links, including for Layer 2 encryption service. Figure 16 shows a map of the western ring network, with links that have an attenuation of above 23 dB highlighted in red.

When the power of transmitted data channels is increased to +20 dBm, this would take the expected maximum level of attenuation that can be sustained by the QKD equipment down to approximately 22 dB. This results in 30.7 % of the link spans in the GÉANT network, or 22.6 % in the western ring only. For the remaining spans of fibre, this would require purchasing additional dark fibre, further driving the cost of the system up.

Part of the fibre spans have an attenuation in the range of 22 dB at 1310 nm and 23.5 dB at 1550 nm, in which it is expected that Toshiba's "long range" equipment from Section 2.2 is able to make use of the link if there are no data waves present. These link spans can be used if there is a separate dark fibre available, which are highlighted in orange. In Figures 13 and 17 these are represented by the area to the left of the orange vertical line. For the link spans highlighted in red, these would have to be redesigned which includes the construction of new amplifier stations as to shorten the distance and lower attenuation of the link spans.

Typically, in commercial optical networks an operational margin is added to services, such that external effects that take place over a longer period of time, such as ageing of the fibre, are expected to degrade the performance of offered services. Commonly 2 dB of margin is added to the sustained attenuation in order to help guarantee proper operation over a longer period of time. However, as no long-term studies have been performed yet on the operation of QKDN, the appropriate margin that should be allowed for is unknown. Figures 19 and 20 shows the percentage of link spans that can be covered, when different levels of margin are included in the expected level of attenuation for each link span.

A comparison can be made with the performance that is expected of QKD equipment produced by IDQuantique presented in Table 2, and the equipment from QNu Labs presented in [99]. According to the system specifications, the IDQuantique equipment is able to sustain a maximum of 18 dB of attenuation at which the SKR is below 2000 bps. This would be able to use 70.7 % of the link spans in the GÉANT network at 1550 nm. The QNu Labs equipment was found to be able to sustain 20.6 dB of

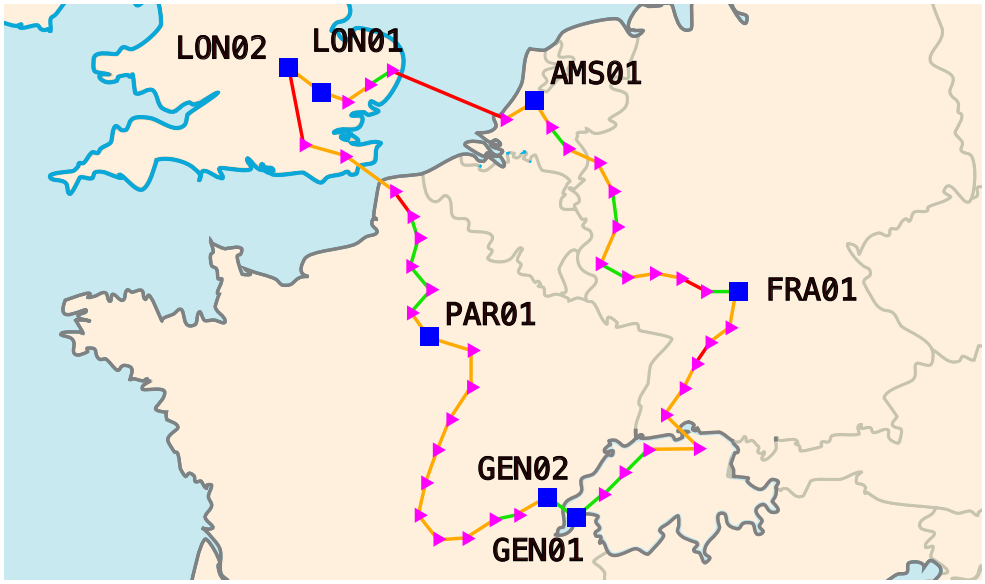


Fig. 16. Map of the western ring of the GÉANT optical network. Link spans highlighted in green have an expected attenuation below 20 dB at 1310 nm. Link spans highlighted in orange have an attenuation below 20 dB at 1550 nm. Link spans highlighted in red have an attenuation above 23 dB at 1550 nm and require alternative solutions. Blue squares are PoPs, magenta triangles amplifier stations. Adaptation of [106].

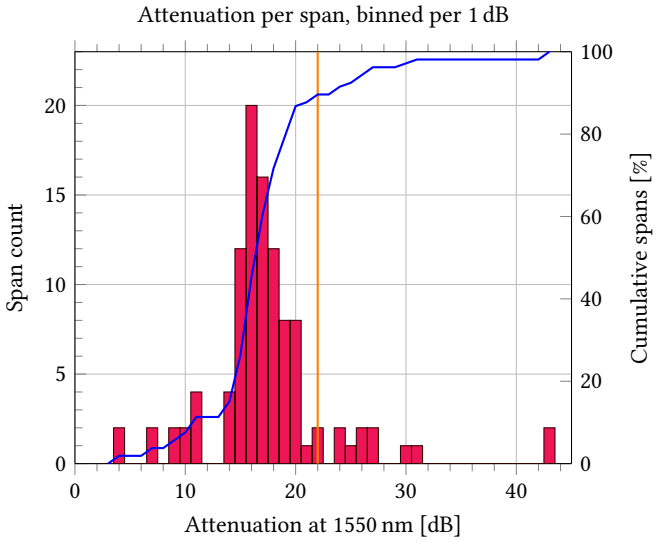


Fig. 17. Histogram of the amount of fibre spans in the western ring of the network, binned per 1 dB against attenuation of the link span at 1550 nm. On the left y-axis there is absolute span count which corresponds to the bar graph in red. On the right y-axis, the cumulative percentage of spans, marked with the blue line. The link spans left of the orange line can be used by long rage QKD equipment that operates in the C-band.

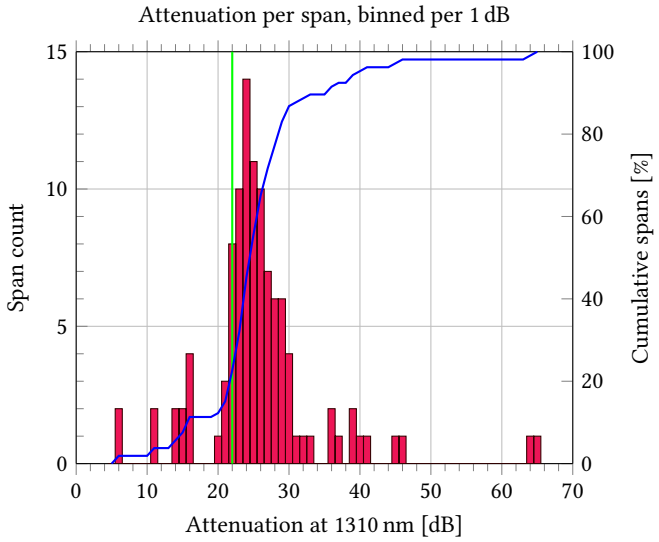


Fig. 18. Same as Figure 17, but with estimated attenuation at 1310 nm. On the link spans left of the green line, it is expected that quantum and data waves can be multiplexed on the same fibre.

attenuation, at a SKR of 5000 kbps, which includes 85.4 % of the link spans in the GÉANT network at 1550 nm [99]. This requires dedicated dark fibre links to be available for QKD traffic.

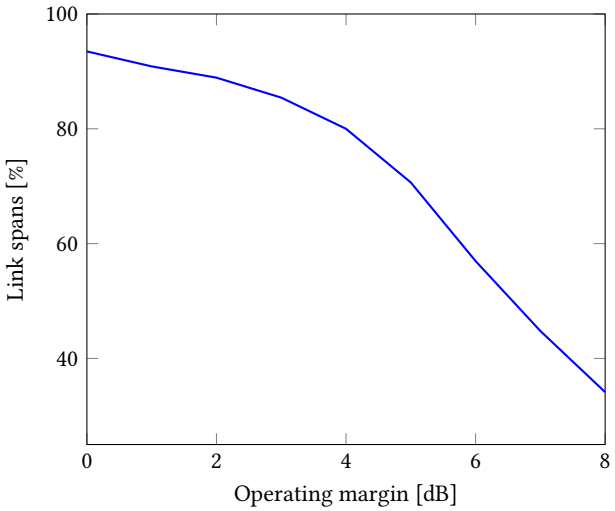


Fig. 19. Percentage of link spans that can be used at 1550 nm, depending on the amount of margin that is taken into account for attenuation. 0 dB of margin correlates to 23 dB of attenuation.

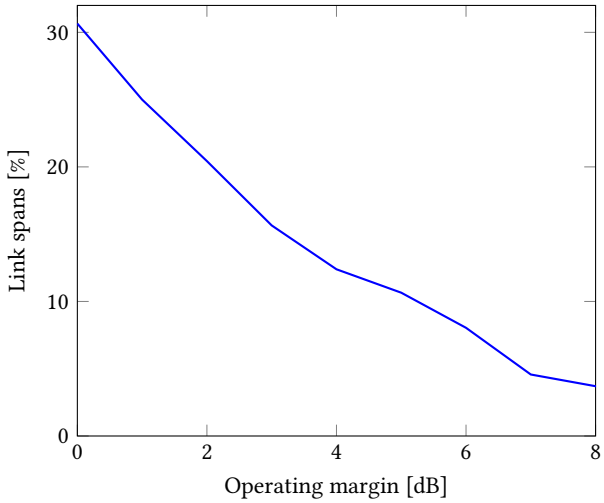


Fig. 20. Same as Figure 19, but at a wavelength of 1310 nm. 0 dB of margin correlates to 22 dB of attenuation.

8 CONCLUSIONS

This section gives an overview of the conclusions that are drawn in this research, which seek to answer the research questions presented in Section 1.4.

Research Question 1 addresses the two services that GÉANT could build in the network. Requirements for both of these services are presented in Section 7, specifically Section 7.1 lists the requirements for the implementation of functional QKD operation. Section 7.2 lists the hardware and software requirements for Layer 2 encryption specifically. It is found that the hardware required to build these services is at a high TRL. The test results presented in Section 6 show that the Toshiba QKD equipment tested performs as claimed. However, the equipment does not have a history of long-term deployment in a production environment, so there are little if any reported results on long-term performance, and specifically of the stability and reliability. A field trial is suggested to understand these long-term challenges.

As discussed in Section 7.1.2, software standards however are currently incomplete. As a result, much software support is still either proprietary or missing. No standardisation-compliant solution that can readily be integrated with the existing software stack in the GÉANT network exists for multiple layers of the architecture, including the QKDN controller, KMs, and QKDN manager.

GÉANT will need to update their existing monitoring system to be able to support the management framework presented in ITU-T recommendation Y.3804. This will typically require the integration of the existing proprietary QKD monitoring solutions with the operations database and dashboard systems of GÉANT. This is not likely to be a complex problem, however the lack of fully developed standards for monitoring a QKDN may hamper this integration. It is recommended to monitor the development of standards and how these are adopted by vendors.

For Research Question 4 on the expected performance of a QKD link in the GÉANT network, the quantitative study as described in Section 5 and its results in Section 6 seek to answer this question. Table 11 combined with Figures 13 and 14 serve to give insight into the expected performance of a QKD link in the GÉANT network. At a maximum sustained level of attenuation of 23.5 dB, we expect that around 36.3 % of the fibre spans in the network could be used at an expected SKR of approximately 1300 bps. This is highlighted in Figure 14 as the area on the left of the green line. Where a third optical fibre is purchased, it is expected that with the use of Toshiba long-range equipment presented in Table 1, it should be possible to cover approximately 90 % of the 230 total fibre spans in the GÉANT network. This is highlighted in Figure 13 as the area on the left of the orange line.

Section 6 shows that for the modelling of the performance of a QKD link, a VOA does not give a representable approximation of dark fibre, which answers Research Question 4a. SKR is found to decrease by approximately 93 %, and QBER to increase by approximately 46 % when using a fibre spool instead of a VOA.

GÉANT should continue to monitor the development of QKD systems, in particular software support in the optical transmission equipment and the maturing of standards. Also, it is expected that over time, the cost of QKD equipment will fall as more competition enters the market and the technology matures. Thie high cost of the current generation of QKD technology makes it difficult to make a good business case for a QKDaaS at this stage. It is also advisable to wait for the outcomes of these national efforts, and take a coordinating role in the development of QKD in Europe. It is also recommended for GÉANT to continue to cooperate with NRENs in Europe, in order to continuously keep up to date with developments in the evolution of standardisation and software solutions related to QKD.

The implementation of one or multiple QKD links in the GÉANT network as a pilot service is possible, however at this moment in time the expected benefits of the use-cases presented in Section 3 do not justify the expected cost that is associated with the implementation of a network-wide deployment. In the future, a two-phase approach is advisable, where first all Layer 2 traffic in (a part of) the GÉANT network is encrypted using QKD. Once this service is operational, QKDaaS could be offered at a later point in time in a QKDN, when required software becomes available and is suitable for a production environment. As the same hardware can be utilised for both of the services, this would introduce an incremental investment on chiefly familiarisation with newly available software for management of a QKDN.

Once a pilot QKD service is deployed in the GÉANT network for testing the long-term stability of such a system, it is highly advised to take the approach of multiplexing data and quantum key traffic onto a shared fibre. The use of a shared fibre medium for data and quantum key communication, if proven to work in a field trial, will decrease the implementation cost significantly, as no new dark fibre needs to be acquired at an estimated cost of €0.19 per metre per year. The results in Section 6 show that there is a difference in performance when both data and quantum key traffic are multiplexed, however, the difference in performance is at an acceptable level for the operation of QKD links. For the western ring alone this could save several million Euro in dark fibre capacity purchases over a period of ten years. However, this requires replacement of IRMs with IAMs along links, as an IRM is incompatible with QKD operation on a shared fibre. For the fibre spans that could currently not be used due to high attenuation, there are three possibilities for resolving this issue; re-design the system with shorter link spans that induce a lower level of attenuation, purchase dedicated dark fibre with shorter link spans, or to wait for the next generation of technology that is able to withstand such levels of attenuation.

In conclusion, considering the incomplete software standards for the maintenance and operation of a QKDN as presented in Section 4 as well as the challenges with retrofitting the required hardware into the

GÉANT network discussed in Section 7.1.3, the following actions are recommended:

- GÉANT should implement a trial QKD link in the GN5 project. This should aim to help understand how to resolve the incompatibility with IRMs as discussed in Section 7.1.3 and the issues regarding long-term reliability.
- GÉANT should work with Infinera to find a solution to the lack of a key exchange API on optical transmission equipment in the GÉANT network, as discussed in Section 7.2.
- GÉANT should work with its community to develop use cases and business cases. The business case will need to consider the high cost of the required equipment and fibre as discussed in Section 7.1.3.
- GÉANT should track the ongoing work in standardisation bodies as discussed in Sections 4.6 and 7.4.

9 DISCUSSION

In this research, it is found that software required for QKD in a production level environment that can readily cooperate with equipment from other vendors is not currently available to purchase. Currently available software solutions do not allow for interoperability between QKD and optical transmission equipment from different vendors in accordance with standardisation efforts presented in Section 4, as these do not form a set of formal industry standards yet. For the implementation of a service where Layer 2 traffic is encrypted standards are complete and implementation by vendors is underway. Hardware implementation is now at a high TRL, but due to the lack of standards, interoperability between vendors was not able to be demonstrated during testing.

What should remain an important aspect of future work, is to investigate the need for QKD in the GÉANT network, and from this develop use cases. Although the need for security is a given, it is nevertheless important to ask the question who would benefit from the efforts that are undertaken in quantum-proof cryptography. From these use cases, a business case will have to be built, which is difficult to justify at the time of writing due to the cost of current-generation QKD equipment being quite high. It is expected that the effect of economies of scale will bring average cost for equipment down in the future. For the offering of a QKDaaS greater experience is required for the management and monitoring of QKDNs, and the associated cost is too high at the time of writing. Such experience can be gained through the deployment of field trials. Commercial deployments exist where Toshiba equipment is used to create QKD services, however these are only at metropolitan scale, for example in London [7]. It is advisable to await results from early deployments and the ongoing research efforts undertaken by NRENs in order to gain more insight into what aspects are lacking in maturity. This includes relatively novel approaches to QKD, such as TF-QKD where GÉANT is currently investigating its performance.

This work has also shown the high value of the possibility to multiplex multiple wavelengths together onto the same shared fibre medium. The cost difference will form a large impact on the overall cost of a developed solution for the GÉANT network, as it helps prevent the need to purchase additional dark fibre for deployment. Another way of decreasing the initial cost is to implement QKD services in the western ring alone at first. This way, the cost of required equipment and potential dark fibre purchases goes down significantly. One link span that stands out is the submarine cable between Amsterdam and London, which has 43 dB of attenuation at 1550 nm. In order to be able to make use of quantum keys across this link with currently available QKD technology, it will be necessary to either relay keys across the rest of the network in order for them to be available at both ends of the link, or rely on another approach to transmitting quantum keys such as satellite-based QKD.

Regarding the performance of the tested equipment by Toshiba, it was found that performance is sufficient for deployment in most existing links in the GÉANT network, including both SKR and QBER. The QBER remained below 7 %. With a QBER below 25 % by such a large margin, it can be stated that the possibility of the presence of an eavesdropper is negligible. For the SKR, the desired performance of the system depends on the service that is to be offered. In the case of Layer 2 encryption, an SKR of only a single bit per second would already result in a satisfactory key rotation time where encryption keys are replaced multiple times per day. For QKDaaS however, this largely correlates with the expected demand at a node in the QKDN, something that will have to be investigated in future work.

Some of the link spans however, cannot be used with QKD services due to current hardware limitations on attenuation that can be sustained. Three possible approaches could be taken to mitigate this, as follows. Two methods exist for lowering the attenuation across a link span, one of which is to have shorter link spans by means of re-designing the system, the other being to purchase additional dark fibre capacity that consists of shorter link spans. The third approach is one of a broader nature, where it is advised to wait for next generation hardware that is either able to sustain higher degrees of attenuation, or an approach to QKD that does not suffer from the same issues as optical fibre does. For example free-space QKD by means of satellite communication could pose a solution to this problem.

In future work that addresses the topology of a QKDN, the network could be approached as a Steiner problem, modelling the network as a k-edge-connected Steiner network, where k indicates the degree of redundancy in the network [73]. For example, with a k of 3 the network remains fully connected if any two links are cut. Alléaume *et al.* have presented similar work, where they introduce formulae for calculating the cost of various topologies of a QKDN [5]. Introducing redundancy on the QKD links would help improve the overall stability and reliability of QKD services that are offered.

The fidelity of the performed tests could be improved in future work. For example, performance at higher degrees of attenuation are still somewhat unknown. Testing could be performed on higher levels of data power, with more granular increments in attenuation especially at the higher levels of attenuation in the range of 20 dB to 25 dB. Currently, the equipment from Toshiba that was tested is marketed to withstand up to 70 km of fibre. This would correlate to 28 dB of attenuation on a fibre where no auxiliary data channels are present, results which could not be achieved in the performed experiments. However, this is something that should be achievable in a realistic test setup.

Toshiba have indicated that a new version of their QKD equipment is available where the maximum level of attenuation that can be used is raised from 23 dB to an advertised 30 dB with the use of higher grade laser sources. This would allow for an estimated percentage of 86 % of the fibre links in the GÉANT network to be used for QKD at 1310 nm. A pilot service that makes use of this newer equipment would be the recommended course of action for further testing, as it will also allow for the investigation of long-term reliability and stability.

The fact that these tests were performed with test setups that relied on VOAs to induce at least part of the attenuation is to be taken into account with the presented performance results of the Toshiba equipment. Since the actual level of attenuation would have differed with the wavelengths at which data was transmitted. A VOA will affect both wavelengths equally, but dark fibre does not. Add to this the fact that it is found that a VOA does not make for a representable source of attenuation compared to dark fibre. Therefore in future work, building test setups that only incorporate dark fibre to induce attenuation could yield more reliable performance compared to a deployment in a production environment.

As has been shown in Section 4, standardisation is not yet at a level where production-grade equipment can (co-)operate adequately, with respect to both the interoperability of equipment itself, and the certification of verified secure operation of a QKD system. Once these standards are published, in particular concerning key delivery, QKDN management, and certification, future work could look at equipment that becomes available that adheres to these standards. Further strengthening the importance of performing a pilot service deployment, where this newly available equipment is tested.

ACKNOWLEDGMENTS

First and foremost, I want to thank Guy Roberts for all his support over the last ten months. From the very first on-boarding meetings at GÉANT until the very end where I relentlessly kept sending new draft versions of my thesis, you've always been kind enough to provide me with insightful feedback and show me the ropes in the organisation. I also want to thank my academic supervisor Pieter-Tjerk de Boer, for the continued support throughout the process of performing my research. I also want to thank Lee Johnson and Andrew Shields for all their support with the Toshiba equipment. And finally, I want to thank all my colleagues at GÉANT, everyone in WP6 for their feedback, and my friends and family for their continued support during my research.

REFERENCES

[1] [n. d.]. ISO - About us. https://www.iso.org/about-us.html

[2] Govind P. Agrawal. 2006. CHAPTER 9 - Fiber Optic Raman Amplifiers. In *Guided Wave Optical Components and Devices*, Bishnu P. Pal (Ed.). Academic Press, Burlington, 131–153. https://doi.org/10.1016/B978-012088481-0/50010-3

[3] Obada Alia, Rodrigo Stange Tessinari, Emilio Hugues-Salas, George T. Kanellos, Reza Nejabati, and Dimitra Simeonidou. 2022. Dynamic DV-QKD Networking in Fully-Meshed Software-Defined Optical Networks. http://arxiv.org/abs/2108.11145 arXiv:2108.11145 [quant-ph].

[4] Claudio Allochio, Mauro Campanella, Tim Chown, Ivana Golub, Xavier Jeannin, Frédéric Loui, Jani Myyry, Damian Parniewicz, Lefteris Poulakakis, Edin Salguero, Nicolas Quintin, Piotr Rydlichowski, Marco Savi, Tomasz Szewczyk, and Maxime Wisslé. 2020. Network Technology Evolution Report. (March 2020), 39.

[5] R Alléaume, F Roueff, E Diamanti, and N Lütkenhaus. 2009. Topological optimization of quantum key distribution networks. *New Journal of Physics* 11, 7 (July 2009), 075002. https://doi.org/10.1088/1367-2630/11/7/075002

[6] Arash Bahrami, Andrew Lord, and Timothy Spiller. 2020. Quantum key distribution integration with optical dense wavelength division multiplexing: a review. *IET Quantum Communication* 1, 1 (July 2020), 9–15. https://doi.org/10.1049/iet-qtc.2019.0005

[7] Annabel Banks. 2022. BT and Toshiba launch first commercial trial of quantum secured communication services. https://www.ey.com/en_uk/news/2022/04/bt-and-toshiba-launch-first-commercial-trial-of-quantum-secured-communication-services

[8] Charles H. Bennett and Gilles Brassard. 2014. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science* 560 (Dec. 2014), 7–11. https://doi.org/10.1016/j.tcs.2014.05.025

[9] Charles H Bennett, Gilles Brassard, and N David Mermin. 1992. Quantum cryptography without Bell's theorem. *Physical review letters* 68, 5 (1992), 557.

[10] Nina Bindel, Jacqueline Brendel, Marc Fischlin, Brian Goncalves, and Douglas Stebila. 2019. Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange. In *Post-Quantum Cryptography*, Jintai Ding and Rainer Steinwandt (Eds.). Vol. 11505. Springer International Publishing, Cham, 206–226. https://doi.org/10.1007/978-3-030-25510-7_12 Series Title: Lecture Notes in Computer Science.

[11] Matthias Bock, Andreas Lenhard, Christopher Chunnilall, and Christoph Becher. 2016. Highly efficient heralded single-photon source for telecom wavelengths based on a PPLN waveguide. *Optics Express* 24, 21 (Oct. 2016), 23992–24001. https://doi.org/10.1364/OE.24.023992 Publisher: Optica Publishing Group.

[12] G Brassard and Charles H Bennett. 1984. Quantum cryptography: Public key distribution and coin tossing. In *International conference on computers, systems and signal processing*.

[13] Yuan Cao, Yongli Zhao, Qin Wang, Jie Zhang, Soon Xin Ng, and Lajos Hanzo. 2022. The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet. *IEEE Communications Surveys & Tutorials* (2022), 1–1. https://doi.org/10.1109/COMST.2022.3144219

[14] T E Chapuran, P Toliver, N A Peters, J Jackel, M S Goodman, R J Runser, S R McNown, N Dallmann, R J Hughes, K P McCabe, J E Nordholt, C G Peterson, K T Tyagi, L Mercer, and H Dardy. 2009. Optical networking for quantum key distribution and quantum communications. *New Journal of Physics* 11, 10 (Oct. 2009), 105001. https://doi.org/10.1088/1367-2630/11/10/105001

[15] Jiu-Peng Chen, Chi Zhang, Yang Liu, Cong Jiang, Weijun Zhang, Xiao-Long Hu, Jian-Yu Guan, Zong-Wen Yu, Hai Xu, Jin Lin, Ming-Jun Li, Hao Chen, Hao Li, Lixing You, Zhen Wang, Xiang-Bin Wang, Qiang Zhang, and Jian-Wei Pan. 2020. Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution Over 509 km. *Physical Review Letters* 124, 7 (Feb. 2020), 070501. https://doi.org/10.1103/PhysRevLett.124.070501 arXiv: 1910.07823.

[16] Teng-Yun Chen, Xiao Jiang, Shi-Biao Tang, Lei Zhou, Xiao Yuan, Hongyi Zhou, Jian Wang, Yang Liu, Luo-Kan Chen, Wei-Yue Liu, Hong-Fei Zhang, Ke Cui, Hao Liang, Xiao-Gang Li, Yingqiu Mao, Liu-Jun Wang, Si-Bo Feng, Qing Chen, Qiang Zhang, Li Li, Nai-Le Liu, Cheng-Zhi Peng, Xiongfeng Ma, Yong Zhao, and Jian-Wei Pan. 2021. Implementation of a 46-node quantum metropolitan area network. *npj Quantum Information* 7, 1 (Sept. 2021), 1–6. https://doi.org/10.1038/s41534-021-00474-3 Number: 1 Publisher: Nature Publishing Group.

[17] Teng-Yun Chen, Jian Wang, Hao Liang, Wei-Yue Liu, Yang Liu, Xiao Jiang, Yuan Wang, Xu Wan, Wei-Qi Cai, Lei Ju, Luo-Kan Chen, Liu-Jun Wang, Yuan Gao, Kai Chen, Cheng-Zhi Peng, Zeng-Bing Chen, and Jian-Wei Pan. 2010. Metropolitan all-pass and inter-city quantum communication network. *Optics Express* 18, 26 (Dec. 2010), 27217. https://doi.org/10.1364/OE.18.027217 arXiv: 1008.1508.

[18] CiViQ [n. d.]. CIVIQ – CIVIQ. https://civiquantum.eu/

[19] Sabine Dahmen-Lhuissier. [n. d.]. ETSI - Our group on Quantum Key Distribution for Users (QKD). https://www.etsi.org/committee/1430-qkd

[20] Sabine Dahmen-Lhuissier. [n. d.]. ETSI - Standards, mission, vision, direct member participation. https://www.etsi.org/about

[21] James Dargan. 2021. Top 25 Quantum Cryptography & Encryption Companies [2022]. https://thequantuminsider.com/2021/01/11/25-companies-building-the-quantum-cryptography-communications-markets/

[22] Christopher C. Davis. 2000. FIBER OPTIC TECHNOLOGY AND ITS ROLE IN THE INFORMATION REVOLUTION. https://user.eng.umd.edu/~davis/optfib.html

[23] DIGITAL-2021-QCI-01-DEPLOY-NATIONAL [n. d.]. Funding & tenders. https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-2021-qci-01-deploy-national

[24] DIGITAL-2021-QCI-01-EUROQCI-QKD [n. d.]. Funding & tenders. https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-2021-qci-01-euroqci-qkd

[25] Mohamed Elboukhari, Mostafa Azizi, and Abdelmalek Azizi. 2010. Quantum Key Distribution Protocols: A Survey. *International Journal of Universal Computer Science* 1, 2 (2010), 9.

[26] ETSI. 2010. *Quantum Key Distribution (QKD); QKD Module Security Specification.* ETSI GS QKD 008 v1.1.1. European Telecommunications Standards Institute, Sophia Antipolis, France.

[27] ETSI. 2010. *Quantum Key Distribution (QKD); Security Proofs.* ETSI GS QKD 005 v1.1.1. European Telecommunications Standards Institute, Sophia Antipolis, France.

[28] ETSI. 2010. *Quantum Key Distribution; Use Cases.* ETSI GS QKD 002 v1.1.1. European Telecommunications Standards Institute, Sophia Antipolis, France.

[29] ETSI. 2016. *Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems.* ETSI GS QKD 011 v1.1.1. European Telecommunications Standards Institute, Sophia Antipolis, France.

[30] ETSI. 2018. *Quantum Key Distribution (QKD); Components and Internal Interfaces.* ETSI GS QKD 003 v2.1.1. European Telecommunications Standards Institute, Sophia Antipolis, France.

[31] ETSI. 2018. *Quantum Key Distribution (QKD); Vocabulary.* ETSI GS QKD 007 v1.1.1. European Telecommunications Standards Institute, Sophia Antipolis, France.

[32] ETSI. 2019. *Quantum Key Distribution (QKD); Device and Communication Channel Parameters for QKD Deployment.* ETSI GS QKD 012 v1.1.1. European Telecommunications Standards Institute, Sophia Antipolis, France.

[33] ETSI. 2019. *Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API.* ETSI GS QKD 014 v1.1.1. European Telecommunications Standards Institute, Sophia Antipolis, France.

[34] ETSI. 2020. *Quantum Key Distribution (QKD); Application Interface.* ETSI GS QKD 004 v2.1.1. European Telecommunications Standards Institute, Sophia Antipolis, France.

[35] ETSI. 2022. *Quantum Key Distribution (QKD); Control Interface for Software Defined Networks.* ETSI GS QKD 015 v2.1.1. European Telecommunications Standards Institute, Sophia Antipolis, France.

[36] ETSI. 2022. *Quantum Key Distribution (QKD); Orchestration Interface for Software Defined Networks.* ETSI GS QKD 018 v1.1.1. European Telecommunications Standards Institute, Sophia Antipolis, France.

[37] EuroHPC [n. d.]. The European High Performance Computing Joint Undertaking (EuroHPC JU). https://eurohpc-ju.europa.eu/index_en

[38] EuroQCI [n. d.]. The European Quantum Communication Infrastructure (EuroQCI) Initiative | Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

[39] Federico Giacon, Felix Heuer, and Bertram Poettering. 2018. KEM combiners. In *IACR International Workshop on Public Key Cryptography*. Springer, 190–218.

[40] GÉANT 2021. GÉANT Services. https://geant.org/services/

[41] Mart Haitjema. 2007. A survey of the prominent quantum key distribution protocols. *Access Link: https://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum* (Dec. 2007).

[42] ID Quantique 2022. Products. https://www.idquantique.com/quantum-safe-security/products/

[43] Kyo Inoue. 2015. Differential Phase-Shift Quantum Key Distribution Systems. *IEEE Journal of Selected Topics in Quantum Electronics* 21, 3 (May 2015), 109–115. https://doi.org/10.1109/JSTQE.2014.2360362

[44] Kyo Inoue and Toshimori Honjo. 2005. Robustness of differential-phase-shift quantum key distribution against photon-number-splitting attack. *Physical Review A* 71, 4 (April 2005), 042305. https://doi.org/10.1103/PhysRevA.71.042305

[45] K. Inoue, E. Waks, and Y. Yamamoto. 2003. Differential-phase-shift quantum key distribution using coherent light. *Physical Review A* 68, 2 (Aug. 2003), 022317. https://doi.org/10.1103/PhysRevA.68.022317

[46] ITU [n. d.]. ITU-T Recommendations. https://www.itu.int/en/ITU-T/publications/Pages/recs.aspx

[47] ITU [n. d.]. Study Group 13 at a glance. https://www.itu.int/en/ITU-T/about/groups/Pages/sg13.aspx

[48] ITU [n. d.]. Study Group 17 at a glance. https://www.itu.int/en/ITU-T/about/groups/Pages/sg17.aspx

[49] ITU-T. [n. d.]. *ISO/IEC DIS 23837-1(en), Information technology security techniques — Security requirements, test and evaluation methods for quantum key distribution — Part 1: Requirements.* ISO/IEC DIS 23837-1. International Organization for Standardization, Geneva, Switzerland.

[50] ITU-T. [n. d.]. *ISO/IEC DIS 23837-2(en), Information technology security techniques — Security requirements, test and evaluation methods for quantum key distribution — Part 2: Evaluation and testing methods.* ISO/IEC DIS 23837-2. International Organization for Standardization, Geneva, Switzerland.

[51] ITU-T. 2000. *TMN management functions.* ITU-T M.3400 – Edition 3. Telecommunication Standardization Sector of ITU, Geneva, Switzerland.

[52] ITU-T. 2006. *Security Assertion Markup Language.* ITU-T X.1141. Telecommunication Standardization Sector of ITU, Geneva, Switzerland.

[53] ITU-T. 2007. *Security requirements for NGN release 1.* ITU-T Y.2701. Telecommunication Standardization Sector of ITU, Geneva, Switzerland.

[54] ITU-T. 2009. *Characteristics of a single-mode optical fibre and cable.* ITU-T G.652. Telecommunication Standardization Sector of ITU, Geneva, Switzerland.

[55] ITU-T. 2017. *IMT-2020 network management and orchestration framework.* ITU-T Y.3111. Telecommunication Standardization Sector of ITU, Geneva, Switzerland.

[56] ITU-T. 2018. *Requirements of the IMT-2020 network.* ITU-T Y.3101 – Cor. 1. Telecommunication Standardization Sector of ITU, Geneva, Switzerland.

[57] ITU-T. 2019. *Overview on networks supporting quantum key distribution.* ITU-T Y.3800 Corrigendum 1. Telecommunication Standardization Sector of ITU, Geneva, Switzerland.

[58] ITU-T. 2019. *Quantum noise random number generator architecture.* ITU-T X.1702. Telecommunication Standardization Sector of ITU, Geneva, Switzerland.

[59] ITU-T. 2020. *Functional requirements for quantum key distribution networks.* ITU-T Y.3801. Telecommunication Standardization Sector of ITU, Geneva, Switzerland.

[60] ITU-T. 2020. *Key combination and confidential key supply for quantum key distribution networks.* ITU-T X.1714. Telecommunication Standardization Sector of ITU, Geneva, Switzerland.

[61] ITU-T. 2020. *Quantum key distribution networks – Control and management.* ITU-T Y.3804. Telecommunication Standardization Sector of ITU, Geneva, Switzerland.

[62] ITU-T. 2020. *Quantum key distribution networks – Key management.* ITU-T Y.3803. Telecommunication Standardization Sector of ITU, Geneva, Switzerland.

[63] ITU-T. 2020. *Security framework for quantum key distribution networks.* ITU-T X.1710. Telecommunication Standardization Sector of ITU, Geneva, Switzerland.

[64] ITU-T. 2021. *The Directory – Authentication framework.* ITU-T X.509 v9.1 – Cor. 1. Telecommunication Standardization Sector of ITU, Geneva, Switzerland.

[65] ITU-T. 2021. *Quantum key distribution networks – Functional architecture.* ITU-T Y.3802 Corrigendum 1. Telecommunication Standardization Sector of ITU, Geneva, Switzerland.

[66] ITU-T. 2021. *Quantum key distribution networks – Requirements for quality of service assurance.* ITU-T Y.3806. Telecommunication Standardization Sector of ITU, Geneva, Switzerland.

[67] ITU-T. 2021. *Quantum key distribution networks – Software-defined networking control.* ITU-T Y.3805. Telecommunication Standardization Sector of ITU, Geneva, Switzerland.

[68] ITU-T. 2022. *Framework for integration of quantum key distribution network and secure storage network.* ITU-T Y.3808. Telecommunication Standardization Sector of ITU, Geneva, Switzerland.

[69] ITU-T. 2022. *Quantum key distribution networks – Quality of service parameters.* ITU-T Y.3807. Telecommunication Standardization Sector of ITU, Geneva, Switzerland.

[70] ITU-T. 2022. *A role-based model in quantum key distribution networks deployment.* ITU-T Y.3809. Telecommunication Standardization Sector of ITU, Geneva, Switzerland.

[71] ITU-T. 2022. *Security framework for quantum key distribution networks – key management.* ITU-T X.1712 – Cor. 1. Telecommunication Standardization Sector of ITU, Geneva, Switzerland.

[72] ITU-T. 2022. *Security requirements and measures for integration of quantum key distribution network and secure storage network.* ITU-T X.1715. Telecommunication Standardization Sector of ITU, Geneva, Switzerland.

[73] Tibor Jordán. 2003. On minimally k-edge-connected graphs and shortest k-edge-connected Steiner networks. *Discrete Applied Mathematics* 131, 2 (Sept. 2003), 421–432. https://doi.org/10.1016/S0166-218X(02)00465-1

[74] David Joseph, Rafael Misoczki, Marc Manzano, Joe Tricot, Fernando Dominguez Pinuaga, Olivier Lacombe, Stefan Leichenauer, Jack Hidary, Phil Venables, and Royal Hansen. 2022. Transitioning organizations to post-quantum cryptography. *Nature* 605, 7909 (May 2022), 237–243. https://doi.org/10.1038/s41586-022-04623-2 Number: 7909 Publisher: Nature Publishing Group.

[75] Ahmed I. Khaleel. 2012. Coherent one-way protocol: Design and simulation. In *2012 International Conference on Future Communication Networks*. 170–174. https://doi.org/10.1109/ICFCN.2012.6206863

[76] Evgeny Kiktenko, Anton Trushechkin, Yury Kurochkin, and Aleksey Fedorov. 2016. Post-processing procedure for industrial quantum key distribution systems. *Journal of Physics: Conference Series* 741 (Aug. 2016), 012081. https://doi.org/10.1088/1742-6596/741/1/012081

[77] D. Lancho, J. Martinez, D. Elkouss, M. Soto, and V. Martin. 2010. QKD in Standard Optical Telecommunications Networks. *arXiv:1006.1858 [quant-ph]* 36 (2010), 142–149. https://doi.org/10.1007/978-3-642-11731-2_18 arXiv: 1006.1858.

[78] Yang Liu, Zong-Wen Yu, Weijun Zhang, Jian-Yu Guan, Jiu-Peng Chen, Chi Zhang, Xiao-Long Hu, Hao Li, Cong Jiang, Jin Lin, Teng-Yun Chen, Lixing You, Zhen Wang, Xiang-Bin Wang, Qiang Zhang, and Jian-Wei Pan. 2019. Experimental Twin-Field Quantum Key Distribution Through Sending-or-Not-Sending. *Physical Review Letters* 123, 10 (Sept. 2019), 100505. https://doi.org/10.1103/PhysRevLett.123.100505 arXiv: 1902.06268.

[79] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. 2005. Decoy State Quantum Key Distribution. *Phys. Rev. Lett.* 94 (Jun 2005), 230504. Issue 23. https://doi.org/10.1103/PhysRevLett.94.230504

[80] Marius Loeffler, Christian Goroncy, Thomas Länger, Andreas Poppe, Alexander Neumann, Matthieu Legré, Imran Khan, Christopher Chunnilall, Diego López, Marco Lucamarini, Andrew Shields, Elisabetta Spigone, Martin Ward, and Vicente Martin. 2020. Current Standardisation Landscape and existing Gaps in the Area of Quantum Key Distribution. (Dec. 2020), 31.

[81] W. H. Louisell, A. Yariv, and A. E. Siegman. 1961. Quantum Fluctuations and Noise in Parametric Processes. I. *Physical Review* 124, 6 (Dec. 1961), 1646–1654. https://doi.org/10.1103/PhysRev.124.1646 Publisher: American Physical Society.

[82] M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields. 2013. Efficient decoy-state quantum key distribution with quantified security. *Optics Express* 21, 21 (Oct. 2013), 24550. https://doi.org/10.1364/OE.21.024550

[83] Marco Lucamarini, Zhiliang Yuan, James F. Dynes, and Andrew J. Shields. 2018. Overcoming the rate-distance barrier of quantum key distribution without using quantum repeaters. *Nature* 557, 7705 (May 2018), 400–403. https://doi.org/10.1038/s41586-018-0066-6 arXiv: 1811.06826.

[84] MagiQ Technologies [n. d.]. MagiQ QPN™| Network Security | Somerville, MA. https://www.magiqtech.com/solutions/network-security/

[85] Ivan Marcikic, Hugues de Riedmatten, Wolfgang Tittel, Valerio Scarani, Hugo Zbinden, and Nicolas Gisin. 2002. Femtosecond Time-Bin Entangled Qubits for Quantum

Communication. *Physical Review A* 66, 6 (Dec. 2002), 062308. https://doi.org/10.1103/PhysRevA.66.062308 arXiv:quant-ph/0205144.

[86] Oliver Maurhart. 2016. AIT QKD R10 Software. https://github.com/axdhill/ait-qkd original-date: 2016-09-19T16:39:17Z.

[87] Abdul Mirza and Francesco Petruccione. 2010. Realizing long-term quantum cryptography. *Journal of the Optical Society of America B* 27, 6 (June 2010), A185. https://doi.org/10.1364/JOSAB.27.00A185

[88] Ali Ibnun Nurhadi and Nana Rachmana Syambas. 2018. Quantum Key Distribution (QKD) Protocols: A Survey. In *2018 4th International Conference on Wireless and Telematics (ICWT)*. 1–5. https://doi.org/10.1109/ICWT.2018.8527822

[89] OpenQKD [n. d.]. Home - OpenQKD. https://openqkd.eu/

[90] K. A. Patel, J. F. Dynes, M. Lucamarini, I. Choi, A. W. Sharpe, Z. L. Yuan, R. V. Penty, and A. J. Shields. 2014. Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks. *Applied Physics Letters* 104, 5 (Feb. 2014), 051123. https://doi.org/10.1063/1.4864398

[91] M Peev, C Pacher, R Alléaume, C Barreiro, J Bouda, W Boxleitner, T Debuisschert, E Diamanti, M Dianati, J F Dynes, S Fasel, S Fossier, M Fürst, J-D Gautier, O Gay, N Gisin, P Grangier, A Happe, Y Hasani, M Hentschel, H Hübel, G Humer, T Länger, M Legré, R Lieger, J Lodewyck, T Lorünser, N Lütkenhaus, A Marhold, T Matyus, O Maurhart, L Monat, S Nauerth, J-B Page, A Poppe, E Querasser, G Ribordy, S Robyr, L Salvail, A W Sharpe, A J Shields, D Stucki, M Suda, C Tamas, T Themel, R T Thew, Y Thoma, A Treiber, P Trinkler, R Tualle-Brouri, F Vannel, N Walenta, H Weier, H Weinfurter, I Wimberger, Z L Yuan, H Zbinden, and A Zeilinger. 2009. The SECOQC quantum key distribution network in Vienna. *New Journal of Physics* 11, 7 (July 2009), 075001. https://doi.org/10.1088/1367-2630/11/7/075001

[92] PICMG 2003. PICMG | AdvancedTCA. https://www.picmg.org/openstandards/advancedtca/

[93] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden. 2020. Advances in Quantum Cryptography. *Advances in Optics and Photonics* 12, 4 (Dec. 2020), 1012. https://doi.org/10.1364/AOP.361502 arXiv: 1906.01645.

[94] QNu Labs [n. d.]. How Quantum Key Distribution (QKD) works? - Armos. https://www.qnulabs.com/armos-quantum-key-distribution/

[95] QuantumXC 2019. Quantum-Safe Encryption | Phio TX. https://quantumxc.com/phio-tx/

[96] Quapital [n. d.]. Quapital Home. https://quapital.eu/

[97] QuintessenceLabs 2021. Quantum Entropy Enhancer. https://www.quintessencelabs.com/products/quantum-key-distribution-qkd/

[98] Martin Roetteler, Michael Naehrig, Krysta M. Svore, and Kristin Lauter. 2017. Quantum resource estimates for computing elliptic curve discrete logarithms. https://doi.org/10.48550/arXiv.1706.06752 arXiv:1706.06752 [quant-ph].

[99] Piotr Rydlichowski. 2022. *Report from QNULabs Armos - Quantum Key Distribution (QKD) system tests in PSNC laboratory.* Technical Report. 39 pages.

[100] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger. 2011. Field test of quantum key distribution in the Tokyo QKD Network. *Optics Express* 19, 11 (May 2011), 10387. https://doi.org/10.1364/OE.19.010387

[101] Valerio Scarani, Antonio Acin, Grégoire Ribordy, and Nicolas Gisin. 2004. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical review letters* 92, 5 (2004), 057901.

[102] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. 2009. The security of practical quantum key distribution. *Reviews of Modern Physics* 81, 3 (Sept. 2009), 1301–1350. https://doi.org/10.1103/RevModPhys.81.1301 Publisher: American Physical Society.

[103] Gautam Shaw, Shyam Sridharan, Shashank Ranu, Foram Shingala, Prabha Mandayam, and Anil Prabhakar. 2020. Equivalence of space and time-bins in DPS-QKD. https://doi.org/10.48550/arXiv.2008.03083 arXiv:2008.03083 [quant-ph].

[104] P.W. Shor. 1994. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 124–134. https://doi.org/10.1109/SFCS.1994.365700

[105] Hitesh Singh, D.L. Gupta, and A.K Singh. 2014. Quantum Key Distribution Protocols: A Review. *IOSR Journal of Computer Engineering* 16, 2 (2014), 01–09. https://doi.org/10.9790/0661-162110109

[106] Ssolbergj. 2007. Map of the Member States of the European Union. https://upload.wikimedia.org/wikipedia/commons/d/df/EU_map_brown.svg Published under CC BY-SA 3.0 license.

[107] Damien Stucki, Sylvain Fasel, Nicolas Gisin, Yann Thoma, and Hugo Zbinden. 2007. Coherent one-way quantum key distribution, Ivan Prochazka, Alan L. Migdall, Alexandre Pauchard, Miloslav Dusek, Mark S. Hillery, and Wolfgang P. Schleich (Eds.). Prague, Czech Republic, 65830L. https://doi.org/10.1117/12.722952

[108] D Stucki, M Legré, F Buntschu, B Clausen, N Felber, N Gisin, L Henzen, P Junod, G Litzistorf, P Monbaron, L Monat, J-B Page, D Perroud, G Ribordy, A Rochas, S Robyr, J Tavares, R Thew, P Trinkler, S Ventura, R Voirol, N Walenta, and H Zbinden. 2011. Long-term performance of the SwissQuantum quantum key distribution network in a field environment. *New Journal of Physics* 13, 12 (Dec. 2011), 123001. https://doi.org/10.1088/1367-2630/13/12/123001

[109] R. S. Tessinari, E. Arabul, O. Alia, A. S. Muqaddas, G. T. Kanellos, R. Nejabati, and D. Simeonidou. 2021. Demonstration of a Dynamic QKD Network Control Using a QKD-Aware SDN Application Over a Programmable Hardware Encryptor. In *Optical Fiber Communication Conference (OFC) 2021 (2021), paper M2B.3*. Optica Publishing Group, M2B.3. https://doi.org/10.1364/OFC.2021.M2B.3

[110] K. Thyagarajan. 2006. CHAPTER 8 - Erbium-Doped Fiber Amplifiers. In *Guided Wave Optical Components and Devices*, Bishnu P. Pal (Ed.). Academic Press, Burlington, 119–129. https://doi.org/10.1016/B978-012088481-0/50009-7

[111] Toshiba 2022. Products | Quantum Key Distribution | TOSHIBA DIGITAL SOLUTIONS CORPORATION. https://www.global.toshiba/ww/products-solutions/security-ict/qkd/products.html

[112] N Walenta, A Burg, D Caselunghe, J Constantin, N Gisin, O Guinnard, R Houlmann, P Junod, B Korzh, N Kulesza, M Legré, C W Lim, T Lunghi, L Monat, C Portmann, M Soucarros, R T Thew, P Trinkler, G Trolliet, F Vannel, and H Zbinden. 2014. A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing. *New Journal of Physics* 16, 1 (Jan. 2014), 013047. https://doi.org/10.1088/1367-2630/16/1/013047

[113] Liu-Jun Wang, Luo-Kan Chen, Lei Ju, Mu-Lan Xu, Yong Zhao, Kai Chen, Zeng-Bing Chen, Teng-Yun Chen, and Jian-Wei Pan. 2015. Experimental multiplexing of quantum key distribution with classical optical communication. *Applied Physics Letters* 106, 8 (Feb. 2015), 081108. https://doi.org/10.1063/1.4913483

[114] Liu-Jun Wang, Kai-Heng Zou, Wei Sun, Yingqiu Mao, Yi-Xiao Zhu, Hua-Lei Yin, Qing Chen, Yong Zhao, Fan Zhang, Teng-Yun Chen, and Jian-Wei Pan. 2017. Long-distance copropagation of quantum key distribution and terabit classical optical data channels. *Physical Review A* 95, 1 (Jan. 2017), 012301. https://doi.org/10.1103/PhysRevA.95.012301

[115] Shuang Wang, Wei Chen, Zhen-Qiang Yin, Yang Zhang, Tao Zhang, Hong-Wei Li, Fang-Xing Xu, Zheng Zhou, Yang Yang, Da-Jun Huang, Li-Jun Zhang, Fang-Yi Li, Dong Liu, Yong-Gang Wang, Guang-Can Guo, and Zheng-Fu Han. 2010. Field test of wavelength-saving quantum key distribution network. *Optics Letters* 35, 14 (July 2010), 2454. https://doi.org/10.1364/OL.35.002454

[116] Xiang-Bin Wang. 2005. A decoy-state protocol for quantum cryptography with 4 intensities of coherent states. *Physical Review A* 72, 1 (July 2005), 012322. https://doi.org/10.1103/PhysRevA.72.012322 arXiv: quant-ph/0411047.

[117] William K. Wootters and Wojciech H. Zurek. 2009. The no-cloning theorem. *Physics Today* 62, 2 (Feb. 2009), 76–77. https://doi.org/10.1063/1.3086114

[118] Z. L. Yuan and A. J. Shields. 2005. Continuous operation of a one-way quantum key distribution system over installed telecom fibre. *Optics Express* 13, 2 (2005), 660. https://doi.org/10.1364/OPEX.13.000660 arXiv: quant-ph/0501160.

A OPTICAL SPECTRUM WITH AND WITHOUT OSC

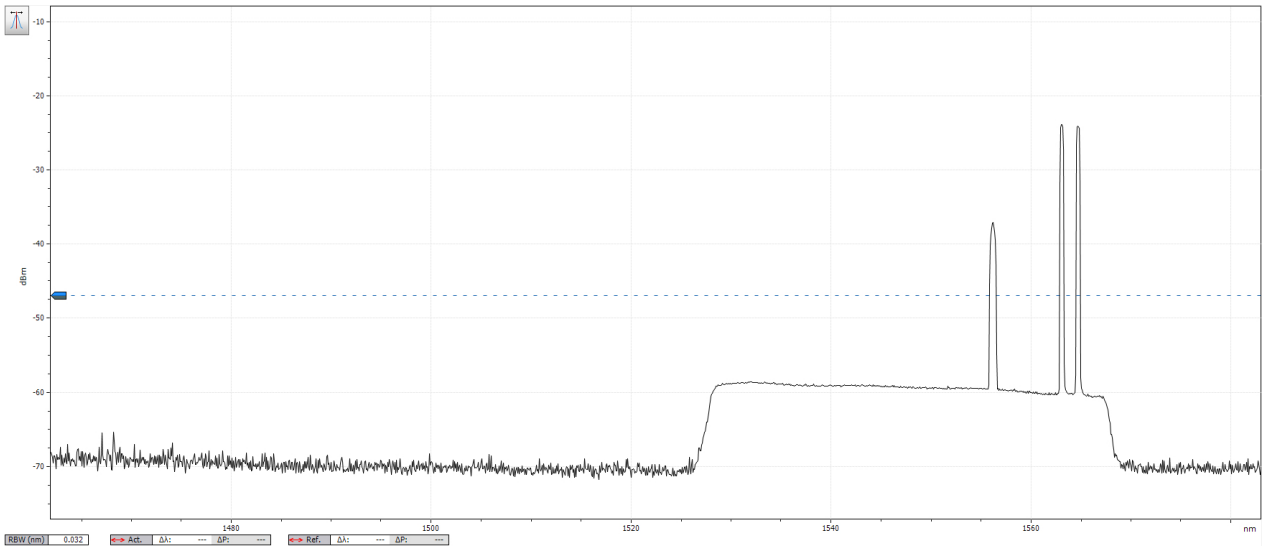


Fig. A-1. Graph that displays the optical wavelengths emitted, no OSC is emitted outside the C-band.

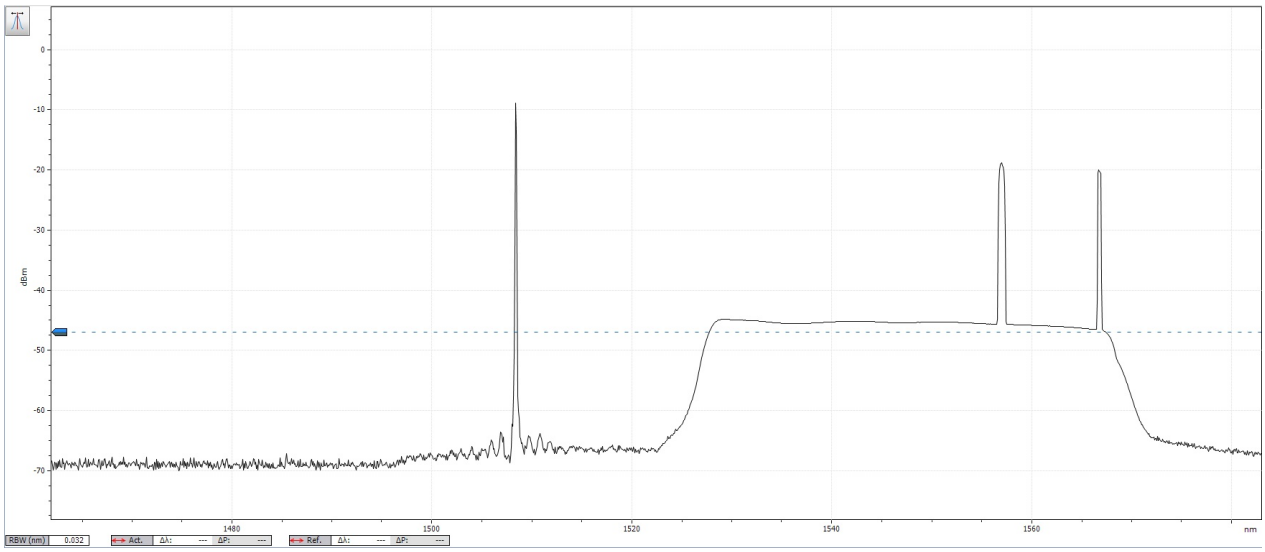


Fig. A-2. Graph that displays the optical wavelengths emitted, note the OSC emitted outside the C-band.

B DATA FROM TOSHIBA EQUIPMENT

The following tables all contain the ten data points output by the Toshiba system, that were used for calculating the average values in Section 6.

B.1 Fixed Attenuators

Data points from the test setup when only using fixed attenuators.

Date	Time	QBER	SKR (bps)
2022-06-23	10:45:11	3.3200 %	973 000
2022-06-23	10:45:33	3.2900 %	1 013 000
2022-06-23	10:45:55	3.1700 %	1 017 000
2022-06-23	10:46:17	3.2700 %	1 019 000
2022-06-23	10:46:39	3.2100 %	1 042 000
2022-06-23	10:47:01	3.2500 %	1 033 000
2022-06-23	10:47:24	3.2400 %	1 013 000
2022-06-23	10:47:46	3.1900 %	1 037 000
2022-06-23	10:48:09	3.2400 %	968 000
2022-06-23	10:48:30	3.2600 %	1 091 000

Table B.1-1. Using fixed attenuators of 10 dB.

B.2 VOAs Only

Data points from the test setup when only using VOAs for inducing attenuation.

Date	Time	QBER	SKR (bps)
2022-05-25	10:19:04	3.3600 %	2 536 000
2022-05-25	10:19:14	3.3500 %	2 487 000
2022-05-25	10:19:22	3.3600 %	2 685 000
2022-05-25	10:19:30	3.2800 %	3 275 000
2022-05-25	10:19:38	3.2900 %	2 743 000
2022-05-25	10:19:46	3.2600 %	2 923 000
2022-05-25	10:19:54	3.3400 %	3 054 000
2022-05-25	10:20:02	3.3100 %	2 644 000
2022-05-25	10:20:10	3.3300 %	3 002 000
2022-05-25	10:20:19	3.2600 %	2 819 000

Table B.2-1. Both VOAs set to 3 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-05-25	17:37:08	3.2700 %	2 642 000
2022-05-25	17:37:17	3.2800 %	2 712 000
2022-05-25	17:37:24	3.1900 %	2 883 000
2022-05-25	17:37:32	3.2000 %	2 997 000
2022-05-25	17:37:40	3.2200 %	2 730 000
2022-05-25	17:37:48	3.2400 %	2 665 000
2022-05-25	17:37:56	3.2000 %	2 867 000
2022-05-25	17:38:04	3.1800 %	2 851 000
2022-05-25	17:38:12	3.1400 %	3 105 000
2022-05-25	17:38:20	3.2400 %	2 839 000

Table B.2-2. Both VOAs set to 4 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-05-25	18:37:41	3.2500 %	2 692 000
2022-05-25	18:37:50	3.3200 %	2 592 000
2022-05-25	18:37:57	3.2000 %	3 097 000
2022-05-25	18:38:05	3.2200 %	2 892 000
2022-05-25	18:38:12	3.2600 %	2 835 000
2022-05-25	18:38:21	3.3100 %	2 650 000
2022-05-25	18:38:29	3.3000 %	2 767 000
2022-05-25	18:38:37	3.2700 %	2 539 000
2022-05-25	18:38:45	3.2300 %	2 837 000
2022-05-25	18:38:53	3.2300 %	2 812 000

Table B.2-3. Both VOAs set to 5 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-05-26	09:34:44	3.2400 %	1 961 000
2022-05-26	09:34:57	3.1800 %	1 884 000
2022-05-26	09:35:09	3.3700 %	1 805 000
2022-05-26	09:35:20	3.3400 %	2 027 000
2022-05-26	09:35:33	3.2000 %	1 745 000
2022-05-26	09:35:45	3.2300 %	1 962 000
2022-05-26	09:35:57	3.2600 %	1 870 000
2022-05-26	09:36:10	3.2000 %	1 926 000
2022-05-26	09:36:21	3.2400 %	2 031 000
2022-05-26	09:36:33	3.4800 %	1 779 000

Table B.2-4. Both VOAs set to 6 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-05-26	10:56:56	3.2500 %	1 789 000
2022-05-26	10:57:08	3.2200 %	1 838 000
2022-05-26	10:57:20	3.1500 %	1 983 000
2022-05-26	10:57:33	3.0900 %	1 833 000
2022-05-26	10:57:46	3.2000 %	1 830 000
2022-05-26	10:57:59	3.2400 %	1 793 000
2022-05-26	10:58:11	3.2300 %	1 817 000
2022-05-26	10:58:24	3.2300 %	1 841 000
2022-05-26	10:58:37	3.2100 %	1 833 000
2022-05-26	10:58:49	3.2300 %	1 864 000

Table B.2-5. Both VOAs set to 7 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-05-26	14:03:27	3.3000 %	1 389 000
2022-05-26	14:03:44	3.1000 %	1 370 000
2022-05-26	14:04:00	3.3700 %	1 371 000
2022-05-26	14:04:15	3.2700 %	1 438 000
2022-05-26	14:04:32	3.2500 %	1 405 000
2022-05-26	14:04:47	3.3900 %	1 362 000
2022-05-26	14:05:04	3.2600 %	1 378 000
2022-05-26	14:05:20	3.3800 %	1 306 000
2022-05-26	14:05:37	3.3500 %	1 348 000
2022-05-26	14:05:53	3.3300 %	1 311 000

Table B.2-6. Both VOAs set to 8 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-05-26	14:41:27	3.2500 %	1 074 000
2022-05-26	14:41:46	3.3800 %	1 056 000
2022-05-26	14:42:07	3.3300 %	1 092 000
2022-05-26	14:42:27	3.3900 %	1 059 000
2022-05-26	14:42:47	3.4400 %	1 117 000
2022-05-26	14:43:07	3.4500 %	1 036 000
2022-05-26	14:43:26	3.4400 %	1 136 000
2022-05-26	14:43:46	3.4700 %	1 085 000
2022-05-26	14:44:07	3.4600 %	1 038 000
2022-05-26	14:44:27	3.3600 %	1 162 000

Table B.2-7. Both VOAs set to 9 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-05-26	15:04:22	3.3000 %	962 000
2022-05-26	15:04:44	3.2900 %	1 019 000
2022-05-26	15:05:06	3.3200 %	1 023 000
2022-05-26	15:05:30	3.3200 %	987 000
2022-05-26	15:05:52	3.4200 %	992 000
2022-05-26	15:06:15	3.4000 %	957 000
2022-05-26	15:06:37	3.4200 %	984 000
2022-05-26	15:07:01	3.5000 %	909 000
2022-05-26	15:07:23	3.3900 %	1 049 000
2022-05-26	15:07:46	3.4500 %	969 000

Table B.2-8. Both VOAs set to 10 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-05-26	17:08:46	3.3300 %	654 000
2022-05-26	17:09:17	3.3000 %	704 000
2022-05-26	17:09:49	3.2400 %	674 000
2022-05-26	17:10:22	3.1500 %	689 000
2022-05-26	17:10:54	3.2600 %	671 000
2022-05-26	17:11:26	3.2200 %	678 000
2022-05-26	17:11:58	3.2500 %	682 000
2022-05-26	17:12:30	3.3500 %	662 000
2022-05-26	17:13:01	3.2000 %	700 000
2022-05-26	17:13:34	3.2600 %	659 000

Table B.2-9. Both VOAs set to 11 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-05-26	16:47:38	3.3000 %	527 000
2022-05-26	16:48:17	3.2800 %	556 000
2022-05-26	16:48:56	3.3000 %	554 000
2022-05-26	16:49:36	3.3200 %	535 000
2022-05-26	16:50:15	3.3100 %	553 000
2022-05-26	16:50:54	3.3100 %	560 000
2022-05-26	16:51:33	3.2400 %	560 000
2022-05-26	16:52:12	3.2900 %	564 000
2022-05-26	16:52:51	3.2900 %	564 000
2022-05-26	16:53:28	3.1900 %	603 000

Table B.2-10. Both VOAs set to 12 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-05-27	10:33:15	3.4500 %	500 000
2022-05-27	10:33:56	3.5000 %	508 000
2022-05-27	10:34:38	3.6000 %	475 000
2022-05-27	10:35:21	3.4000 %	501 000
2022-05-27	10:36:04	3.6300 %	464 000
2022-05-27	10:36:46	3.4500 %	503 000
2022-05-27	10:37:29	3.3600 %	503 000
2022-05-27	10:38:11	3.2900 %	528 000
2022-05-27	10:38:54	3.3100 %	514 000
2022-05-27	10:39:37	3.2300 %	525 000

Table B.2-11. Both VOAs set to 13 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-05-27	10:56:12	3.3000 %	346 000
2022-05-27	10:57:12	3.3500 %	345 000
2022-05-27	10:58:11	3.3600 %	349 000
2022-05-27	10:59:10	3.3500 %	346 000
2022-05-27	11:00:11	3.4600 %	326 000
2022-05-27	11:01:09	3.4500 %	341 000
2022-05-27	11:02:08	3.5000 %	319 000
2022-05-27	11:03:07	3.4700 %	329 000
2022-05-27	11:04:05	3.5000 %	336 000
2022-05-27	11:05:03	3.4400 %	343 000

Table B.2-12. Both VOAs set to 14 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-05-27	11:20:31	3.3000 %	286 000
2022-05-27	11:21:47	3.4000 %	274 000
2022-05-27	11:23:03	3.3400 %	279 000
2022-05-27	11:24:19	3.4000 %	272 000
2022-05-27	11:25:34	3.3100 %	288 000
2022-05-27	11:26:49	3.4000 %	282 000
2022-05-27	11:28:04	3.5100 %	274 000
2022-05-27	11:29:17	3.3600 %	289 000
2022-05-27	11:30:31	3.4400 %	288 000
2022-05-27	11:31:44	3.3900 %	295 000

Table B.2-13. Both VOAs set to 15 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-05-27	11:46:34	3.4500 %	253 000
2022-05-27	11:47:58	3.4700 %	251 000
2022-05-27	11:49:22	3.5100 %	246 000
2022-05-27	11:50:45	3.3900 %	252 000
2022-05-27	11:52:08	3.4200 %	253 000
2022-05-27	11:53:31	3.3600 %	250 000
2022-05-27	11:54:54	3.4100 %	252 000
2022-05-27	11:56:15	3.4300 %	245 000
2022-05-27	11:57:37	3.4000 %	250 000
2022-05-27	11:58:59	3.3700 %	251 000

Table B.2-14. Both VOAs set to 16 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-05-27	13:43:21	3.3800 %	184 000
2022-05-27	13:45:15	3.5400 %	177 000
2022-05-27	13:47:13	3.5800 %	172 000
2022-05-27	13:49:09	3.3700 %	183 000
2022-05-27	13:51:09	3.4500 %	173 000
2022-05-27	13:53:08	3.5000 %	170 000
2022-05-27	13:55:07	3.4700 %	170 000
2022-05-27	13:57:08	3.4400 %	172 000
2022-05-27	13:59:05	3.4400 %	177 000
2022-05-27	14:01:01	3.4400 %	176 000

Table B.2-15. Both VOAs set to 17 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-05-27	15:00:17	3.8900 %	137 000
2022-05-27	15:02:29	3.6400 %	152 000
2022-05-27	15:04:39	3.7200 %	143 000
2022-05-27	15:06:52	3.4500 %	158 000
2022-05-27	15:09:07	3.4700 %	151 000
2022-05-27	15:11:20	3.5900 %	146 000
2022-05-27	15:13:29	3.4100 %	165 000
2022-05-27	15:15:38	3.4900 %	159 000
2022-05-27	15:17:47	3.4600 %	163 000
2022-05-27	15:19:57	3.4300 %	164 000

Table B.2-16. Both VOAs set to 18 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-05-27	15:46:15	3.6500 %	115 000
2022-05-27	15:48:50	3.6600 %	123 000
2022-05-27	15:51:30	3.7300 %	116 000
2022-05-27	15:54:13	3.9900 %	99 000
2022-05-27	15:56:56	3.6800 %	120 000
2022-05-27	15:59:43	3.4200 %	124 000
2022-05-27	16:02:28	3.4900 %	123 000
2022-05-27	16:05:14	3.4800 %	123 000
2022-05-27	16:08:00	3.4700 %	126 000
2022-05-27	16:10:43	3.4500 %	127 000

Table B.2-17. Both VOAs set to 19 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-05-27	16:26:26	3.4600 %	88 000
2022-05-27	16:30:19	3.5300 %	86 000
2022-05-27	16:34:16	3.5700 %	83 000
2022-05-27	16:38:06	3.5400 %	88 000
2022-05-27	16:41:57	3.6000 %	87 000
2022-05-27	16:45:43	3.7700 %	82 000
2022-05-27	16:49:37	3.6500 %	83 000
2022-05-27	16:53:35	3.5100 %	89 000
2022-05-27	16:57:34	3.7400 %	76 000
2022-05-27	17:01:29	3.6200 %	81 000

Table B.2-18. Both VOAs set to 20 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-05-28	15:26:15	3.6900 %	66 000
2022-05-28	15:31:16	3.6100 %	65 000
2022-05-28	15:36:20	3.8300 %	57 000
2022-05-28	15:41:12	3.7600 %	63 000
2022-05-28	15:46:01	3.7100 %	66 000
2022-05-28	15:50:52	3.9500 %	59 000
2022-05-28	15:55:49	3.6700 %	64 000
2022-05-28	16:00:54	3.6500 %	63 000
2022-05-28	16:05:51	3.6800 %	65 000
2022-05-28	16:10:42	3.5800 %	70 000

Table B.2-19. Both VOAs set to 21 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-05-29	13:49:27	3.9500 %	45 000
2022-05-29	13:55:28	3.8700 %	50 000
2022-05-29	14:01:31	3.9700 %	48 000
2022-05-29	14:07:33	3.8400 %	49 000
2022-05-29	14:13:30	3.5800 %	57 000
2022-05-29	14:19:37	4.0200 %	46 000
2022-05-29	14:25:40	4.3900 %	40 000
2022-05-29	14:31:41	3.8100 %	49 000
2022-05-29	14:37:42	4.0800 %	42 000
2022-05-29	14:43:46	3.8200 %	50 000

Table B.2-20. Both VOAs set to 22 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-05-29	15:21:49	4.1100 %	34 000
2022-05-29	15:29:51	3.9700 %	34 000
2022-05-29	15:37:45	3.8100 %	38 000
2022-05-29	15:45:21	4.2100 %	33 000
2022-05-29	15:53:10	4.0400 %	35 000
2022-05-29	16:01:06	3.8100 %	37 000
2022-05-29	16:08:47	4.1400 %	33 000
2022-05-29	16:16:36	4.0000 %	36 000
2022-05-29	16:24:36	3.9800 %	33 000
2022-05-29	16:32:17	4.0600 %	35 000

Table B.2-21. Both VOAs set to 23 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-05-29	17:14:15	3.9500 %	27 000
2022-05-29	17:24:07	4.0100 %	29 000
2022-05-29	17:33:57	4.4100 %	26 000
2022-05-29	17:44:07	4.0700 %	26 000
2022-05-29	17:53:57	4.1000 %	28 000
2022-05-29	18:03:49	4.1600 %	29 000
2022-05-29	18:13:49	4.0800 %	26 000
2022-05-29	18:23:39	4.3700 %	25 000
2022-05-29	18:33:41	4.2100 %	26 000
2022-05-29	18:43:50	4.1100 %	26 000

Table B.2-22. Both VOAs set to 24 dB of attenuation.

B.3 VOAs and Fibre

Data points from the test setup when using VOAs and spools of optical fibre combined for inducing attenuation. Both fibre spools are 50 km, and the system as a whole has a total insertion loss of 13.1 dB from `Alice` to Bob. This level of attenuation should be added to the set value of the VOAs, as given in the tables below.

Date	Time	QBER	SKR (bps)
2022-06-01	14:49:51	3.9900 %	45 000
2022-06-01	14:56:43	4.1600 %	44 000
2022-06-01	15:03:43	4.0100 %	46 000
2022-06-01	15:10:53	4.2700 %	38 000
2022-06-01	15:18:03	4.1500 %	42 000
2022-06-01	15:25:00	4.0700 %	46 000
2022-06-01	15:32:01	4.1600 %	44 000
2022-06-01	15:39:03	4.1900 %	42 000
2022-06-01	15:46:07	4.1700 %	42 000
2022-06-01	15:52:56	4.1000 %	48 000

Table B.3-1. Both VOAs set to 1 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-06-02	08:34:33	4.2800 %	36 000
2022-06-02	08:42:16	4.2800 %	37 000
2022-06-02	08:49:59	4.1500 %	37 000
2022-06-02	08:57:41	4.5200 %	29 000
2022-06-02	09:05:27	4.5700 %	32 000
2022-06-02	09:13:05	4.2400 %	38 000
2022-06-02	09:20:47	4.5000 %	29 000
2022-06-02	09:28:30	4.2100 %	36 000
2022-06-02	09:36:13	4.2300 %	38 000
2022-06-02	09:43:58	4.2300 %	36 000

Table B.3-2. Both VOAs set to 2 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-06-02	10:36:26	4.1600 %	26 000
2022-06-02	10:48:17	4.2700 %	24 000
2022-06-02	11:00:10	4.2300 %	25 000
2022-06-02	11:11:53	4.3200 %	25 000
2022-06-02	11:23:50	4.2000 %	25 000
2022-06-02	11:35:34	4.4000 %	23 000
2022-06-02	11:47:30	4.1600 %	25 000
2022-06-02	11:59:09	4.3400 %	25 000
2022-06-02	12:11:03	4.2800 %	24 000
2022-06-02	12:22:57	4.3200 %	24 000

Table B.3-3. Both VOAs set to 3 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-06-02	12:54:08	5.0300 %	17 000
2022-06-02	13:06:14	4.5200 %	22 000
2022-06-02	13:18:19	4.5400 %	22 000
2022-06-02	13:30:28	4.8300 %	19 000
2022-06-02	13:42:36	4.5800 %	21 000
2022-06-02	13:54:37	4.7200 %	21 000
2022-06-02	14:06:47	4.5000 %	21 000
2022-06-02	14:18:54	5.0100 %	18 000
2022-06-02	14:31:01	4.6000 %	21 000
2022-06-02	14:43:03	4.4900 %	23 000

Table B.3-4. Both VOAs set to 4 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-06-03	06:46:03	4.6200 %	14 000
2022-06-03	07:04:40	4.6800 %	13 000
2022-06-03	07:23:18	4.5200 %	14 000
2022-06-03	07:41:45	4.7000 %	13 000
2022-06-03	08:00:16	4.6400 %	13 000
2022-06-03	08:18:56	4.6700 %	13 000
2022-06-03	08:37:11	4.7100 %	13 000
2022-06-03	08:55:34	4.5800 %	13 000
2022-06-03	09:14:05	4.6700 %	13 000
2022-06-03	09:32:23	4.5500 %	14 000

Table B.3-5. Both VOAs set to 5 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-06-03	10:22:14	4.8800 %	9000
2022-06-03	10:45:49	5.0200 %	8000
2022-06-03	11:09:22	5.0600 %	8000
2022-06-03	11:32:49	4.8600 %	10 000
2022-06-03	11:56:13	4.9200 %	9000
2022-06-03	12:19:48	4.9800 %	8000
2022-06-03	12:43:27	5.0700 %	8000
2022-06-03	13:06:48	4.9200 %	9000
2022-06-03	13:30:09	4.9600 %	9000
2022-06-03	13:53:39	4.9200 %	9000

Table B.3-6. Both VOAs set to 6 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-06-06	00:57:11	5.3200 %	6000
2022-06-06	01:26:48	5.2600 %	6000
2022-06-06	01:56:29	5.3800 %	5000
2022-06-06	03:56:38	5.4200 %	6000
2022-06-06	04:20:44	5.3200 %	7000
2022-06-06	06:22:37	5.3600 %	7000
2022-06-06	07:27:55	5.2500 %	6000
2022-06-06	09:29:11	5.1600 %	8000
2022-06-06	09:29:11	5.1600 %	8000
2022-06-06	10:37:16	5.3000 %	6000

Table B.3-7. Both VOAs set to 7 dB of attenuation. Note the anomalies of a long delay after 01:56:29, and the double timestamp at 09:29:11

Date	Time	QBER	SKR (bps)
2022-06-07	04:28:15	5.9100 %	3000
2022-06-07	05:05:18	5.9000 %	3000
2022-06-07	05:42:24	5.7900 %	3000
2022-06-07	06:19:39	5.7800 %	4000
2022-06-07	06:56:39	5.8600 %	4000
2022-06-07	07:34:00	5.8400 %	4000
2022-06-07	08:11:16	5.7400 %	4000
2022-06-07	08:48:29	5.7700 %	4000
2022-06-07	09:25:44	5.8500 %	3000
2022-06-07	10:02:49	5.8300 %	3000

Table B.3-8. Both VOAs set to 8 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-06-08	00:56:27	6.4000 %	2000
2022-06-08	01:36:32	6.4600 %	2000
2022-06-08	02:16:39	6.4500 %	1000
2022-06-08	02:57:13	6.4200 %	2000
2022-06-08	03:37:34	6.5600 %	1000
2022-06-08	04:17:44	6.3900 %	2000
2022-06-08	04:57:25	6.4100 %	2000
2022-06-08	05:38:09	6.3600 %	2000
2022-06-08	06:18:45	6.3700 %	2000
2022-06-08	06:58:56	6.4400 %	2000

Table B.3-9. Both VOAs set to 9 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-06-08	08:41:54	6.8800 %	0
2022-06-08	09:29:01	7.0900 %	0
2022-06-08	10:15:50	6.8400 %	0
2022-06-08	11:03:06	6.7500 %	1000
2022-06-08	11:50:33	7.0000 %	0
2022-06-08	12:37:50	6.7400 %	1000
2022-06-08	13:25:05	6.9600 %	0
2022-06-08	14:12:22	6.9400 %	0
2022-06-08	14:59:46	6.8800 %	0
2022-06-08	15:47:33	6.7800 %	1000

Table B.3-10. Both VOAs set to 10 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-06-09	12:05:01	8.0100 %	0
2022-06-09	13:17:25	8.0000 %	0
2022-06-09	14:29:54	8.0900 %	0
2022-06-09	15:42:42	8.0900 %	0
2022-06-09	16:55:21	8.0800 %	0
2022-06-09	18:08:13	8.0900 %	0
2022-06-09	19:21:29	8.0000 %	0
2022-06-09	20:34:55	7.8900 %	0
2022-06-09	21:47:06	8.1400 %	0
2022-06-09	22:59:39	7.9000 %	0

Table B.3-11. Both VOAs set to 11 dB of attenuation. The non-zero SKR is below 1000 bps, and is therefore rounded down by the equipment.

Date	Time	QBER	SKR (bps)
2022-06-10	22:48:59	8.7200 %	0
2022-06-11	00:05:10	8.9700 %	0
2022-06-11	01:22:02	8.9300 %	0
2022-06-11	02:38:54	8.9900 %	0
2022-06-11	03:55:45	9.0500 %	0
2022-06-11	05:12:12	8.8400 %	0
2022-06-11	06:28:56	8.9400 %	0
2022-06-11	07:45:19	8.8200 %	0
2022-06-11	09:01:37	8.7100 %	0
2022-06-11	10:18:45	8.8100 %	0

Table B.3-12. Both VOAs set to 12 dB of attenuation. The non-zero SKR is below 1000 bps, and is therefore displayed as such.

B.4 VOAs, Fibre, and Data

Data points from the test setup when using VOAs and spools of optical fibre combined for inducing attenuation. Both fibre spools are 50 km, and the system as a whole has a total insertion loss of 10.6 dB from `Alice` to Bob. This level of attenuation should be added to the set value of the VOAs, as given in the tables below. A single data wave is transmitted in both directions centred around 1563.0 nm.

B.4.1 Baseline measurements. Data points when no data wave is introduced to the shared fibre.

Date	Time	QBER	SKR (bps)
2022-07-04	08:55:47	3.7400 %	82 000
2022-07-04	08:59:48	3.6600 %	91 000
2022-07-04	09:03:54	3.5100 %	93 000
2022-07-04	09:08:01	3.7300 %	86 000
2022-07-04	09:12:13	3.8200 %	83 000
2022-07-04	09:16:24	3.6900 %	86 000
2022-07-04	09:20:35	3.5800 %	87 000
2022-07-04	09:24:40	4.0900 %	71 000
2022-07-04	09:28:48	3.6600 %	86 000
2022-07-04	09:32:55	3.6300 %	88 000

Table B.4-1. Both VOAs set to 1 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-03	23:11:12	3.5900 %	78 000
2022-07-03	23:16:01	3.6600 %	76 000
2022-07-03	23:20:59	3.6800 %	73 000
2022-07-03	23:25:56	4.0600 %	62 000
2022-07-03	23:30:52	3.8000 %	71 000
2022-07-03	23:35:46	3.5500 %	80 000
2022-07-03	23:40:35	3.6200 %	77 000
2022-07-03	23:45:27	3.8500 %	70 000
2022-07-03	23:50:24	3.6300 %	75 000
2022-07-03	23:55:17	3.7500 %	73 000

Table B.4-2. Both VOAs set to 2 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-04	09:52:56	4.0600 %	49 000
2022-07-04	09:59:05	3.7800 %	58 000
2022-07-04	10:05:17	3.9700 %	55 000
2022-07-04	10:11:35	3.8000 %	56 000
2022-07-04	10:17:50	3.8000 %	59 000
2022-07-04	10:24:00	3.8400 %	56 000
2022-07-04	10:30:10	3.9900 %	53 000
2022-07-04	10:36:30	3.7100 %	60 000
2022-07-04	10:42:42	3.7200 %	60 000
2022-07-04	10:48:50	3.7000 %	60 000

Table B.4-3. Both VOAs set to 3 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-04	11:17:51	4.1100 %	40 000
2022-07-04	11:26:01	3.9800 %	41 000
2022-07-04	11:34:03	3.9000 %	42 000
2022-07-04	11:41:58	4.0500 %	40 000
2022-07-04	11:50:04	4.0200 %	40 000
2022-07-04	12:23:14	4.0900 %	41 000
2022-07-04	12:30:40	4.1200 %	42 000
2022-07-04	12:38:06	4.2100 %	40 000
2022-07-04	12:45:40	4.1900 %	39 000
2022-07-04	12:53:05	4.1400 %	39 000

Table B.4-4. Both VOAs set to 4 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-05	08:45:59	4.2600 %	31 000
2022-07-05	08:55:23	4.0500 %	35 000
2022-07-05	09:04:54	4.2200 %	31 000
2022-07-05	09:14:26	4.2400 %	31 000
2022-07-05	09:23:55	4.0100 %	35 000
2022-07-05	09:33:24	4.1000 %	34 000
2022-07-05	09:42:52	4.1500 %	33 000
2022-07-05	09:52:31	4.0500 %	34 000
2022-07-05	10:01:57	4.0800 %	34 000
2022-07-05	10:11:36	4.1700 %	32 000

Table B.4-5. Both VOAs set to 5 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-05	06:59:55	4.5500 %	22 000
2022-07-05	07:11:53	4.1600 %	25 000
2022-07-05	07:23:54	4.4900 %	22 000
2022-07-05	07:35:55	4.1500 %	25 000
2022-07-05	07:47:51	4.3900 %	24 000
2022-07-05	07:59:44	4.1900 %	25 000
2022-07-05	07:59:44	4.1900 %	25 000
2022-07-05	08:11:37	4.4500 %	22 000
2022-07-05	08:23:38	4.3800 %	23 000
2022-07-05	08:23:38	4.3800 %	23 000

Table B.4-6. Both VOAs set to 6 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-05	10:48:10	4.5700 %	16 000
2022-07-05	11:04:07	4.4800 %	17 000
2022-07-05	11:20:19	4.5300 %	17 000
2022-07-05	11:36:21	4.5400 %	16 000
2022-07-05	11:52:26	4.4300 %	18 000
2022-07-05	12:08:13	4.3900 %	18 000
2022-07-05	12:24:18	4.4900 %	17 000
2022-07-05	12:40:11	4.6200 %	16 000
2022-07-05	12:56:08	4.3700 %	18 000
2022-07-05	13:12:10	4.4300 %	18 000

Table B.4-7. Both VOAs set to 7 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-05	13:49:35	4.7100 %	13 000
2022-07-05	14:08:00	4.7100 %	13 000
2022-07-05	14:26:34	4.8000 %	13 000
2022-07-05	14:45:05	4.7200 %	13 000
2022-07-05	15:03:42	4.7500 %	13 000
2022-07-05	15:22:24	4.7200 %	13 000
2022-07-05	15:40:59	4.5900 %	14 000
2022-07-05	15:59:29	4.8700 %	12 000
2022-07-05	16:18:26	4.6900 %	13 000
2022-07-05	16:37:09	4.7300 %	13 000

Table B.4-8. Both VOAs set to 8 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-06	04:48:39	4.9000 %	8000
2022-07-06	05:17:54	4.9900 %	8000
2022-07-06	05:47:23	4.9900 %	8000
2022-07-06	06:16:30	4.8700 %	8000
2022-07-06	06:45:49	5.0400 %	7000
2022-07-06	07:14:57	4.9700 %	8000
2022-07-06	07:44:06	4.8900 %	8000
2022-07-06	08:13:34	4.7900 %	9000
2022-07-06	08:42:36	4.8800 %	8000
2022-07-06	09:11:44	4.9000 %	8000

Table B.4-9. Both VOAs set to 9 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-06	10:20:15	5.5300 %	6000
2022-07-06	10:49:43	5.4200 %	6000
2022-07-06	11:19:20	5.4900 %	6000
2022-07-06	11:48:48	5.4800 %	6000
2022-07-06	12:18:21	5.3800 %	6000
2022-07-06	12:48:02	5.4300 %	6000
2022-07-06	13:17:29	5.4600 %	6000
2022-07-06	13:46:54	5.3400 %	6000
2022-07-06	14:16:21	5.3500 %	6000
2022-07-06	14:45:47	5.4100 %	6000

Table B.4-10. Both VOAs set to 10 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-07	00:50:36	6.0000 %	2000
2022-07-07	01:36:38	5.9000 %	3000
2022-07-07	02:22:54	5.9300 %	3000
2022-07-07	03:08:58	5.8500 %	3000
2022-07-07	03:55:11	6.0600 %	2000
2022-07-07	04:41:07	5.9200 %	3000
2022-07-07	05:27:17	6.0300 %	2000
2022-07-07	06:12:58	5.9400 %	3000
2022-07-07	06:58:52	6.0100 %	2000
2022-07-07	07:44:46	6.0200 %	2000

Table B.4-11. Both VOAs set to 11 dB of attenuation.

B.4.2 Single Wave at 0 dB*m.* Data points when a single data wave at a power level of 0 dBm is introduced to the shared fibre.

Date	Time	QBER	SKR (bps)
2022-06-24	16:03:20	3.6400 %	84 000
2022-06-24	16:07:25	3.5800 %	93 000
2022-06-24	16:11:34	3.7000 %	82 000
2022-06-24	16:15:45	3.8000 %	86 000
2022-06-24	16:19:54	4.1900 %	75 000
2022-06-24	16:24:01	3.8700 %	83 000
2022-06-24	16:28:14	3.4300 %	94 000
2022-06-24	16:32:22	3.6800 %	87 000
2022-06-24	16:36:30	3.5900 %	90 000
2022-06-24	16:40:40	3.6100 %	86 000

Table B.4-12. Both VOAs set to 1 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-06-26	23:13:18	3.6900 %	74 000
2022-06-26	23:18:11	3.6900 %	76 000
2022-06-26	23:23:05	3.8200 %	71 000
2022-06-26	23:28:00	3.5500 %	78 000
2022-06-26	23:32:56	3.7100 %	75 000
2022-06-26	23:37:46	3.7500 %	76 000
2022-06-26	23:42:34	3.9400 %	72 000
2022-06-26	23:47:27	3.8600 %	71 000
2022-06-26	23:52:24	3.6200 %	76 000
2022-06-26	23:57:22	3.6800 %	74 000

Table B.4-13. Both VOAs set to 2 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-06-27	09:27:02	3.8700 %	54 000
2022-06-27	09:33:18	3.7600 %	57 000
2022-06-27	09:39:26	3.8700 %	57 000
2022-06-27	09:45:43	3.7700 %	57 000
2022-06-27	09:51:58	3.7600 %	57 000
2022-06-27	09:58:05	3.8200 %	57 000
2022-06-27	10:04:15	3.9300 %	56 000
2022-06-27	10:10:35	3.7700 %	58 000
2022-06-27	10:16:47	3.7800 %	57 000
2022-06-27	10:22:58	3.8300 %	59 000

Table B.4-14. Both VOAs set to 3 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-06-27	13:36:02	3.9400 %	36 000
2022-06-27	13:45:37	4.0700 %	34 000
2022-06-27	13:55:03	4.0600 %	33 000
2022-06-27	14:04:25	3.9200 %	36 000
2022-06-27	14:13:51	4.0400 %	35 000
2022-06-27	14:23:12	4.0300 %	34 000
2022-06-27	14:32:30	3.8300 %	39 000
2022-06-27	14:41:54	3.8000 %	38 000
2022-06-27	14:51:15	3.9200 %	36 000
2022-06-27	15:00:28	4.0600 %	34 000

Table B.4-15. Both VOAs set to 4 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-06-27	11:37:00	4.7300 %	26 000
2022-06-27	11:46:30	4.2700 %	31 000
2022-06-27	11:55:54	4.0700 %	33 000
2022-06-27	12:05:23	4.4700 %	29 000
2022-06-27	12:14:52	4.0700 %	33 000
2022-06-27	12:24:19	4.2500 %	32 000
2022-06-27	12:33:45	4.2200 %	32 000
2022-06-27	12:43:12	4.0900 %	33 000
2022-06-27	12:52:41	4.5500 %	28 000
2022-06-27	13:02:15	4.0200 %	34 000

Table B.4-16. Both VOAs set to 5 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-06-27	18:55:00	4.2300 %	25 000
2022-06-27	19:06:56	4.3200 %	24 000
2022-06-27	19:18:55	4.3000 %	24 000
2022-06-27	19:30:41	4.2000 %	26 000
2022-06-27	19:42:45	4.5900 %	21 000
2022-06-27	19:54:41	4.4700 %	22 000
2022-06-27	20:06:34	4.5000 %	22 000
2022-06-27	20:18:27	4.2400 %	25 000
2022-06-27	20:30:14	4.2900 %	25 000
2022-06-27	20:42:09	4.2100 %	25 000

Table B.4-17. Both VOAs set to 6 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-06-28	06:13:35	4.4600 %	18 000
2022-06-28	06:28:27	4.4500 %	19 000
2022-06-28	06:43:23	4.3000 %	20 000
2022-06-28	06:58:16	4.4100 %	19 000
2022-06-28	07:13:07	4.4100 %	19 000
2022-06-28	07:28:18	4.6000 %	16 000
2022-06-28	07:43:19	4.6000 %	17 000
2022-06-28	07:58:16	4.5200 %	18 000
2022-06-28	08:13:09	4.4800 %	19 000
2022-06-28	08:28:05	4.6100 %	17 000

Table B.4-18. Both VOAs set to 7 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-06-28	09:06:35	4.7900 %	12 000
2022-06-28	09:25:02	4.6400 %	14 000
2022-06-28	09:43:36	4.7200 %	13 000
2022-06-28	10:02:22	4.7400 %	13 000
2022-06-28	10:21:05	4.8700 %	12 000
2022-06-28	10:39:53	4.8300 %	12 000
2022-06-28	10:58:24	4.9000 %	13 000
2022-06-28	11:17:03	4.7600 %	13 000
2022-06-28	11:35:35	4.7500 %	13 000
2022-06-28	11:54:12	4.7000 %	14 000

Table B.4-19. Both VOAs set to 8 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-06-28	13:19:14	5.0900 %	9000
2022-06-28	13:42:59	5.1300 %	9000
2022-06-28	14:06:37	5.1200 %	9000
2022-06-28	14:30:17	5.2700 %	8000
2022-06-28	14:53:51	5.2500 %	8000
2022-06-28	15:17:27	5.1300 %	9000
2022-06-28	15:40:57	5.3600 %	7000
2022-06-28	16:04:42	5.2200 %	8000
2022-06-28	16:28:27	5.1100 %	9000
2022-06-28	16:52:07	5.1300 %	9000

Table B.4-20. Both VOAs set to 9 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-06-29	03:40:13	5.6800 %	5000
2022-06-29	04:11:45	5.7000 %	5000
2022-06-29	04:43:10	5.5800 %	6000
2022-06-29	05:14:43	5.4300 %	6000
2022-06-29	05:46:26	5.6200 %	5000
2022-06-29	06:17:43	5.7300 %	5000
2022-06-29	06:49:18	5.5700 %	6000
2022-06-29	07:21:00	5.6300 %	5000
2022-06-29	07:52:27	5.5900 %	6000
2022-06-29	08:24:09	5.5700 %	6000

Table B.4-21. Both VOAs set to 10 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-06-29	09:51:33	5.9000 %	3000
2022-06-29	10:37:48	5.9400 %	3000
2022-06-29	11:23:41	5.9500 %	3000
2022-06-29	12:09:30	5.8200 %	3000
2022-06-29	12:55:24	5.8300 %	3000
2022-06-29	13:41:28	5.9000 %	3000
2022-06-29	14:27:49	5.9900 %	2000
2022-06-29	15:14:03	5.8300 %	3000
2022-06-29	16:00:03	5.8300 %	3000
2022-06-29	16:46:35	5.8100 %	3000

Table B.4-22. Both VOAs set to 11 dB of attenuation.

B.4.3 Single Wave at 3 dB*m.* Data points when a single data wave at a power level of 3 dBm is introduced to the shared fibre.

Date	Time	QBER	SKR (bps)
2022-06-30	09:24:14	3.9200 %	102 000
2022-06-30	09:28:37	3.7500 %	108 000
2022-06-30	09:33:12	3.7800 %	101 000
2022-06-30	09:37:40	3.8100 %	101 000
2022-06-30	09:42:09	3.7400 %	102 000
2022-06-30	09:46:33	3.6200 %	114 000
2022-06-30	09:50:52	3.7900 %	108 000
2022-06-30	09:55:19	3.9400 %	100 000
2022-06-30	09:59:46	3.5800 %	111 000
2022-06-30	10:04:15	3.6300 %	106 000

Table B.4-23. Both VOAs set to 1 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-06-30	10:28:13	3.8800 %	74 000
2022-06-30	10:32:39	3.6600 %	81 000
2022-06-30	10:37:12	3.7100 %	80 000
2022-06-30	10:41:45	3.9400 %	71 000
2022-06-30	10:46:19	3.8800 %	75 000
2022-06-30	10:50:56	3.7500 %	76 000
2022-06-30	10:55:30	4.0900 %	64 000
2022-06-30	11:00:02	3.9100 %	73 000
2022-06-30	11:04:35	3.7900 %	77 000
2022-06-30	11:09:09	3.9900 %	71 000

Table B.4-24. Both VOAs set to 2 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-06-30	11:58:55	3.9500 %	58 000
2022-06-30	12:05:19	3.8300 %	54 000
2022-06-30	12:11:44	4.0600 %	48 000
2022-06-30	12:18:06	3.9000 %	53 000
2022-06-30	12:24:17	3.8600 %	57 000
2022-06-30	12:30:37	3.8600 %	55 000
2022-06-30	12:36:57	3.7700 %	57 000
2022-06-30	12:43:15	3.8600 %	56 000
2022-06-30	12:49:26	3.9400 %	55 000
2022-06-30	12:55:46	3.8400 %	55 000

Table B.4-25. Both VOAs set to 3 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-06-30	21:04:08	4.0600 %	35 000
2022-06-30	21:13:24	4.1600 %	33 000
2022-06-30	21:22:34	3.9100 %	37 000
2022-06-30	21:31:48	3.9900 %	36 000
2022-06-30	21:41:03	3.9900 %	36 000
2022-06-30	21:50:12	4.0700 %	36 000
2022-06-30	21:59:29	3.9900 %	36 000
2022-06-30	22:08:42	4.0300 %	35 000
2022-06-30	22:17:53	3.9300 %	39 000
2022-06-30	22:27:10	3.9700 %	36 000

Table B.4-26. Both VOAs set to 4 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-01	06:25:53	4.3800 %	28 000
2022-07-01	06:35:17	4.1100 %	34 000
2022-07-01	06:44:39	4.2100 %	31 000
2022-07-01	07:28:39	4.2400 %	29 000
2022-07-01	07:58:51	4.1700 %	33 000
2022-07-01	08:08:10	4.2800 %	32 000
2022-07-01	08:17:33	4.1400 %	32 000
2022-07-01	08:26:55	4.2400 %	33 000
2022-07-01	08:36:25	4.2500 %	31 000
2022-07-01	08:45:49	4.0900 %	35 000

Table B.4-27. Both VOAs set to 5 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-01	09:26:48	4.4400 %	19 000
2022-07-01	09:41:10	4.2500 %	22 000
2022-07-01	09:55:57	4.2800 %	21 000
2022-07-01	10:10:39	4.3800 %	20 000
2022-07-01	10:25:15	4.2400 %	21 000
2022-07-01	10:39:59	4.2000 %	21 000
2022-07-01	10:54:47	4.3000 %	21 000
2022-07-01	11:09:33	4.1700 %	22 000
2022-07-01	11:24:10	4.3000 %	21 000
2022-07-01	11:38:57	4.1800 %	22 000

Table B.4-28. Both VOAs set to 6 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-01	12:25:52	4.6500 %	16 000
2022-07-01	12:41:34	4.5200 %	18 000
2022-07-01	12:57:51	4.7100 %	15 000
2022-07-01	13:14:04	4.5500 %	16 000
2022-07-01	13:30:11	4.5500 %	17 000
2022-07-01	13:46:14	4.5300 %	17 000
2022-07-01	14:02:06	4.6000 %	16 000
2022-07-01	14:18:11	4.5600 %	17 000
2022-07-01	14:34:19	4.5600 %	17 000
2022-07-01	14:50:15	4.5000 %	18 000

Table B.4-29. Both VOAs set to 7 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-02	06:50:12	4.6900 %	13 000
2022-07-02	07:10:17	4.7800 %	12 000
2022-07-02	07:30:39	4.8100 %	12 000
2022-07-02	07:50:46	4.8100 %	13 000
2022-07-02	08:10:48	4.8100 %	12 000
2022-07-02	08:30:35	4.9300 %	12 000
2022-07-02	08:50:31	4.8300 %	12 000
2022-07-02	09:10:30	4.7600 %	13 000
2022-07-02	09:30:28	4.8000 %	12 000
2022-07-02	09:50:15	4.8000 %	12 000

Table B.4-30. Both VOAs set to 8 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-02	12:47:59	5.2800 %	8000
2022-07-02	13:13:21	5.3000 %	8000
2022-07-02	13:38:28	5.2600 %	8000
2022-07-02	14:03:40	5.2700 %	8000
2022-07-02	14:28:39	5.2000 %	9000
2022-07-02	14:53:54	5.1900 %	8000
2022-07-02	15:19:07	5.1600 %	9000
2022-07-02	15:44:10	5.2300 %	8000
2022-07-02	16:09:21	5.2500 %	8000
2022-07-02	16:34:11	5.2700 %	8000

Table B.4-31. Both VOAs set to 9 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-02	17:28:04	5.4600 %	6000
2022-07-02	17:57:25	5.5700 %	5000
2022-07-02	18:26:47	5.5000 %	6000
2022-07-02	18:56:18	5.4000 %	6000
2022-07-02	19:26:04	5.4300 %	6000
2022-07-02	19:55:38	5.4800 %	6000
2022-07-02	20:25:08	5.4500 %	6000
2022-07-02	20:54:43	5.5600 %	5000
2022-07-02	21:24:16	5.4600 %	6000
2022-07-02	21:53:43	5.5700 %	5000

Table B.4-32. Both VOAs set to 10 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-03	03:22:59	6.3200 %	2000
2022-07-03	04:03:00	6.2200 %	2000
2022-07-03	04:42:51	6.3800 %	2000
2022-07-03	05:22:38	6.2000 %	3000
2022-07-03	06:02:43	6.3500 %	2000
2022-07-03	06:42:51	6.3900 %	2000
2022-07-03	07:22:40	6.4200 %	2000
2022-07-03	08:02:23	6.3800 %	2000
2022-07-03	08:42:50	6.3300 %	2000
2022-07-03	09:23:04	6.3900 %	2000

Table B.4-33. Both VOAs set to 11 dB of attenuation.

B.5 VOAs, Fibre, and More Data

In the following subsections, the test setup is identical to the one in the previous subsection, apart from the insertion loss that now adds up to 13.54 dB in total. This is the amount of attenuation that should be added to the level of attenuation that the VOAs are set to. Optical wavelengths are transmitted in both directions centred around 1563.0 nm and 1564.6 nm.

B.5.1 Multiple Waves at −1 dBm Total. Data points when multiple waves at a total power level of −1 dBm are introduced to the shared fibre.

Date	Time	QBER	SKR (bps)
2022-07-19	13:54:56	3.7900 %	83 000
2022-07-19	13:59:19	3.9000 %	80 000
2022-07-19	14:03:35	3.8100 %	84 000
2022-07-19	14:07:54	3.7700 %	86 000
2022-07-19	14:12:12	3.9300 %	79 000
2022-07-19	14:16:32	3.8300 %	82 000
2022-07-19	14:20:51	3.8400 %	81 000
2022-07-19	14:25:10	3.8900 %	77 000
2022-07-19	14:29:25	3.8800 %	81 000
2022-07-19	14:33:44	3.8400 %	82 000

Table B.5-1. Both VOAs set to 1 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-19	15:03:05	3.8100 %	40 000
2022-07-19	15:12:06	3.9500 %	37 000
2022-07-19	15:21:14	3.9600 %	36 000
2022-07-19	15:30:06	4.1000 %	36 000
2022-07-19	15:39:04	3.9100 %	38 000
2022-07-19	15:48:07	3.9500 %	37 000
2022-07-19	15:57:08	4.0700 %	37 000
2022-07-19	16:06:12	4.0900 %	35 000
2022-07-19	16:15:14	3.9700 %	38 000
2022-07-19	16:24:19	3.8100 %	39 000

Table B.5-2. Both VOAs set to 4 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-19	19:04:43	4.6300 %	15 000
2022-07-19	19:21:17	4.5300 %	17 000
2022-07-19	19:37:43	4.3600 %	18 000
2022-07-19	19:54:16	4.5200 %	17 000
2022-07-19	20:10:53	4.5600 %	16 000
2022-07-19	20:27:46	4.5700 %	15 000
2022-07-19	20:44:35	4.5300 %	16 000
2022-07-19	21:01:22	4.6000 %	15 000
2022-07-19	21:18:21	4.7100 %	15 000
2022-07-19	21:35:33	4.7300 %	14 000

Table B.5-3. Both VOAs set to 7 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-20	09:42:02	5.2800 %	7000
2022-07-20	10:09:12	5.2700 %	7000
2022-07-20	10:36:28	5.2900 %	7000
2022-07-20	11:03:30	5.4600 %	6000
2022-07-20	11:29:46	5.1500 %	8000
2022-07-20	11:56:29	5.3500 %	7000
2022-07-20	12:23:25	5.2200 %	8000
2022-07-20	12:50:24	5.2300 %	7000
2022-07-20	13:17:04	5.2400 %	7000
2022-07-20	13:43:46	5.1900 %	8000

Table B.5-4. Both VOAs set to 9 dB of attenuation.

B.5.2 Multiple Waves at 6 dB*m Total.* Data points when multiple waves at a total power level of 6 dBm are introduced to the shared fibre.

Date	Time	QBER	SKR (bps)
2022-07-20	16:32:13	4.0600 %	70 000
2022-07-20	16:36:54	4.0300 %	70 000
2022-07-20	16:41:41	3.9400 %	71 000
2022-07-20	16:46:29	4.0700 %	66 000
2022-07-20	16:51:12	3.9800 %	73 000
2022-07-20	16:55:52	4.0100 %	71 000
2022-07-20	17:00:34	3.9700 %	74 000
2022-07-20	17:05:23	4.0700 %	67 000
2022-07-20	17:10:14	4.2500 %	58 000
2022-07-20	17:15:06	4.2100 %	60 000

Table B.5-5. Both VOAs set to 1 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-20	17:54:44	4.2400 %	35 000
2022-07-20	18:03:16	4.4200 %	32 000
2022-07-20	18:12:00	4.2500 %	35 000
2022-07-20	18:20:29	4.3800 %	33 000
2022-07-20	18:28:58	4.4300 %	33 000
2022-07-20	18:37:46	4.4700 %	31 000
2022-07-20	18:46:23	4.3500 %	34 000
2022-07-20	18:54:54	4.3600 %	35 000
2022-07-20	19:03:32	4.2000 %	37 000
2022-07-20	19:12:05	4.2000 %	37 000

Table B.5-6. Both VOAs set to 4 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-20	19:59:52	4.8700 %	13 000
2022-07-20	20:16:49	4.8400 %	13 000
2022-07-20	20:33:54	4.6600 %	14 000
2022-07-20	20:51:02	4.9200 %	13 000
2022-07-20	21:08:01	4.7700 %	14 000
2022-07-20	21:25:12	5.0900 %	12 000
2022-07-20	21:42:12	5.0700 %	12 000
2022-07-20	21:59:09	4.8500 %	13 000
2022-07-20	22:16:15	4.9400 %	12 000
2022-07-20	22:33:07	4.8700 %	13 000

Table B.5-7. Both VOAs set to 7 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-21	04:37:49	5.2800 %	8000
2022-07-21	05:04:27	5.3500 %	7000
2022-07-21	05:30:56	5.4600 %	6000
2022-07-21	05:57:41	5.4100 %	7000
2022-07-21	06:24:32	5.2700 %	7000
2022-07-21	06:51:08	5.4000 %	6000
2022-07-21	07:17:23	5.3000 %	7000
2022-07-21	07:43:51	5.3500 %	7000
2022-07-21	08:10:23	5.3300 %	7000
2022-07-21	08:37:00	5.2000 %	8000

Table B.5-8. Both VOAs set to 9 dB of attenuation.

B.5.3 Multiple Waves at 9 dB*m Total.*

Data points when multiple waves at a total power level of 9 dBm are introduced to the shared fibre.

Date	Time	QBER	SKR (bps)
2022-07-21	09:30:17	4.2800 %	65 000
2022-07-21	09:34:33	4.2100 %	69 000
2022-07-21	09:38:50	4.2900 %	69 000
2022-07-21	09:43:12	4.4300 %	69 000
2022-07-21	09:47:31	4.1100 %	75 000
2022-07-21	09:51:47	4.1200 %	74 000
2022-07-21	09:56:03	4.1500 %	68 000
2022-07-21	10:00:20	4.1300 %	71 000
2022-07-21	10:04:37	4.1800 %	69 000
2022-07-21	10:08:56	4.1500 %	71 000

Table B.5-9. Both VOAs set to 1 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-21	11:25:38	4.4000 %	33 000
2022-07-21	11:34:02	4.4300 %	32 000
2022-07-21	11:42:35	4.8800 %	27 000
2022-07-21	11:50:58	4.6400 %	30 000
2022-07-21	11:59:14	4.8200 %	26 000
2022-07-21	12:07:38	4.6100 %	31 000
2022-07-21	12:16:00	4.5900 %	31 000
2022-07-21	12:24:25	4.4500 %	33 000
2022-07-21	12:32:52	4.7800 %	28 000
2022-07-21	12:41:23	4.8100 %	27 000

Table B.5-10. Both VOAs set to 4 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-21	13:12:15	5.0500 %	14 000
2022-07-21	13:27:20	5.0000 %	14 000
2022-07-21	13:42:27	5.0700 %	14 000
2022-07-21	13:57:31	4.9400 %	15 000
2022-07-21	14:12:48	5.0500 %	14 000
2022-07-21	14:27:58	4.8900 %	15 000
2022-07-21	14:43:25	4.9400 %	14 000
2022-07-21	14:58:45	4.8900 %	15 000
2022-07-21	15:14:05	4.9200 %	16 000
2022-07-21	15:29:25	4.8100 %	16 000

Table B.5-11. Both VOAs set to 7 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-22	03:37:47	5.8600 %	4000
2022-07-22	04:11:24	5.8500 %	4000
2022-07-22	04:45:09	5.8900 %	4000
2022-07-22	05:18:31	5.9100 %	3000
2022-07-22	05:52:08	6.0300 %	3000
2022-07-22	06:25:45	5.8000 %	4000
2022-07-22	06:59:17	5.9900 %	3000
2022-07-22	07:32:52	5.9000 %	4000
2022-07-22	08:06:25	6.0400 %	3000
2022-07-22	08:39:32	5.9300 %	3000

Table B.5-12. Both VOAs set to 10 dB of attenuation.

B.5.4 Multiple Waves at 12 dB*m Total.* Data points when multiple waves at a total power level of 12 dBm are introduced to the shared fibre.

Date	Time	QBER	SKR (bps)
2022-07-22	10:37:40	4.3700 %	68 000
2022-07-22	10:41:48	4.5600 %	64 000
2022-07-22	10:46:01	4.3500 %	69 000
2022-07-22	10:50:18	4.4700 %	64 000
2022-07-22	10:54:32	4.4000 %	65 000
2022-07-22	10:58:43	4.4500 %	64 000
2022-07-22	11:02:53	4.4000 %	71 000
2022-07-22	11:07:02	4.4300 %	67 000
2022-07-22	11:11:14	4.6100 %	60 000
2022-07-22	11:15:28	4.3600 %	68 000

Table B.5-13. Both VOAs set to 1 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-22	14:38:19	4.6400 %	31 000
2022-07-22	14:46:49	5.2500 %	23 000
2022-07-22	14:55:21	4.9100 %	26 000
2022-07-22	15:03:48	4.8600 %	26 000
2022-07-22	15:12:20	4.9100 %	26 000
2022-07-22	15:20:45	4.6700 %	29 000
2022-07-22	15:29:09	4.7200 %	28 000
2022-07-22	15:37:46	4.8100 %	27 000
2022-07-22	15:46:06	5.0500 %	25 000
2022-07-22	15:54:31	5.0300 %	21 000

Table B.5-14. Both VOAs set to 4 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-22	17:52:36	5.2700 %	11 000
2022-07-22	18:10:16	5.1900 %	11 000
2022-07-22	18:27:20	5.1000 %	12 000
2022-07-22	18:44:23	5.2000 %	12 000
2022-07-22	19:01:26	5.0700 %	13 000
2022-07-22	19:18:19	5.1800 %	12 000
2022-07-22	19:35:19	5.1800 %	11 000
2022-07-22	19:52:34	5.1800 %	11 000
2022-07-22	20:09:51	5.1800 %	11 000
2022-07-22	20:26:57	5.2000 %	11 000

Table B.5-15. Both VOAs set to 7 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-23	09:38:35	6.2000 %	2000
2022-07-23	10:11:35	6.1900 %	2000
2022-07-23	10:44:50	6.2500 %	2000
2022-07-23	11:18:02	6.1500 %	3000
2022-07-23	11:51:34	6.1600 %	3000
2022-07-23	12:24:42	6.1500 %	2000
2022-07-23	12:57:41	6.1000 %	3000
2022-07-23	13:30:48	6.2400 %	2000
2022-07-23	14:04:06	6.2100 %	2000
2022-07-23	14:37:23	6.0300 %	3000

Table B.5-16. Both VOAs set to 10 dB of attenuation.

B.5.5 Multiple Waves at 15 dB*m Total.* Data points when multiple waves at a total power level of 15 dBm are introduced to the shared fibre.

Date	Time	QBER	SKR (bps)
2022-07-24	10:21:02	4.8900 %	59 000
2022-07-24	10:25:08	4.9800 %	57 000
2022-07-24	10:29:20	4.9300 %	57 000
2022-07-24	10:33:31	4.8400 %	61 000
2022-07-24	10:37:43	4.9300 %	56 000
2022-07-24	10:41:55	4.9100 %	56 000
2022-07-24	10:46:07	4.9100 %	56 000
2022-07-24	10:50:18	4.9700 %	55 000
2022-07-24	10:54:27	4.8300 %	60 000
2022-07-24	10:58:40	5.1300 %	51 000

Table B.5-17. Both VOAs set to 1 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-24	11:33:25	5.3300 %	22 000
2022-07-24	11:41:54	5.1700 %	25 000
2022-07-24	11:50:21	5.2600 %	25 000
2022-07-24	11:58:54	5.0600 %	27 000
2022-07-24	12:07:27	5.2200 %	24 000
2022-07-24	12:15:43	5.2700 %	24 000
2022-07-24	12:24:25	5.1000 %	25 000
2022-07-24	12:32:59	5.1000 %	25 000
2022-07-24	12:41:23	5.1900 %	25 000
2022-07-24	12:49:49	5.1900 %	25 000

Table B.5-18. Both VOAs set to 4 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-24	13:20:14	5.6700 %	9000
2022-07-24	13:36:55	5.7900 %	7000
2022-07-24	13:53:41	5.6300 %	9000
2022-07-24	14:10:33	5.5500 %	10 000
2022-07-24	14:27:20	5.8100 %	7000
2022-07-24	14:44:14	5.7200 %	9000
2022-07-24	15:00:57	5.6700 %	9000
2022-07-24	15:17:48	5.7300 %	9000
2022-07-24	15:34:42	5.6900 %	9000
2022-07-24	15:51:34	5.7400 %	8000

Table B.5-19. Both VOAs set to 7 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-24	18:19:06	6.6600 %	2000
2022-07-24	18:53:10	6.8200 %	1000
2022-07-24	19:27:13	6.7000 %	1000
2022-07-24	20:00:50	6.7600 %	1000
2022-07-24	20:34:24	6.5900 %	2000
2022-07-24	21:07:41	6.7500 %	1000
2022-07-24	21:41:35	6.7500 %	1000
2022-07-24	22:15:14	6.7500 %	1000
2022-07-24	22:48:57	6.7900 %	1000
2022-07-24	23:22:50	6.6800 %	2000

Table B.5-20. Both VOAs set to 10 dB of attenuation.

B.5.6 Multiple Waves at 17.8 dB*m Total.* Data points when multiple waves at a total power level of 17.8 dBm are introduced to the shared fibre.

Date	Time	QBER	SKR (bps)
2022-07-13	13:56:00	5.5400 %	47 000
2022-07-13	13:59:56	5.5200 %	51 000
2022-07-13	14:04:02	5.4500 %	50 000
2022-07-13	14:08:09	5.4400 %	49 000
2022-07-13	14:12:14	5.5100 %	48 000
2022-07-13	14:16:17	5.3900 %	52 000
2022-07-13	14:20:24	5.4700 %	50 000
2022-07-13	14:24:21	5.4700 %	53 000
2022-07-13	14:28:26	5.5600 %	48 000
2022-07-13	14:32:33	5.4800 %	50 000

Table B.5-21. Both VOAs set to 1 dB of attenuation.

Date	Time	QBER	SKR (bps)
2022-07-13	16:30:19	8.1300 %	0
2022-07-13	17:12:24	8.1000 %	0
2022-07-13	17:55:01	8.1300 %	0
2022-07-13	18:37:34	8.1600 %	0
2022-07-13	19:20:14	8.1000 %	0
2022-07-13	20:02:08	8.0300 %	0
2022-07-13	20:44:31	8.0800 %	0
2022-07-13	21:26:32	8.1600 %	0
2022-07-13	22:08:59	8.1100 %	0
2022-07-13	22:51:05	8.1900 %	0

Table B.5-22. Both VOAs set to 11 dB of attenuation.