UNIQORN

Affordable Quantum Communication for Everyone

EU Horizon-2020 Project **UNIQORN**

Affordable Quantum Communication for Everyone:
Revolutionizing the Quantum Ecosystem from Fabrication to Application

EU Horizon-2020, FET Flagship on Quantum Technologies
Grant Agreement nº 820474

Document:	**Deliverable**	
Type:	Report	
Dissemination Level:	Public	
Title:	**Initial Specifications of UNIQORN Devices and Initial Definition of Application Scenarios**	
Work-Package / Task(s):	WP2 / T2.1	
Document number:	**D2.1**	Latest Revision: Version 1.2
Delivery Date Planned:	M04 / Jan. 2019	Pages: 46
Document Owner:	E. Hugues-Salas – UNIVBRIS	Label: D2_1_UNIQORN_Initial_Specifications_and_Application_Scenarios_Version-FINAL.doc
Contributors:	ALL	
Abstract:	This deliverable includes the initial specifications required for subsystems and network infrastructures as well as the proposed UNIQORN use cases and applications.	
Key words:	DPS, QRNG, SPAD, Squeezed Light, QKD, EPR, Entanglement, System-on-Chip, CV Receiver, SDN, ROADM, Whitebox, 5G, Oblivious Transfer, One Time Program, Coexistence	

Revision History

Version	Revision points	Version Author(s)	Date
1.0	Structuring	E.Hugues-Salas	03/11/2018
1.1	Co-Integration	E.Hugues-Salas	27/01/2019
1.2	Final updates and preparation for submission	H.Hübel	30/01/2019

Author List

Organisation	Name	Email
UNIVBRIS	E. Hugues-Salas	e.huguessalas@bristol.ac.uk
UNIVBRIS	G. Kanellos	gt.kanellos@bristol.ac.uk
UNIVBRIS	R. Nejabati	Reza.Nejabati@bristol.ac.uk
AIT	H. Hübel	hannes.huebel@ait.ac.at
UPB	H. Herrmann	Herald.herrmann@uni-paderborn.de
DTU	T. Gehring	tobias.gehring@fysik.dtu.dk
UNIVIE	P. Walther	philip.walther@univie.ac.at
UNIVIE	M.C. Röhsner	marie-christine.roehsner@univie.ac.at
MLNX	P. Bakopoulos	paraskevasb@mellanox.com
MLNX	G. Patronas	giannisp@mellanox.com
HHI	M. Kleinert	moritz.kleinert@hhi.fraunhofer.de
ICCS/NTUA	C. Kouloumentas	ckou@mail.ntua.gr
UIBK	H. Thiel	Hannah.Thiel@student.uibk.ac.at
UIBK	A. Schlager	Alexander.Schlager@uibk.ac.at
UIBK	G. Weihs	Gregor.Weihs@uibk.ac.at
TUE	X. Leijtens	X.J.M.Leijtens@tue.nl
POLIMI	F. Zappa	franco.zappa@polimi.it
COSM	F. Setaki	fsetaki@cosmote.gr

Reviewer List

Organisation	Name	Email
HHI	M. Kleinert	moritz.kleinert@hhi.fraunhofer.de
TUE	X. Leijtens	X.J.M.Leijtens@tue.nl

Copyright Statement

Funding Acknowledgement:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 820474:
UNIQORN quantum-uniqorn.eu

Table of contents

List of Figures

List of Tables

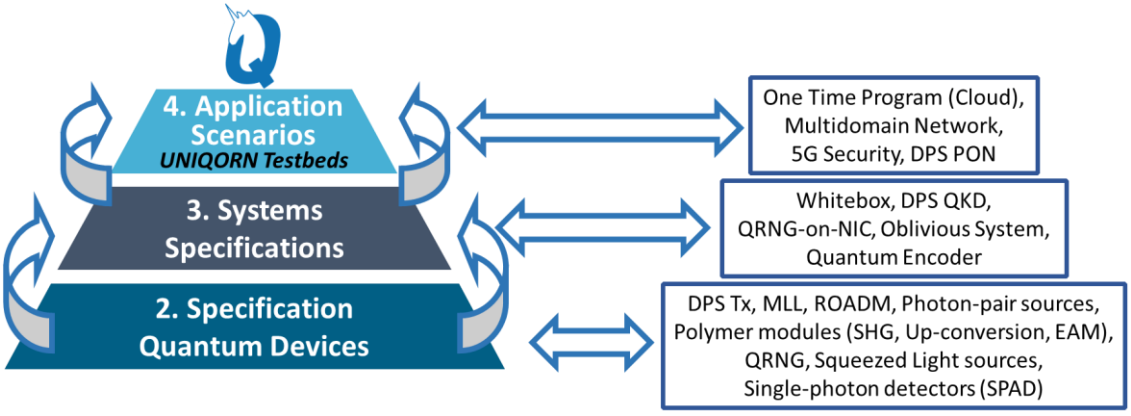
Executive Summary

The second quantum revolution is imminent and quantum communications is one of the main reasons since it has been identified as information-theoretical secure for data transmission. However, to achieve quantum communication networks, available compact and high-performance modules are needed together with deployed experimental testbeds for the evaluation of these modules with real application scenarios.

Under these premises, the Quantum Flagship UNIQORN project was designed aiming at early prototyping of components and system-on-chip implementations. In UNIQORN, complex systems will be integrated into highly miniaturized quantum-optic modules enabling quantum mechanical features such as entanglement and light squeezing. Moreover, these quantum technologies will be assessed in novel protocols such as oblivious transfer and one-time programs. To prototype these UNIQORN quantum technologies, field trials will be undertaken in city networks and the national dark fibre considering different real network scenarios.

This deliverable D2.1 includes the first steps towards these goals within the UNIQORN project. In D2.1, the main specifications of the UNIQORN quantum technologies are described based on the component and system functionalities of each technology. Initial set of parameters are defined, considering the technologies proposed with view on the integration of systems within potential quantum communication networks and applications. With regards to the applications, D2.1 list important scenarios where the quantum technologies developed in UNIQORN could be implemented.

The methodology used for this deliverable includes the discussion of the quantum devices contemplated within the UNIQORN framework. This will be the foundation for the systems that integrate the different technologies in order to achieve specific functionalities. In turn, the systems created in UNIQORN will be evaluated in field-trials. More importantly, very well-defined use cases will determine the usability of the quantum technologies proposed.



The first part of this deliverable D2.1 includes the description and initial specification of the quantum devices to be developed during the UNIQORN project. One of the quantum devices developed in UNIQORN is the differential phase shift (DPS) transmitter, which is specified in this D2.1. The DPS main building blocks are described considering its functionality and operation. Also, to convert wavelengths in the regime for photon-pair generation, a compact-size mode-locked laser is specified. To this end, different types of photon-pair sources are included in the D2.1, such as polarisation-entangled and time-bin sources. Add-on polymer modules are also specified in this document for different functionalities such as up-conversion, SHG and electro-absorption modulator.

The implementation of reconfigurable optical add/drop multiplexers (ROADMs) is also included within UNIQORN for routing telecommunication channels together with quantum channels and initial specifications are included in this deliverable. In addition, the design of quantum random number generators (QRNGs) is included in D2.1 and will exploit a microelectronic chip of Single-Photon Avalanche Diode (SPAD) arrays with 1x2 and 1x16 arrays of single-photon avalanche detectors (SPADs) and the implementation of a continuous-variable (CV) receiver is specified, considering the major challenge of manufacturing coherent detectors.

With regards to squeezed light sources, UNIQORN will follow two approaches in the design. One is based on a periodically poled lithium niobite (PPLN) waveguide and the other approach is based on a bulk PPKTP crystal. The initial specifications of such approaches are listed in this deliverable D2.1.

The second part of this deliverable D2.1 includes the system specifications. In this part, the design of a quantum white box is specified, with the main requirements listed. The main functionality of this quantum white box will focus on the flexible allocation of classical and quantum channels. Also, a DPS QKD system is briefly described in this document, as an integration of the previous work on DPS transmitters. Heralded single-photon sources described in this D2.1 will be built, during the UNIQORN project, with wavelength conversion capabilities based on PPLN waveguides. The specification of a QRNG integrated on a network interface card (NIC) is also described in here for practical evaluation in an operational system.

In addition to the previously mentioned systems, UNIQORN includes the design and specification of the oblivious and one-time program distribution systems, described in this D2.1. In this oblivious system, squeezed light sources will be used to implement an equivalent prepare-and-measure scheme. For the one-time program distribution system, UNIQORN contemplates the demonstration of a quantum information processing to execute and encode classical computation. Initial specifications are described in this document as well.

The third and final part of this deliverable D2.1 includes the UNIQORN application scenarios. One-time programs for cloud processing are detailed in this D2.1 with practical key performance indicators. These programs can be successfully applied with an arbitrarily high success probability in the implementation of one-time digital signatures. Oblivious transfer is also detailed in this document, aiming at the secure database access application.

With respect to optical networks, UNIQORN foresees the application scenarios of multidomain networking, 5G quantum security and DPS-based passive optical network (PON). For the case of the multidomain network, the operator's metro network of COSMOTE is used as a reference for study of potential coexistence of classical and quantum channels. Then, the networking infrastructure in Bristol is considered for evaluating this coexistence. Regarding the 5G quantum security scenarios, in UNIQORN different aspects are considered and the key performance indicators are listed in D2.1. These 5G quantum security scenarios considered comprise novel 5G fronthaul and backhaul designs, including Internet of Things (IoT) infrastructures secured by quantum communications.

1 Introduction

The UNIQORN project aims at developing key components for quantum communication systems. These components are differential phase-shift (DPS) transmitters, mode-locked laser modules, reconfigurable optical add/drop multiplexers (ROADMs), photon-pair sources, add-on polymer modules, quantum random number generator (QRNG), squeezed light sources, continuous-variable (CV) receivers, and Single-Photon Avalanche Diode (SPAD) detectors. Based on these components, main quantum systems will be assembled for further UNIQORN network-level integration. Systems such as quantum whiteboxes, DPS QKD, heralded photon sources, QRNG-on-Network Interface Card (NIC), oblivious system and one-time program distribution system (quantum encoder) are UNIQORN building blocks for heterogeneous quantum networks and applications. Moreover, in UNIQORN, selected quantum applications will be evaluated in laboratories and in field considering current and future network infrastructures. Scenarios such as one-time programs for cloud-based processing, oblivious transfer, multidomain networks, 5G quantum security and DPS passive optical networks (PONs) are foreseen as important applications to be tested and demonstrated during the UNIQORN project.

1.1 Purpose and scope of the document

Deliverable D2.1 contains the initial specifications of the devices and systems to be delivered within the timeframe of UNIQORN. Since the design of such devices and systems will be continuously progressing, this deliverable D2.1 is considered as a living document, meaning that regular updates will be taken into account considering feedback from the design and experiments of other work packages. Several key parameters are listed in this document D2.1 together with some approximations of their values to provide a reference of the work that will be delivered. With respect to applications, deliverable D2.1 will provide the initial set of scenarios considered in UNIQORN to demonstrate the capabilities of the devices and systems designed. These scenarios will respond to different key performance indicators (KPIs) included in this document D2.1 to evaluate the application in an objective manner.

1.2 Relation to other project work

Deliverable D2.1 will consider the feedback from other work packages (WPs). For the device designs, D2.1 will take into account feedback from WP3 and WP4. From WP7, D2.1 will consider the feedback of the experimental work. The output of task T2.1 will be the main provider of this D2.1 for a comprehensive set of documents summarizing all targeted network-level specifications for reference scenarios.

1.3 Structure of the document

The structure of deliverable D2.1 includes three main chapters: chapter 2 “Device Specifications”, chapter 3 “Systems Specifications” and chapter 4 “UNIQORN Application Scenarios”. In Chapter 2, sever subsections are included for different devices. Chapter 3 includes the explanation of six systems to be developed in UNIQORN. Chapter 4 contains five application scenarios that will be demonstrated during UNIQORN.

2 Device Specifications

2.1 DPS Transmitter

As shown in Figure 2-1, a DPS transmitter consists of an InP-based continuous-wave laser, which is phase-modulated by an exploiting the electro-optic effect of the material. The phase modulator is driven at symbol rate R_{sym} by a waveform generator according to random numbers. A Mach-Zehnder modulator might be used as pulse carver, used to remove transitions between subsequent symbols and thereby mitigating a security loophole. An optical attenuator is used to reduce the mean photon number per pulse μ to the order of magnitude 0.1. The pulse picker duty cycle will be around 2 (blanking):1(signal). A very high dynamic range of the attenuation is chosen in order to allow the transmitter to work in the quantum regime (single photon level) as well as at power levels that can be detected with classical PIN diodes.

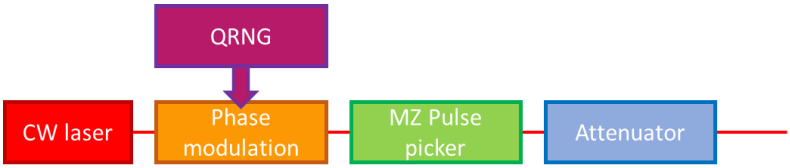


Figure 2-1. DPS Transmitter.

2.1.1 DPS Transmitter Specifications

For the DPS transmitter, the summary of the main specifications are described in table 2-1.

Table 2-1. DPS Transmitter Specifications

***I*. DPS Transmitter**			min	typ	max	Choice	Comment
EML/RSOA							
Wavelength	λ	nm		1550			
Linewidth	F	kHz	100	500	1000		
Optical power	P	mW		1			
Modulation							
Symbol rate	R	GHz		1			
V_π	V	V	0.1	0.5	1		
Mach-Zehnder pulse carver							
Extinction ratio	Ext	dB	10	20	30		
Attenuation							
Mean photon number per symbol	μ			0.1		0.1	
Dynamic range			30	40	45		

2.2 Mode-Locked Laser module

The pump lasers needed to create photon pairs around 1550 nm require their wavelengths to be around 775 nm. Since compact, pulsed laser sources with high repetition rates are not common at those wavelengths, UNIQORN pursues an approach whereby compact mode-

locked lasers will be produced in the project, that emit radiation at 1550 nm which is then converted to the 775 nm pump wavelength using second-harmonic generation (SHG) modules. For the packaging there are two options, either a fiber pigtail or direct bonding to the SHG chip. An on-chip SOA amplifier section will boost the power to around 15 dBm, this should guarantee enough pump power at 775 nm even after the SHG module.

2.2.1 Mode-locked laser

Table 2-2. Mode-Locked Laser Specifications

***I*. Mode locked laser**			min	typ	max	Choice	Comment
Wavelength	λ	nm	1540	1550	1560		
Pulse width	τ	ps	15	20	25		
Optical power	P	mW	1	1	1.5		
Amplified power	P_{amp}	mW	20	25	30		
Repetition rate	R	GHz	2	2.5	5		

2.3 ROADM

A reconfigurable optical add-drop multiplexer (ROADM) is widely used in optical telecommunication networks for routing different channels of light in WDM systems. Individual wavelengths carrying data channels can be added or dropped from a transport fiber without the need of signal conversion between optical and electronic domain. The main advantage of a ROADM over a fixed optical add-drop multiplexer (OADM) is the ability to reconfigure the add/drop wavelengths after the initial deployment of the system. Within the framework of UNIQORN, the quantum ROADM will work as a node for distributing the quantum entangled pairs produced by the time-bin entangled photon source. For this purpose, a 4 degree ROADM will be implemented, where the south port will act as the input port for the source.

The entangled photon source emits orthogonally polarized photon pairs near 1550nm wavelength in a rather broadband spectrum. Arrayed waveguide gratings (AWG) in the ROADM are utilized as optical multiplexers/demultiplexers to slice this broadband spectrum in four CWDM channels (λ_1 to λ_4). The channels lie symmetrically around the center, so that the entangled photons of a pair are separated in channels λ_1,λ_4 and λ_2,λ_3.

Since the entangled pair source has two spatial modes, the south port of the ROADM must have two inputs and therefore two AWGs, one for each polarization. Each photon of the pair can be then routed towards the output ports of the ROADM using 1×2 switches in the form of thermo-optically tuned Y-branch splitters. The four CWDM channels are recombined through AWGs at the output ports before exiting the ROADM.

The implementation of the ROADM is based on AWGs and 1x2 switches, which can be integrated on the PolyBoard platform. Ideally, we would like to have full connectivity and wavelength choice in the ROADM so that every wavelength pair of entangled photons can be distributed to any two-output port combination. This results in a ROADM design that comprises five AWGs and twelve switches, as shown in Figure 2-2. This design can be extremely challenging due to the number of components and the large number of waveguide crossings that features. Lower design complexity can be achieved with a ROADM design that offers reduced connectivity. This design is implemented with five AWGs and four 1x2 switches as shown in Figure 2-3, while keeping full wavelength choice.

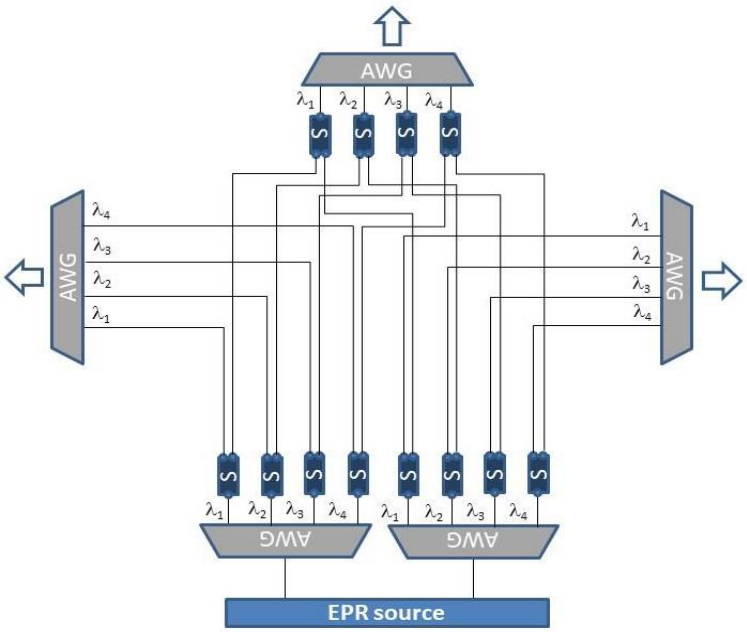


Figure 2-2. First quantum ROADM design offering full connectivity and wavelength choice.

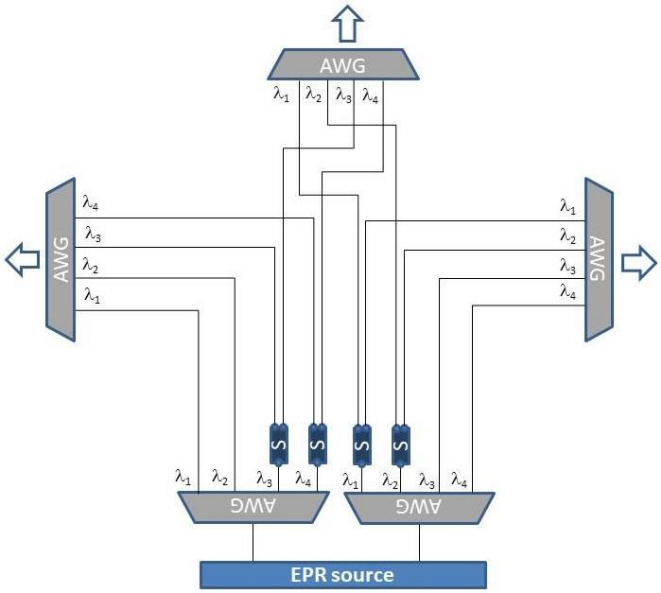


Figure 2-3. Second quantum ROADM design offering reduced connectivity, while keeping full wavelength choice.

In both versions of the quantum ROADM, good operation is based on the assumption of the very low polarization sensitivity of the PolyBoard platform. Although this is true, the platform can still feature low polarization dependence, which can affect the performance of the ROADM to a certain extent. In order to eliminate this problem, a polarization rotator can be inserted in one of the two input ports, enabling the operation of the ROADM with a single polarization state (provided of course that the EPR source is attached to the ROADM and the interconnection between the two modules is realized with the use of polarization maintaining (PM) fibers.

2.3.1 ROADM Specifications

Table 2-3. ROADM Specifications

***I.* ROADM**	min	typ	max	Choice	Comment
Number of WDM channels	-	-	-	4	-
Node degrees	-	-	-	4	-
Channel spacing	-	-	-	To be defined	-
Fiber-to-Fiber loss (dB)	5	6	7	-	-
Cross-talk between WDM channels	25	30	35	-	Depending on the channel spacing

2.4 Photon-pair sources

2.4.1 Photon-pair source

A photon-pair emitter is the main building block for almost all entangled and heralded photon sources. In essence it constitutes of a nonlinear material which when excited by a pump laser converts some of the pump photons into photon pairs. The most widely used processes are spontaneous parametric down conversion (SPDC) and four-wave mixing in materials with $\chi^{(2)}$ and $\chi^{(3)}$ optical nonlinearities. The individual photons of the pair are often referred to as *signal* and *idler*. After the creation of the photon pair, the signal and idler photons are separated using either polarization or spectral distinguishability.

Due to its simplicity, the photon pair source will be the first source module to be integrated on the polymer platform in UNIQORN. This source will produce highly asymmetric photon pairs with the signal wavelength at 810nm and the idler wavelength at 1550nm. The assembly is pumped with a cw-laser at 532nm [Hübel-2007]. For the first chip design both, signal and idler photons, will be coupled from the polymer chip into single mode fibers to characterise the performance of the source. In a first generation the pump is coupled via a polarization maintaining fiber to the polymer substrate. In further iteration cycles, direct coupling of the pump from a laser chip to the PolyBoard is foreseen, if proper laser chips are available.

The type-0 phase-matched SPDC process will take place in a ppLN crystal with inscribed waveguides generating the non-degenerate photon pair with parallel polarisations Low-loss waveguides fabricated by Ti-indiffusion enable an efficient butt-coupling to the PolyBoard. Quasi phase-matching is obtained by periodical domain inversion (periods around 6 µm). Fine-adjustment is accomplished using temperature tuning. During operation the chip temperature must be stabilized to about 0.1 °C.

Due to the strong confinement in the waveguide, only small pump powers in the order of tens of µW of pump power inside the waveguide are needed. Precise alignment between the waveguides on the polymer and the inscribed waveguide on the ppLN crystal is needed to result in low coupling losses and high heralding efficiencies. To accomplish this, the ppLN crystals are inserted into etched grooves on the PolyBoard. The pump light will be coupled directly into the ppLN waveguide without intermediate polymer waveguide. At the output of the crystal, signal and idler wavelengths are coupled into a polymer waveguide supporting both wavelengths. The vertical alignment between polymer and ppLN waveguide is defined by the precisely etched groove on the PolyBoard chip. In the lateral direction, the crystal is aligned actively with respect to the polymer waveguide. Heater elements in the PolyBoard below the ppLN crystal allow for the localized setting of the required operating temperature.

Signal and idler photons are split on the chip using a dichroic mirror. Care needs to be taken to remove all residual pump light especially in the signal arm where single photon detectors will be used (on and off chip) which are sensitive the wavelength of both signal and pump light. This

will be accomplished by a high reflective coating for the pump at the ppLN waveguide facet and special long pass filter with high attenuation at the pump wavelength (OD>12).

Adaptation to include a detection module for the signal photons directly on the polymer substrate will be discussed in section 3.3.

Table 2-4. Photon Pair Source Specifications

***I.* Photon pair source**			min	typ	max	Choice	Comment
Parameters							
Wavelength pump	λ	nm		532			
Pump Power	P	mw		1			
Wavelength signal	λ	nm		810			
Wavelength idler	λ	nm		1550			
PDC bandwidth (idler)	Δλ	nm		1			
Coupling loss ppLN to polymer (signal, idler)	η	dB		1	2		
Coupling loss polymer to single mode fiber (signal, idler)	η	dB		1	2		
Long-pass filtering of pump light	OD	dB		12			
Source brightness	B	c/s/mW/THz		3×10^8			

2.4.2 Polarisation-entangled photon source

In the course of the UNIQORN project, we will build a source of polarization-entangled photon pairs based on the scheme published in [Laudenbach-2017]. We will configure it to emit photons in a state:

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

which is known to be anti-correlated in any basis. As we plan to use this source for a communication protocol where one photon will be measured locally while the other one will be deployed to a potentially distant client we have chosen to implement a source of photon pairs with very different wavelengths optimised for their respective applications. The photon manipulated and measured locally will be created at a wavelength in the vicinity of 800 nm since for this wavelength comparatively cheap and efficient single photon APDs exist.

As the other photon of the pair will have to be sent to a client in a potentially distant location, our main concern is to minimize the photon loss in this transmission. Thus, we would like the wavelength of this photon to be in a telecom band, which allows for low loss when the photon is transmitted through a fiber.

Fortunately, there was recent work by [Laudenbach-2017] showing how polarization entangled photon pair sources with very degenerate wavelengths can be built. The choice of exact wavelength is a trade-off between available pump laser, effective detection at the short wavelength and low-loss transmission for the long wavelength photon.

One thing that should be considered is that In this kind of source narrow filtering in at least one of the arms is required to ensue indistinguishability of the two down-conversion processes and thus high fidelity with the desired maximally entangled state.

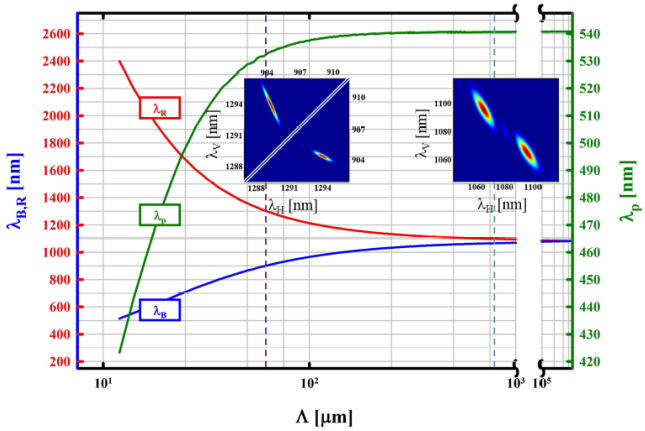


Figure 2-4. Possible combination of pump, signal, and idler wavelengths [Laudenbach-2017]

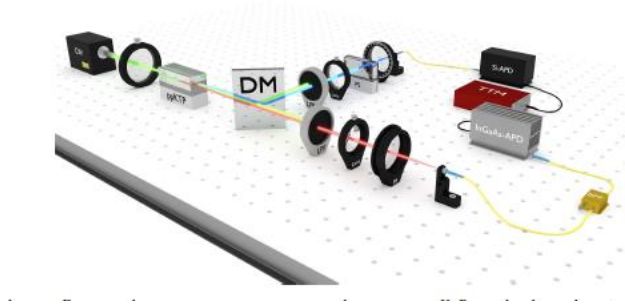


Figure 2-5 General outline of polarisation-entangled photon source [Laudenbach-2017]

For our implementation (building upon our previous work in [Roehsner-2017]) we have chosen the following the parameters for the source of Table 2-5.

Table 2-5. EPR (Polarisation-Entangled Photon) Source Specifications

***I.* EPR SOURCE**	Comment
Pump: • 515.095nm • spectral bandwidth 0.057nm • power: up to 100mW Crystal: • ppKTP • 30mm • Poling period: 33.53μm • Temperature: 50°C Single Photons • 1512nm • 781.24nm • Filter 0.45nm in the 1512 arm	These are parameters currently planned for our bulk experiment The source isn't finished or fully tested yet They were chosen for practical reasons mentioned in the text above

2.4.3 Time-bin entangled photon source

The time-bin entangled photon pair source is based on AlGaAs Bragg-reflection waveguides (BRW), which are either pumped by a laser source near 775 nm wavelength or directly electrically excited. The BRWs produce photon pairs near 1550 nm wavelength in a rather broad band between 1500 and 1600 nm. Because the two photons of a pair are orthogonally polarized, they are split by an on-chip polarizing beam splitter to be routed towards the two outputs. The outputs may be preceded by AWGs that separate the photons into DWDM channels so that channels that lie symmetrically around the center receive entangled photons of a pair, respectively. The time-bin entanglement is achieved in the case of laser pumping by an on-chip interferometer, which splits the pump laser pulse into two coherent copies separated by about 200 ps. In the case of direct electric excitation, the BRW-internal laser will be pulsed by two successive current pulses, so that the optical phase between them remains coherent. Due to the fast time-response extremely short delay interferometers can be used resulting in a size reduction from the current optical breadboard arrangement of about 60x30 cm^2 for the preparation and analysis interferometers to an effective chip size of perhaps 1x0,5 cm^2, which is a linear reduction of 1/60 and an area reduction of 1/3600. Neither device is commercially available as a standard component at this time.

The target of this source is to allow DWDM-compatible DV QKD between virtually arbitrary pairs of users given dynamic DWDM channel switching.

Table 2-6. EPR (Time-bin Entangled Photon) Source Specifications

***I.* EPR SOURCE**			min	typ	max	Choice	Comment
Parameters							
Wavelength	λ	nm	1500	1550	1600	Preferably higher wavelengths	The spectral bandwidth of our photon pair source is typically around 100 nm broad. Hence, we can choose the desired wavelength by spectral filtering.
Power	P	dB		Single Photons			Roughly hundreds of thousands of counts per second. Depends on the power of the pump.
Internal losses	dB/mm		2	2.2	5		Not measured for active samples. We expect the losses to be below 10 dB/mm for active samples.

2.5 Add-on polymer modules

2.5.1 Up-conversion module

The aim of the up-conversion module is to provide a small device capable of changing (up-converting) the wavelength of incoming single-photons to a lower wavelength. In particular the device aims to convert single-photons in the C-band (around 1550nm) into single photons towards the visible part of the spectrum. The advantage gained thereby is of course the detection of the C-band photons with integrated CMOS SPADs rather than the direct detection

using bulky and expensive InGaAs APDs or SSPDs. The target is not so much to increase overall detection efficiency but to provide a cheap and miniaturised detector for single-photons at telecom wavelengths. In UNIQORN, such an up-conversion module will be designed based on sum-frequency generation inside a waveguide inscribed ppLN crystal on the polymer platform.

Previous results on up-conversion detection done by several groups revealed that a long wavelength pumping is preferable, i.e. the strong pump should be at a wavelength which is much longer than the wavelength of the photon to be converted [Pelc-2011]. If a shorter pump wavelength is used, strong additional noise occurs mainly due to up-conversion of photons generated either by Raman scattering or by spurious non-phasematched SPDC both generated by the strong pump signal.

As the PolyBoard technology does not support waveguiding at long wavelengths due to absorption of the polymer, the ppLN device will be placed at the input of the module and directly connected to the input fibers. On the ppLN chip pump and signal paths are combined by means of a wavelength dependent directional coupler ("pump coupler") followed by the periodically poled section for the conversion process. At the output facet of the ppLN chip a specifically tailored dielectric mirror suppresses the transmitted pump beam. Subsequent filtering is performed in the PolyBoard by inserting proper high-pass and bandpass filters. Thus, the module will feature just the sum-frequency generation on the poly-board, together with the appropriate filtering. In this instance the strong pump field will be generated off-chip in an external laser source and launched with optical fibers into the ppLN chip. Similarly, the detection of the short wavelength signal will also be performed off-chip with fiber coupled Si-APD modules.

A second generation should integrate as well microelectronic CMOS chips containing the Si-SPADS on the polymer board. Care has to be taken to minimise stray light and provide for sufficient filtering of the pump light to minimise background counts at the Si-SPAD pixels.

Table 2-7. Up-Conversion Module Specifications

***I.* Up-Conversion module**			min	typ	max	Choice	Comment
Parameters							
Wavelength pump	λ	nm		>1700			Selection of the final pump wavelength depends on the availability of suited pump modules
Pump Power	P	mW		100			
Wavelength signal	λ	nm		1550			
Wavelength up-converted photon	λ	nm	810	850	880		
Intrinsic efficiency		%		50			
Total system efficiency	η	%		10			

2.5.2 SHG pump module

The aim of the SHG module is to provide a polymer-based solution to convert pump light at 1550nm, where different kinds of laser modules are available to 775nm where the light can act as a pump for SPDC processes. Using the initial wavelength of 1550nm would result in photon pairs with wavelengths in the 3 μm range for which there are currently no applications in quantum communications. In UNIQORN there are modules planned which either operate in cw-mode or enabling the frequency doubling of short, i.e. ≈20 ps long, pump pulses.

In the first generation of the SHG modules the pump light will be coupled via fibers to the modules. In the second-generation modules the pump lasers at 1550nm should be directly coupled to the PolyBoard. For the pulsed-laser SHG modules, the generated SHG output will be coupled into a single mode fiber. The first generation of the cw module will also couple the SHG to a fiber and in a final version, the cw SHG module will be integrated with the squeezing crystal on the same PolyBoard.

To maximise the conversion efficiency waveguide inscribed crystals will be incorporated onto the polymer board. Internal conversion efficiencies for the cw laser will be > 10%, whereas the pulsed laser will achieve 20% SHG efficiency. Since the original pump pulse is close or exactly at the wavelengths of the single photons produced by the SPDC, great care has to be taken to remove all pump light (1550nm) at the output of the SHG stage before the SHG is used as pump in the SPDC crystal. This pump suppression is obtained with specifically tailored dielectric coatings at the output facet of the ppLN waveguide and additional low pass filters in the subsequent PolyBoard stage.

Table 2-8. SHG Module Specifications.

***I.* SHG module**			Min	typ	max	Choice	Comment
Parameters 20-ps pulse pump							
Wavelength pump	λ	nm		~1550			
Pump Power @1550nm	P	mW		10			
Pump pulse width	τ	ps		20			
Pump rep. rate		GHz		2.5			
Pump Power @775nm	P	mW		2			
SHG efficiency		%		20			
Parameters cw pump							
Wavelength pump	λ	nm		1550			
Pump Power @1550nm	P	mW		100			
Pump Power @775nm	P	mW		10			
SHG efficiency		%		>10			

2.5.3 Electro-Absorption modulator

The EAMs are based on graphene layers that are directly integrated with the polymer waveguides during the fabrication process. By employing two graphene layers insulated by a dielectric layer with a thickness of approx. 50 nm, the optical absorption in the graphene layers can be tuned. In the EAM section the light will be coupled from the polymer waveguide into a silicon nitride ridge waveguide in order to reduce the mode filed diameter and enhance the graphene-light interaction. Electrical contacts facilitate the biasing of the EAM and depending on the applied voltage, the optical transmission can be tuned from an absorbing into a transparent state.

Using this approach, optical extinction ratios of 10 dB at optoelectronic bandwidths of 10 GHz are targeted. Due to the linear energy dispersion relation of graphene and the wide

transparency of the polymer waveguides, the EAMs are able to operate across a broad wavelength range from 1250 nm to 1600 nm.

Table 2-9. Electro-Absorption Modulator Specifications

***I.* Electro-Absorption modulator**			min	typ	max	Choice	Comment
Parameters							
Operating wavelength	λ	nm	1250	1550	1630		
Optical input power	P	mW		1	10		
DC offset voltage	V_{DC}	V			15		
Driving voltage	V_{RF}	V		4	6		
Bandwidth	f_{3dB}	GHz		10			
Extinction ratio	ER	dB		10			

2.6 QRNG

To generate a truly random number, which cannot be reconstructed by a third party, the intrinsic uncertainties in quantum mechanical measurements can be employed to realise a quantum random number generator or QRNG. In principle, a QRNG is made up of 2 essential parts. The first one, also called the entropy source consists of a quantum system with some random physical quantity and the measurement equipment that reads these random variables and yields the raw bit string, which might still include bias and correlations between the events. The postprocessing block takes the raw bits and distils a shorter sequence without correlations. For example, the task includes the elimination of double click events (when both SPADs fired, in a 1x2 SPAD implementation), biases in detection or splitting ratio, and an overall entropy extraction to achieve a uniform output sequence [Herrero-2017].

A QRNG will be developed using the random output path of a photon impinging on a beamsplitter. A pulsed laser will create photon pulses with MHz repetition rate, which are attenuated to near single photon level using static and adjustable attenuators on the polymer board. The adjustable attenuator is based on a Y waveguide branch equipped with heating electrodes. By locally heating on of the output waveguides, the splitting ratio can be tuned. In combination with a further heating section, the optical power in the heated optical path is suppressed by more than 70 dB at a wavelength of 1550 nm. This structure can be cascaded in order to achieve higher attenuations. The photon pulse is then split on an adjustable 50:50 beamsplitter with the two output paths connected to fibers for off-board detection. The first module for such QRNG will consist only of the adjustable attenuator and beam splitter, with both the pulsed laser and the Si-SPAD modules off the polymer board.

Integration with the NIC adaptor will be trough external programmable digital electronics, which reads in the raw bit string from the Si-SPAD array chip. On-board processing power will be used for post-processing, the final random bit string is provided via a suitable interface and can be forwarded to the NIC for Usage. The programmable digital electronics should also trigger the pulsed pump laser and, if needed, will generate a gate pulse for the Si-SPAD detectors. The SPAD array chip will host some counting functionality to extract the information of the triggered pixel and to properly signal multi detection events. Preliminary digitisation of the triggers of the SPADs will also be performed on chip.

2.6.1 QRNG with 1x2 SPAD array

In the second integration step the pulsed laser (785nm) will be added to the polymer platform The laser is pulsed again in the MHz range using an external trigger signal. Detection of the

pulses after the beamsplitter is now integrated on the polymer as well. A 1 x 2 SPAD detector (either two modules or a single chip) will detect the photons from the two output ports and generate a signal which is further processed through a FPGA board. Since the SPADs are front illuminated, a packaging methodology needs to be developed to feed the electronic contacts, which are on the same side, around the optical input and make them accessible. The same SPAD integration methodology as for the other polymer modules will be used. Output from the PolyBoard is designed to accept either a fiber array (250μm) or direct butt-coupling to the SPAD array chip.

2.6.2 QRNG with 1x16 SPAD array

To increase the generation rate of the QRNG without changing the laser repetition rate, the number of possible paths will be increased from two to sixteen pixels. A 1x16 Si-SPAD array chip will be developed to detect all sixteen channels. Since there are 16 possibilities for a detection event, the number of raw bits per pulse is increased to 4 bits per pulse. The main challenge will be the integration of the SPAD array chip with all electrical and optical contacts in the correct places to facilitate packaging of the PolyBoard-SPAD assembly. The 1x16 SPAD array chip will be tested on a FPGA board, to check the correct sensing of the triggered pixel and the extraction of the raw random stream for further processing.

2.6.3 QRNG Specifications

Table 2-10. QRNG Specifications

***I.* QRNG**			min	typ	max	Choice	Comment
Parameters							
Wavelength	λ	nm		785			
Repetition rate	R	MHz	1	5	10		Depending on SPAD deadtimes
Fixed attenuators	OD	dB		30	40		Depending on power of laser diode
Adjustable attenuator	OD	dB		1-10			
Beamsplitter splitting ratio		%	45:55	50:50	55:45		The splitting ratio will be adjustable
Number of Channels	N		2	2-16	16		Two implementations with 1x2 and 1x16 SPAD detectors (either modules or array chips)

2.7 Squeezed Light Source

Squeezed light is a quantum state of light, which exhibits a lower noise variance than a regular coherent state in one of the quadrature amplitudes of the electromagnetic field, at the expense of a larger noise variance in the conjugate one. Squeezed light has many applications in quantum metrology, computing and communication. It can for instance be used to improve certain aspects of continuous-variable quantum key distribution systems and to implement quantum cryptographic primitives like oblivious transfer. The most successful generation systems are based on parametric down-conversion using the second order nonlinearity of a crystal. The performance of the squeezed light generation and the application of squeezed light depends critically on low optical loss – a challenge in the design of systems on a chip.

A squeezed light source consists of a nonlinear material like periodically poled potassium titanyl phosphate (PPKTP) or lithium niobate (PPLN) in an optical cavity. The UNIQORN squeezed

light module will embed this cavity on the polymer interposer. Two different approaches to the design of the squeezing source will be pursued:

1. A PPLN waveguide with coated endfaces for defining the cavity. This waveguide couples directly to the polymer waveguide on one side and to a single-mode fibre or the polymer waveguide on the other.

2. A bulk PPKTP crystal sandwiched between GRIN lenses with coated endfaces. The GRIN lenses serve to focus the light to/from the polymer waveguides down into the crystal. The output is similarly coupled to either polymer of single-mode fibre (via free space).

The nonlinear materials require temperature control to achieve phase matching in the nonlinear process. An optical cavity for both the squeezed light (at 1550 nm) and the pump beam (at half the wavelength, 775 nm), enhances the process so that less pump power is required. Optical loss inside the cavity has to be absolutely minimized to obtain a useful amount of squeezing.

The squeezed light source has to be pumped with 775 nm light, which is generated by the SHG module from 2.5.2. A reference tone (for instance at 40 MHz) indicating the squeezed quadrature has to be inserted into the squeezed light source and phase locked to the pump.

2.7.1 Squeezed Light Source Specifications

Table 2-11. Squeezed Light Source Specifications

***I*. Squeezed Light Source**			min	typ	max	Choice	Comment
Parameters							
Squeezed Light Wavelength	λ	[nm]		1550			
Laser Linewidth		kHz		<1			
Pump wavelength	λ	[nm]		775			
Reference tone		[MHz]		40			Frequency shifted laser beam, e.g. by acousto-optical modulator
Coupling loss, cavity to single-mode fibre		dB		0.5			
Intra-cavity loss		dB			0.3		
Squeezing level		dB		-4			Measured after direct outcoupling from edge of polymer board
SHG pump power		mW			100		
Pump threshold power		mW		100	200		

2.8 CV Receiver

A CV receiver is a coherent detector, which measures the quadrature components of incoming light signals. This is done by mixing the light signal with a strong classical reference beam, usually referred to as local oscillator, at a balanced beamsplitter. The of the beamsplitter are measured by PIN diodes which convert the optical power to an electric current. The current difference between the two PIN diodes is proportional to the *I* or *Q* quadrature, depending on the LO's phase. This current difference is amplified to a measurable voltage by a transimpedence amplifier (TIA). The electronic noise caused by the TIA and the saturation limit of the PIN diodes are the main limitations for the detector's clearance, i.e. the ratio between the

shot noise (measured by LO) and the electronic noise. One of the major challenges in the manufacturing of coherent detectors is keeping the clearance low even for high frequency ranges, i.e. electronic bandwidths.

2.8.1 CV Receiver Specifications

Table 2-12. CV Receiver Specifications

***I.* CV RECEIVER**			min	typ	max	Choice	Comment
Parameters low-noise receiver:							
Frequency Range	F	GHz	0.01	0.1	10	1	
Clearance	C	dB	6	16	30	25	
Efficiency	η		0.5	0.8	1	0.99	
Common-mode rejection ratio	CMRR	dB	20	30	50	≥ 40	
Local oscillator relative intensity noise	RIN	dBc/Hz	-180	-130	-100	≤ -130	
Parameters high-speed receiver:							
Frequency Range	F	GHz	0.01	0.1	10	10	
Clearance	C	dB	6	16	30	16	
Efficiency	η		0.5	0.8	1	0.9	
Common-mode rejection ratio	CMRR	dB	20	30	50	≥ 40	
Local oscillator relative intensity noise	RIN	dBc/Hz	-180	-130	-100	≤ -130	

3 System Specifications

3.1 Quantum White Box

The use of white boxes in optical networks has attracted increasing interest over the last years to allow node disaggregation and interoperation of modules from different suppliers, enabling network optimisation and reducing costs [Sambo-2018, Velasco-2018]. White boxes have also been considered an important component for data centres since white boxes prove advantageous for server's configurations [Robinson-2018]. Practical white box solutions have recently become available such as the Facebook solution named "Voyager", which is considered the first white box transponder and routing solution [Lyubomirsky-2016]. This Voyager unit includes a packet transponder and open line transport system with open optical specifications enabling any user to contribute to the systems, components and/or software. In addition, this Voyager node system allows open and programmable network architectures.

Based on the previous definition, a white box has to comply with the following requirements:

- Disaggregation of network functionalities: Be built with discrete, open subsystems and interfaces that allow individual configuration and integration
- Allow system programmability to support varied applications
- Support vendor-agnostic integration and interoperability

3.1.1 White Box Design and Requirements

As part of the UNIQORN project, the design of a quantum white box (QWB) will allow for effectively and flexibly handling and routing the quantum and the classical signals simultaneously in advanced optical network topologies.

Specifically, the UNIQORN QWB will consider the following application scenario:

i. *Full mesh optical network*. The QWB will support a full-mesh topology both for classical and quantum channels

ii. *Dynamic Network.* The UNIQORN QWB will allow dynamic network configuration in terms of topology, traffic allocation and resource allocation.

iii. *Quantum and Classical Channels Coexistence*. The QWB designed and implemented in UNIQORN will allow for co-existence of classical and quantum channels. In the first implementation scenario, optical links for quantum and classical channels will be physically separated to allow seamless transmission of quantum channels. However, all signals will use the same routing elements in the nodes. The second version will consider co-existence of quantum and classical channels in the same fiber.

In order to support the above networking application scenario, the QWB will be designed to support "Add/drop/passthrough" functionalities, where the QWB will employ the fundamental quantum ROADM component designed in section 2.3 to arbitrarily add and drop quantum and classical ports.

In essence, the UNIQORN QWB will support the traditional ROADM functionalities of add/drop, pass-through and regeneration (repeater). However, for the purpose of the quantum channels, these functionalities will be adapted to the quantum processes in order to support the quantum protocols which will be integrated in the add/drop and regeneration functions. In addition, in this QWB architecture, reconfigurability is critical and the QWB must allow the quantum and classical components to be added or removed on demand, according to network design

considerations. To this end, a backplane platform can be considered (e.g. optical cross-connect, wavelength selective switch, arrayed waveguide grating router, etc.) to enable the plug-in or unplugging of components.

3.1.2 Quantum Whitebox Architecture.

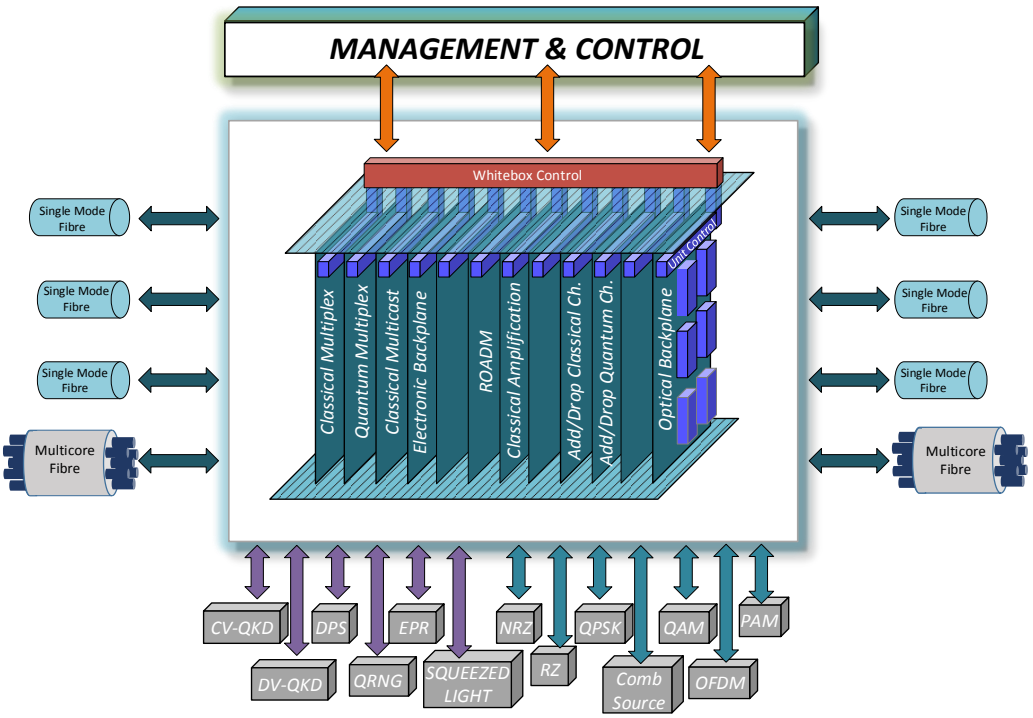


Figure 3-1: Quantum Whitebox architecture.

Figure 3-1 shows a generic architecture of the proposed quantum Whitebox. In this whitebox, several operational units provide the functionalities to support the quantum and classical network applications. The ROADM functionalities will allow add and drop processing as well as pass through of classical and quantum signals. Basic multiplex of channels for both quantum and classical signals will be also undertaken in the QWB to transmit/receive signals to/from the optical fibres interfaced. An optical backplane will be integrated for dynamic synthesis of components and for interconnections from components to ports.

Each unit will include a control block, which will interface to the centralized control of the QWB. This centralized QWB management and control platform will also be responsible for the communication with other QWBs.

3.1.3 Quantum Whitebox Specifications

Table 3-1 shows the main parameters required for the Quantum Whitebox.

Table 3-1. Quantum Whitebox Specifications

***I.* Quantum WhiteBox**			min	typ	max	Choice	Comment
Number of Line Ports			1		6		Node degree considered is 6
Number of Client Ports			40				Reference standard ROADM (e.g. ADVA FSP 3000)

3.2 DPS QKD

3.2.1 DPS QKD Specifications

The phase-encoded quantum states travel from the transmitter (Sec. 2.1) to the receiver in a commercial telecom silica fibre. The receiver consists of a delay interferometer i.e. a beamsplitter (BS) followed by two optical paths with different travel time which are recombined at a second BS whose two output ports are monitored by InGaAs single-photon detectors. The respective detectors will register a photon event depending on the relative phase between two subsequent pulses. According to which detector was triggered, Bob will assign a bit value to each photon event. After sifting out unregistered pulses (due to optical loss or limited detection efficiency), Alice and Bob compare a significant fraction of their bit strings over an authenticated classical channel in order to estimate the quantum-bit error rate (QBER). If the QBER remains under a certain threshold, they proceed with error correction and privacy amplification in order to distil a secure key.

Table 3-2. DPS QKD Specifications

***I.* DPS QKD**			min	typ	max	Choice	Comment
DPS Transmitter							
Key Rate	K	b/s	1		20		
DPS Receiver							
Bandwidth	B	GHz	12.5		100		
Insertion Loss	l_L	dB	0.1		0.6		

3.3 Heralded single-photon source

Single-photon heralding is most widely realised using photon-pair generation by spontaneous parametric down-conversion (SPDC). The photons are separated into different spatial modes by virtue of to their optical wavelength, polarisation or scattering angle. Detection of one photon reveals the presence of the other and its availability for further quantum-information processing. UNIQORN aims to build a heralded photon source with wavelength conversion 532 nm → 810 nm + 1550 nm based on PPLN waveguides integrated into a polymer-based PIC (see Sec. 2.4.1 for further description and specifications). The 810 nm photon will be detected directly on chip using a CMOS-integrated Silicon single-photon avalanche diode (SPAD) with optical interface to the polymer waveguide. After implementation and evaluation of a first heralded photon source, we aim to implement four LN waveguides each connected to an individual Si-

SPAD. Simultaneous pumping SPDC sources increases the probability of a successful photon-pair event even with limited optical power per source (exaggerated power per source would cause detrimental multi-pair emissions). The Si-SPADS will trigger an optical switch or and electro-absorption modulator (Sec. 2.5.3) to let pass the heralded 1550 nm photon (or block it in case multiple heralding events were triggered at the same time). Moreover, we will evaluate the feasibility of polymer-based bandpass filters to suppress spectral correlations between signal and idler and thereby increase the spectral purity and the interference visibility of the 1550 nm photons.

Table 3-3. Heralded Single-Photon Source Specifications

***I*. Heralded single-photon source**			min	typ	max	Choice	Comment
SPDC source							
Wavelength pump	λ	nm		532			
Pump Power	P	mw		1			~10 μW inside the waveguides
Wavelength signal	λ	nm		810			
Wavelength idler	λ	nm		1550			
Coupling loss ppLN to polymer (signal, idler)	η	dB		1	2		
Coupling loss polymer to single mode fiber (idler)	η	dB		1	2		
Long-pass filtering of pump light	OD	dB		12			
Source brightness	B	c/s/mW/THz					
Si-SPADs							
Quantum efficiency	η			0.15			
Dark counts	DC	Hz		< 50			
Timing jitter	J	ps		200			
Heralding efficiency							
without bandpass filters	η_{herald}			0.75			
with bandpass filters	η_{herald}			0.1			

3.4 QRNG on NIC

The target of the QRNG on NIC task is to demonstrate the seamless integration of experimental quantum devices, such as the Uniqorn QRNG, with commercial equipment; exploiting this way the true quantum randomness in a realistic networking security scenario. The current security schemes (as well as many other applications) assume the capability of the network devices to generate truly random numbers, rendering the introduction of QRNGs into communication networks the first and most feasible step towards quantum secure communications.

The following paragraphs describe the integration of the Uniqorn QRNG in a classical IP network via the MLNX BlueField smartNIC. The Bluefield SmartNIC, high-level schematic shown in Figure 3-2, is an innovative and high performance programmable networking engine that comes in different speeds, numbers of CPU cores and PCIe widths; from dual-port 25GbE PCIe Gen4.0 x8 to dual-port 100GbE PCIe Gen4.0 x16, supporting 4/8/16 Arm cores.

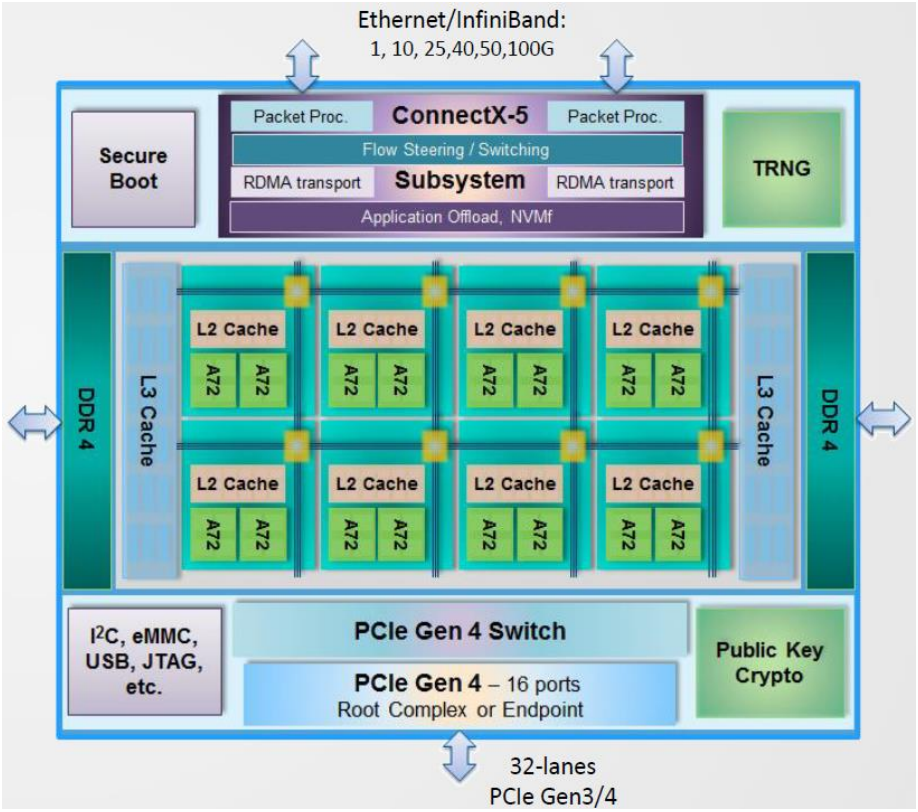


Figure 3-2. Bluefield high level schematic

Bluefield SmartNIC combines hardware encryption accelerators with embedded software and fully integrated advanced network capabilities, making it an ideal platform for developing proprietary security applications. It includes Arm v8 (64-bit) cores that provide cryptography extensions (A64, A32 and T32 instructions) for AES, SHA-1, SHA-224 and SHA-256. Moreover, it utilizes dedicated hardware for Public key exchange (RSA, Diffie-Hellman, DSA, ECC, EC-DSA and EC-DH) and for the generation of random numbers (True Random Number Generator with entropy source).

The QRNG transfers the random numbers to the SmartNIC via a serial digital interface such as USB or I2C. Since each random number created by the QRNG is 4-bit long, which is shorter than the random numbers used by modern security protocols, multiple QRNG outputs will be concatenated to reach the required size. The true random numbers are transferred in a continuous fashion from the QRNG to the SmartNIC and they are stored in a “random numbers pool” in the SmartNIC’s memory. The integration of the QRNG in a realistic scenario with the classical security protocol stack (e.g. public key exchange and encryption according to IPsec) will be realized using the BlueField’s hardware and software functions, while bypassing the onboard Random Number Generator and retrieving true random numbers from the “random numbers pool”.

Figure 3-3 depicts the main building blocks for the end-to-end ecosystem including the proposed QRNG on NIC. The two hosts are network devices that need to exchange data over a secure IP network. The security related functions are offloaded to the BlueField SmartNICs; an example of a common security scheme involves the Diffie–Hellman key exchange and the IPsec authentication and encryption. The random numbers required by the security protocols for the establishment of a secure connection are generated by the Uniqorn QRNG, providing this way stronger security and demonstrating the seamless integration with a real communications network.

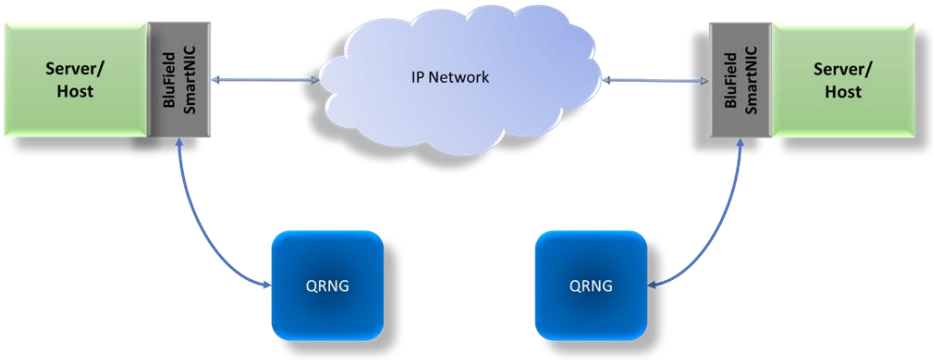


Figure 3-3. End-to-end demonstration of QRNG integration

3.4.1 QRNG Specifications

Table 3-4. QRNG on NIC Specifications

***I*. QRNG on NIC**			min	typ	max	Choice	Comment
NIC							
Host interface	B_H	Gb/s	1		138		x16/x8 PCIe Gen 3.0/4.0
Network interface	B_N	Gb/s	1		100		*2xQSFP28 ports*
QRNG							
Repetition Rate	B	MHz	1	5	10		Depending on SPAD deadtimes

3.5 Oblivious System (OS)

The continuous variable implementation of 1 out of 2 random oblivious transfer is described in our recent paper [Furrer-2018]. In the following, we first give a short summary of oblivious transfer and summarize its implementation. We will also give some information about alternative implementations if the required specifications on the on-chip quantum source cannot be met.

Oblivious transfer is a basic cryptographic primitive that involves two parties, Alice and Bob, who do not trust each other. The two parties thereby want to be ensured that the other party cannot cheat or maliciously influence the outcome. The goal of the oblivious transfer protocol is the following:

Alice has two messages and Bob wants to learn one of them according to his choice. The oblivious transfer protocol guarantees that Bob learns only one of the two messages but not both. The protocol also guarantees that Alice does not learn which of the messages Bob learned.

The security of oblivious transfer against malicious parties can only be obtained in the noisy storage model. The noisy storage model restricts the power of Bob by limiting the amount of quantum memories he possesses and by making assumptions on their efficiency and excess noise.

Oblivious transfer has been demonstrated in proof-of-principle experiments with discrete variables [Erven-2014] and continuous variables [Furrer-2018]. Our previous proof-of-principle experiment using continuous variables is based on Einstein-Podolsky-Rosen entanglement. The entanglement source generates entanglement by interfering two squeezed states with a pi/2 phase shift on a balanced beam splitter. One of the output modes of the beam splitter was kept

by Alice while the other was distributed to Bob. Both parties performed homodyne detection with a random choice between two orthogonal quadratures.

In Uniqorn, we will implement an equivalent prepare-and-measure scheme instead of using entanglement. In the prepare-and-measure scheme, a squeezed state is randomly prepared with amplitude or phase squeezing and displaced according to a Gaussian distribution.

The implementation will use the squeezed light source implemented on the PolyBoard and combined with an additional phase modulator for the pump beam for quadrature shifting. The output of the squeezed light will be displaced by coherent states. After transmission to Bob, we will perform homodyne detection using the CV receiver developed in this project. The random choice of quadrature and the randomness required for the displacements will be generated using the QRNG on NIC.

For successful implementation, the overall loss must be lower than 30% including channel, transmitter and receiver loss. This constitutes an outstanding challenge but will be solved by dedicating special efforts on reducing losses at the two stations. As an alternative to CV oblivious transfer, we will also consider a discrete variable version based on polarization entanglement combined with a BB84 detector [Erven-2014]. These technologies are also developed within UNIQORN. Using this approach to oblivious transfer the stringent loss condition is however traded with stringent requirements on the quantum bit error rate, which must be lower than 1 % [Erven-2014].

3.5.1 Oblivious System Specifications

Table 3-5. Oblivious System Specifications

***I*. Oblivious System**			min	typ	max	Choice	Comment
Overall Efficiency	QE	%	70		100	80%	
Receiver Vacuum Noise to Electronic Noise Clearance			dB	20			
Wavelength		nm		1550			
Symbol rate		kHz	100	500	1000		
QRNG		bit		10			Required bits per symbol.

3.6 One-time Program Distribution System – Quantum Encoder

In our recent paper [Roehsner-2017], we describe and motivate our protocol for a quantum advantage for probabilistic one-time programs. This document contains a short summary and motivation.

Let's start with the problem statement shown in Figure 3-4:

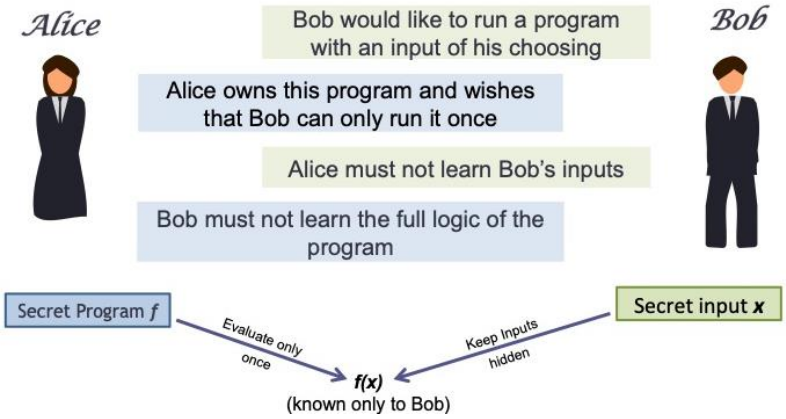


Figure 3-4. Problem statement: A sender Alice and A receiver Bob would like to allow Bob to compute f(x) while not disclosing f or x to the respective other party

This problem can be solved using a one-time program (first introduced in [Goldwasser-2008]). Which we describe in our paper as follows: One-time programs are a computational paradigm that allows for functions that can be executed one time and one time only. Thus, if a software vendor encodes a function f as a one-time program, a user having only one copy of that program can obtain only one input-output pair (x; f(x)) before the program becomes inoperable. In the classical world, this is only possible through the use of one-time hardware or one-time memories [Goldwasser-2008], special purpose hardware that is physically destroyed after being used once. However, it is unclear whether such hardware can be realised in an absolutely secure way. An adversary may attack the specific implementation, seeking to circumvent or reverse whatever physical process is used to disable the device after a single use. Certain features of quantum mechanics, such as the no-cloning theorem [Wootters-1982], [Dieks-1982] and the irreversibility of measurements [Von Neumann-1955], suggest that it may enable a solution to this problem. It was recently shown, however, that deterministic one-time programs are impossible even in the quantum regime [Broadbent-2013]. As a result, it is believed that neither classical nor quantum information-theoretically secure one-time programs are possible [Goldwasser-2008], [Broadbent-2013], [Aaronson-2009], [Mayers-1997], [Lo-1998], [Hayashi-2006] without further assumptions [Liu-2014], [Liu-2015], [Erven-2014], [Yao-1982]. Here, we demonstrate theoretically and experimentally that quantum mechanics does enable a form of probabilistic onetime program, which shows an advantage over any possible classical counterpart. These rely on quantum information processing to execute but encode entirely classical computation. Such probabilistic one-time programs circumvent existing no-go results by allowing a (bounded) probability of error in the output of the computation. We show that these quantum one-time programs offer a trade-off between accuracy and number of lines of the truth table read, which is not possible in the classical case. Remarkably, the experimental requirements to encode the probabilistic one-time programs we introduce are comparable to those of many quantum key distribution implementations, allowing for technological advances in that field to be harnessed for a new application.

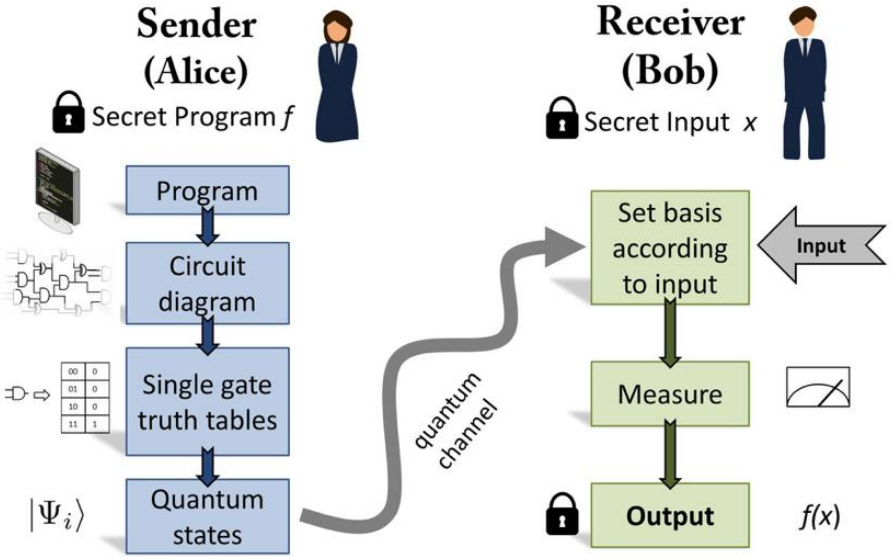


Figure 3-5. General scheme of the one-time programs where a classical software is encoded onto quantum states which allow a one time and one time only execution.

3.6.1 Quantum Processor Specifications

Table 3-6. Quantum Processor Specifications

***I.* Quantum Processor**			previous implementation	planned improved setup	Comment
Gate rate	R_G	Hz	0.24	1000	
Pump Wavelength	λ_P	nm	394.5	515	
Distance Alice - Bob	d	m	0.5	700	Through an underground fibre connecting different buildings
Wavelength single photons	λ_S	nm	789	781&1512	

4 UNIQORN Application Scenarios

4.1 One Time Programs for Cloud-Based Processing

4.1.1 Description of the Application

In principle our scheme can be used to encode any classical function and implement it in a one-time manner (e.g. to use it to implement the Millionaires Problem as shown in our paper [Roehsner-2017]). In this case, the probabilistic nature of the individual gates should always be considered.

An example of an application that can succeed with an arbitrarily high success probability (at the price of sending more quantum information) is our implementation of one-time digital signatures. This allows a sender Alice to delegate one-time power of attorney to Bob (he can sign one and only document in her name). This is achieved by sending multiple copies of one-time programs able to encrypt the hash the message of Bob's choice (the one-time programs

encrypt using Alice's private key and the hash of the message is the input to the program) and certifying that the expected number of programs gives the correct output before the signature is accepted. The principle of the digital signature is shown in the Figure 4-1.

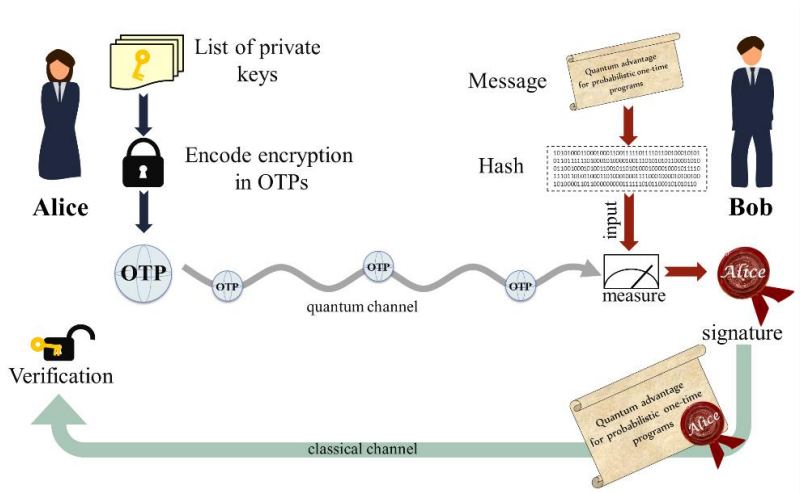


Figure 4-1. Description of the digital signature scheme.

4.1.2 Components and Functionalities. Mapping to UNIQORN

In our paper we have shown the first proof-of-principle implementation of such programs. The main challenge in our implementation was the low gate rate due to losses and active switching. Furthermore, due to the chosen wavelength Alice and Bob had to be in the same lab (losses in a long fibre would have been too high). Thus, our work within the unicorn project will aim to increase the gate rates while adapting the setup to the requirements of a sender and receiver in more distant locations only connected by a standard telecom fibre.

To implement one-time programs, we require a few central building blocks:

- Source: a source of single photons or photon pairs (photon pairs might be necessary for heralding or remote state preparation)
- State Preparation: A way to (randomly) prepare the four gate states we require to build arbitrary programs
- Detectors: Efficient single photon detectors
- Quantum channel: A (ideally low loss) quantum channel between Alice and Bob (e.g. an optical fibre)
- Measurement: A way for Bob to (randomly) measure in one of two mutually unbiased bases
- Evaluation: Some classical logic and post processing

During the course of the UNIQORN project we aim to improve this first implementation significantly by using a modified approach. We will use a source of entangled photons to perform remote state preparation from Alice to Bob. Using this new source and by adapting the program design we will be able to remove any need for active switching from the implementation. This will allow us to increase the gate rate significantly.

4.1.3 Requirements and Key Performance Indicators

Table 4-1. KPIs for One Time Programs for Cloud Processing

***I.* Key Performance Indicator**		
Fidelity		0.95
Gate rate	Hz	1000
Single gate success probability	%	>0.8

Note: Since our states will not be prepared directly but by remote state preparation it might be slightly lower than in the previous experiment.

4.2 Oblivious Transfer

4.2.1 Description of the Application

Oblivious transfer is a basic cryptographic primitive, which can be used to implement any two-party cryptographic protocol. One possible application is secure database access. Here, a user has access to N entries in a database according to his permission profile. The user would like to access one of the N entries but likes the database to be oblivious about which one he accessed.

The above-described application can be implemented with 1 out of N oblivious transfer. Our system performs 1 out of 2 random oblivious transfer, i.e. the messages held by Alice are random. 1 out of 2 oblivious transfer can be constructed from its random version by XORing the actual message with the oblivious message [Erven-2014]. 1 out of N oblivious transfer can be constructed from 1 out of 2 [Naor-1999].

4.2.2 Components and Functionalities. Mapping to UNIQORN

The main system components are:

1) Source: A squeezed light source including a laser and a second-harmonic generator, all three developed in UNIQORN emitting squeezed light.

2) Detector: A continuous variable homodyne detector comprising a local oscillator, a balanced beam splitter and two high efficiency photo diodes and a transimpedance amplifier for read-out.

3) A quantum random number generator generating random bits for quadrature choices and displacement.

4) Post-processing: The post-processing software performs error reconciliation and privacy amplification.

4.2.3 Requirements and Key Performance Indicators

Table 4-2. KPIs Oblivious Transfer

***I.* Key Performance Indicator**		
Overall Quantum Efficiency	%	80
Symbol Rate	kHz	500

4.3 Multi-domain Network

4.3.1 Description of the Application

The QWB of section 3.1 will be leveraged for the multidomain network application. In this application, quantum channels will coexist with channels originated from different networks (e.g. access, metro, core, data centre). The QWB will also include multi-dimensional connectivity, in which multicore fibre (MCF)-based spatial division multiplexing (SDM) will be used (within laboratory testbeds), as well as wavelength division multiplexing (WDM).

4.3.2 Components and Functionalities. Mapping to UNIQORN

As a starting point, a practical operator's network configuration will be considered for the coexistence studies. To this end, the metro network topology of COSMOTE in Greece will be used as a reference to provide the initial parameters of the classical network for the coexistence in a subsequent stage. Figure 4-2 shows COSMOTE's network topology which includes three main optical rings interconnected via a 4-degree node and two 3-degree nodes.

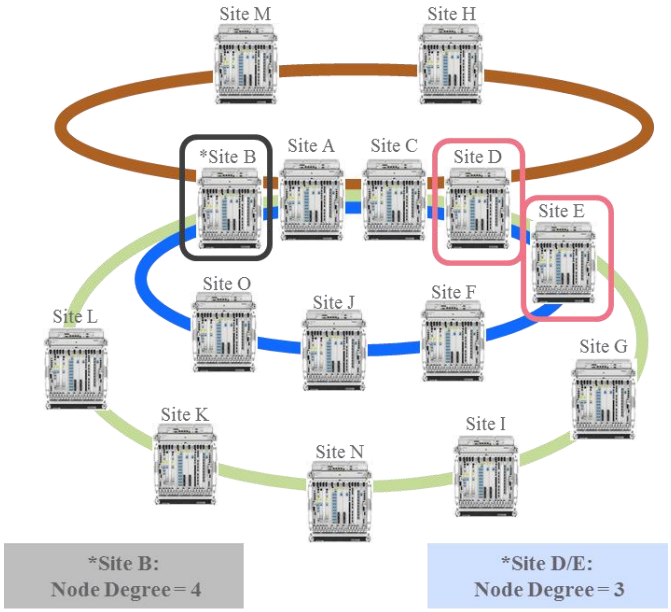


Figure 4-2. COSMOTE's Network Configuration

In summary, COSMOTE's network includes 15 sites with optical add/drop multiplexers interconnected with standard single-mode fibres for a total of 17 links. A maximum number of 44 channels (wavelengths) is available per link with 100GHz wavelength spacing. The average length per link is 13km with an average loss of 7.5dBs. With respect to launching powers of the classical channels, the average total power of the set of wavelengths is 8.7dBm and the launch power per wavelength is -5.4dBm, with an OSNR of 16.9dB. The network includes channels using OTN (OTU-2 and OUT-4) protocol as well as Ethernet 10GbE/100GbE. Optical amplifiers in the links with functionalities such as pre-amplifiers, boosters and in-line amplifiers are installed in the sites of the network together with dispersion compensation modules.

In UNIQORN, parts of COSMOTE's network topology will be emulated considering the critical nodes and links for coexistence in between classical and quantum channels. To achieve this network emulation, network components in Bristol, UK, will be contemplated (Figure 4-3). For instance, the UK National Dark Fiber Infrastructure Service (NDFIS) [NDFIS-2014] will be considered, with optical fibre connectivity between Bristol, Southampton, London and Cambridge.

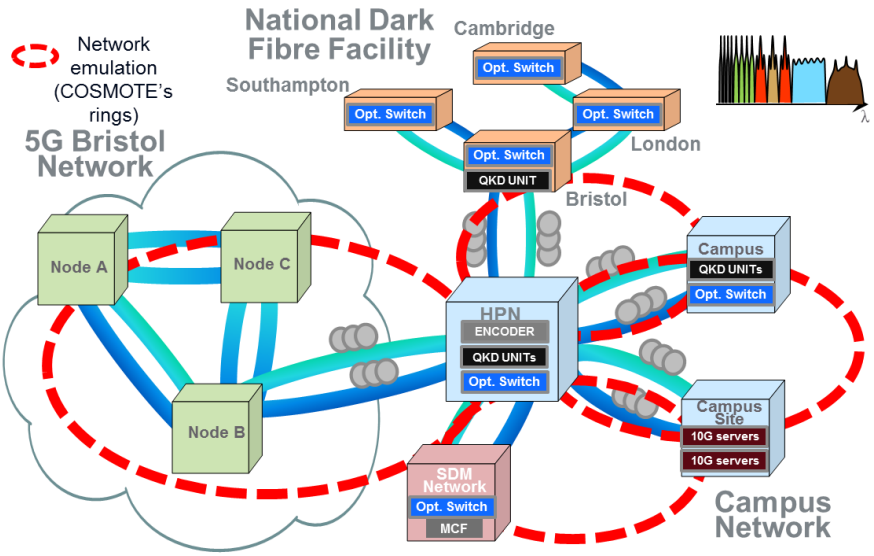


Figure 4-3. Network facilities in Bristol (UK) for network emulation.

UNIQORN partner UNIVBRIS directly maintains the following NDFIS sites:

- University of Bristol site, located in the High Performance Networks (HPN) laboratory.
- Bradley Stoke site, located within Bristol area and within an industrial park.
- Froxfield Site, located in the countryside, in between Bristol and London.

NDFIS allows the use of the infrastructure in a scheduled basis and access to interconnection and colocation sites is possible to temporarily install equipment that complies with EMI standards and regulations. In addition, UNIVBRIS maintains the SDN controller of NDFIS. The controller used is OpenDayLight (ODL) version Lithium, and the optical switches include an OpenFlow 1.0+ agent, which enables the communication with the centralized SDN controller.

Also, from the HPN laboratory, connectivity to the 5G Bristol metro network could be available with dark fibre links to different sites. A DV-QKD system (Alice and Bob) is available as well as optical switches and wavelength selective switches (WSS) in the UNIVBRIS infrastructure. In addition, within the University campus, interface to a 7-core multicore fibre is available as well as 24 fibre pairs with 200m length connected to a HPN lab colocation site. In addition, bandwidth-variable transmitters (with DP-QPSK and 16-QAM), for classical channel emulation as well as layer 2 Encoder/Decoder (10G) are included in the UNIVBRIS experimental setup.

In addition, UNIQORN aims to provide an embedded artificial intelligence (AI)-enhanced SDN mechanism to support coexistence of classical and QKD channels over the same medium efficiently, to support slicing and allow composition and operation of multiple QKD services in the same metro-network. In this scenario, interoperability between different classical channel patterns and different QKD systems will be validated. The work on [Ou-2018] will be used as a reference to this AI application (Figure 4-4).

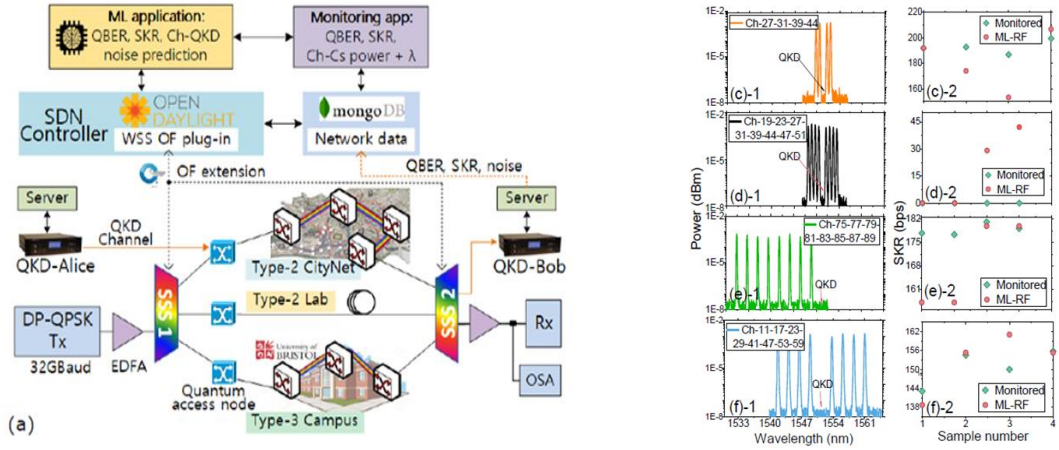


Figure 4-4. Machine learning-assisted QKD networking

As shown in [Ou-2018] the coexistence of classical and a DV-QKD channel is enabled over the campus and city network infrastructure, and quantum parameters (e.g. SKR and QBER) are used to allow a machine learning application to predict the optimum channel allocation and to reconfigure the optical spectrum channel plan by using the provided SDN controller.

UNIQORN technologies (e.g. EPR sources, CV-QKD, DPS, etc) could be integrated in this AI framework, using the developed QWBs and monitoring quantum parameters related to the components designed. For instance, the quantum ROADM of section 2.3 will be used as a component of the QWB to enable the coexistence of classical and quantum channels. The QRNG (section 2.6), squeezed light source (section 2.7) and the CV receiver (section 2.8) could be synthesized in the QWBs to enable different functionalities and performances in the quantum network.

4.3.3 Requirements and Key Performance Indicators

Table 4-3. KPIs Multidomain Network

***I.* Key Performance Indicator**		
Number of Classical Channels		20
Number of Quantum Channels		5
Wavelength Offset Ch-C/Ch-QKD	nm	1.6
Optical Power Range (Ch-C)	dB	-25 to -15
QBER (Ch-QKD) @25km DV-QKD	%	3%
SKR (Ch-QKD) @25km DV-QKD	b/s	500b/s
QBER (Ch-QKD) @50km CV-QKD	%	3%
SKR (Ch-QKD) @50km CV-QKD	b/s	10kb/s
QKD Types		DV-QKD, CV-QKD
Protocols		BB84, COW

4.4 5G Quantum Security

4.4.1 Description of the Application

In 5G, security is fundamental to deliver successful 5G networks across a wide range of industry verticals to enable new 5G services and use cases [5GAmericas-2018]. For instance, 5G will enable *IoT* with applications such as city sensors (e.g. temperature, humidity, air pressure, etc.). In this new IoT network, multiple devices generate data that is forwarded to a specific IoT gateway. This process corresponds to the lifecycle of IoT, which includes the devices, the network, the final endpoint and the user application. However, several security flaws can appear in this process and the use of secure quantum keys will be beneficial, since the properties of quantum mechanics will be used inherently with photons to transfer a shared secret key between two entities.

In UNIQORN, 5G security will be considered under several scenarios: *i)* a secure 5G fronthaul design will be provided, considering different technologies and approaches, *ii)* a new design of a 5G backhaul platform will be demonstrated, considering components at the edge of the 5G network and *iii)* to deal with the security need of IoT in a 5G infrastructure, UNIQORN will include a full stack framework based on SDN which initially discovers IoT devices and provisions them to an IoT platform, considering quantum encryption over the IoT gateway, securing the entire payload that will be transmitted. Low-cost quantum-secured IoT technologies developed in UNIQORN will be also evaluated in this 5G Testbed (e.g. DPS transceivers).

4.4.2 Components and Functionalities. Mapping to UNIQORN

Fronthaul - Secure Fronthaul Protocol Implementation

During UNIQORN, quantum security in the fronthaul design of the Radio Access Network (RAN) is foreseen since remote radio heads (RRHs) are connected to a baseband unit (BBU) pool with optical fibres to enable high data transmission. Security breaches are possible at the protocol level requiring advanced methods to guarantee the confidentiality of the data.

To this end, in the UNIQORN project we will include the design and implementation of quantum security-QKD for relevant fronthaul protocols. Figure 4-5 shows the main components of this implementation where a field programmable gate array (FPGA) will enable different channels to be encrypted and decrypted, using a quantum key generated by a QKD process. Different channels will also be enabled, following multiplexing and demultiplexing over a single fibre or with dedicated optical fibres.

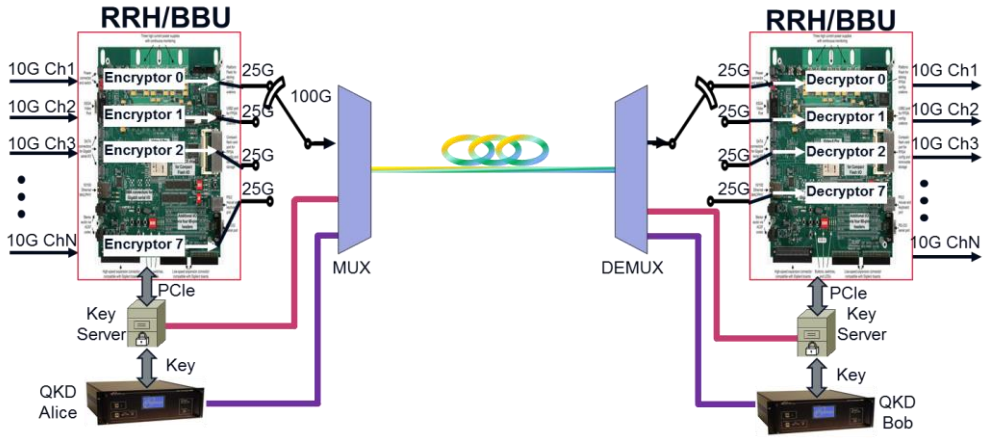


Figure 4-5. 5G Fronthaul Implementation

Backhaul - Secure Compute Nodes Network demonstration

In UNIQORN we will propose and demonstrate a design of a platform for 5G backhaul, which is secured by QKD. QKD will enable the generation of symmetrical keys, which will be used to secure information in transit. Figure 4-6 shows the backhaul infrastructure, which includes

computing nodes with optical switches, QKD units and servers. These nodes will be interconnected with each other and the cloud servers via the optical switches and optical fibres.

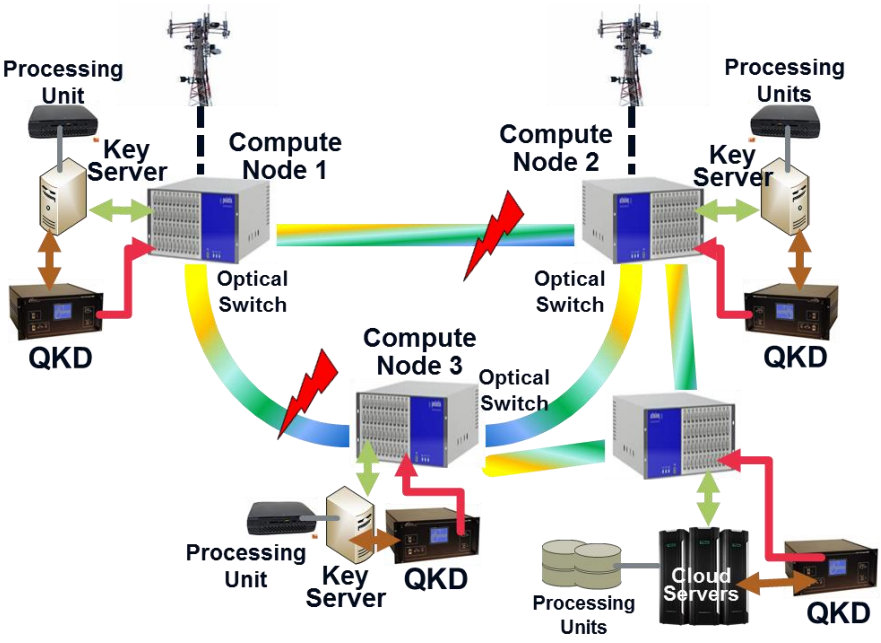


Figure 4-6. 5G Backhaul Demonstration

QKD IoT

In UNIQORN, the security in an IoT platform will be considered within an end-to-end 5G ecosystem. An initial step towards this IoT security has been proposed in [Mavromatis-2018] in which a software-defined IoT network is integrated with fibre-based QKD technology to provide the IoT devices with quantum-secure keys to enhance their battery lifetime. The use of off-the-shelf DV-QKD systems was presented through a field trial network infrastructure to establish a secure connection between a server that represents the data centre and IoT devices. In [Mavromatis-2018], QKD served both as an enhanced key source mechanism relying on quantum true random generation and as a secure mechanism to distribute the keys through the optical network to the IoT gateways and then the IoT devices, thus completely replacing the embedded key generation processes otherwise present in current IoT networks. Figure 4-7 shows the architecture of the integrated optical QKD system and IoT network.

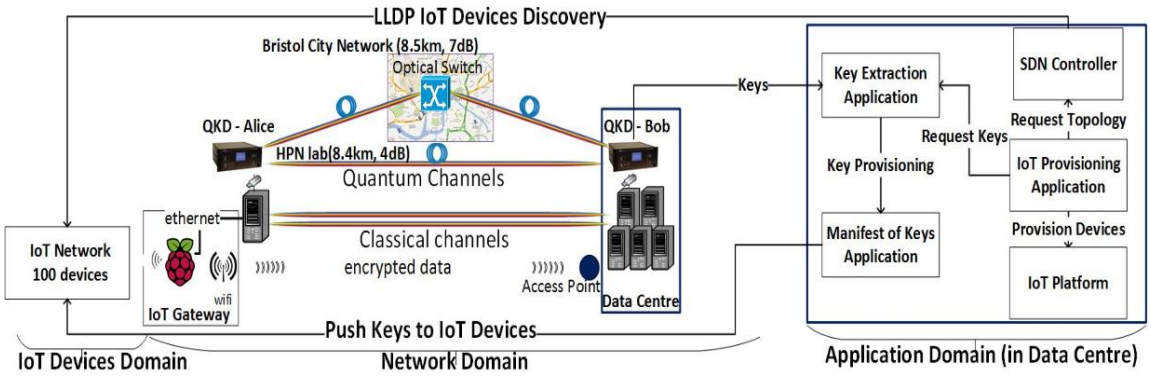


Figure 4-7. Architecture of the integrated optical QKD system and IoT network

4.4.3 Requirements and Key Performance Indicators

Table 4-4. KPIs 5G Quantum Security

***I.* Key Performance Indicator**		
Number of IoT devices		20
Number of QIoT devices		5
Type of QIoT devices		DPS transmitter
Quantum Security Protocol		BB84
IoT security Protocol		HTTPS
Power Efficiency Improvement	%	10-20%
Secret Key Rate (Gateway link)	b/s	1800
QBER (Gateway Link)	%	<4%

4.5 DPS-based Passive Optical Networks

4.5.1 Description of the Application

The use of quantum channels within the deep fiber infrastructure to secure the encryption of optical data flows will be targeted within UNIQORN. The goal of multiplexing weak DPSQKD signals with strong classical data streams through shared passive optical topologies remains a great challenge due to the restrictions linked with the Raman noise photons [Fröhlich-2015]. Within UNIQORN, the integration of PIC-based, low-cost DPS-QKD pairs with the deployed Upstream/Downstream (US/DS) traffic profiles will be pursued for advanced encryption data-layer encryption for optical network users. The targeted UNIQORN quantum access network structure will be based on the use quantum transmitters, which will be placed at the network endpoints (ONTs) while the required complex optical hardware of single-photon detectors will be hosted at the centralized node at OLT [Fröhlich-2015]. Moving one step forward, the targeted classical/quantum integration strategy will also focus on the use of shared optical hardware to serve the needs of classical US/DS PON traffic and quantum key exchange. The DPSQKD transmitter prototypes will be the key ingredients for this adaptable network structure by switching their operation from the classical to the quantum regime through controllable and high-precision attenuation circuitries. As an essential part of future deep fiber access era, the integration of UNIQORN DPSQKD quantum link to secure the optical link between the centralized BBU and mmWave RRH of future analog 5G mobile fronthauling will be also investigated.

4.5.2 Components and Functionalities. Mapping to UNIQORN

The DPSQKD protocol will be initially evaluated through the installed COSMOTE-NTUA dark fiber link focusing on the performance indicators of the quantum link (e.g. baseline error rate, QBER, maximum sifted and source key rate). During the course of the UNIQORN project we aim to extend this transmission through dark fibers by emulating an integration scheme where this DPSQKD link coexists with the classical traffic flows obtained through the deployed GPON topology of COSMOTE. Based on this deployed network structure and its traffic profile features, simulation studies will be pursued aiming at the optimum allocation of the quantum channel.

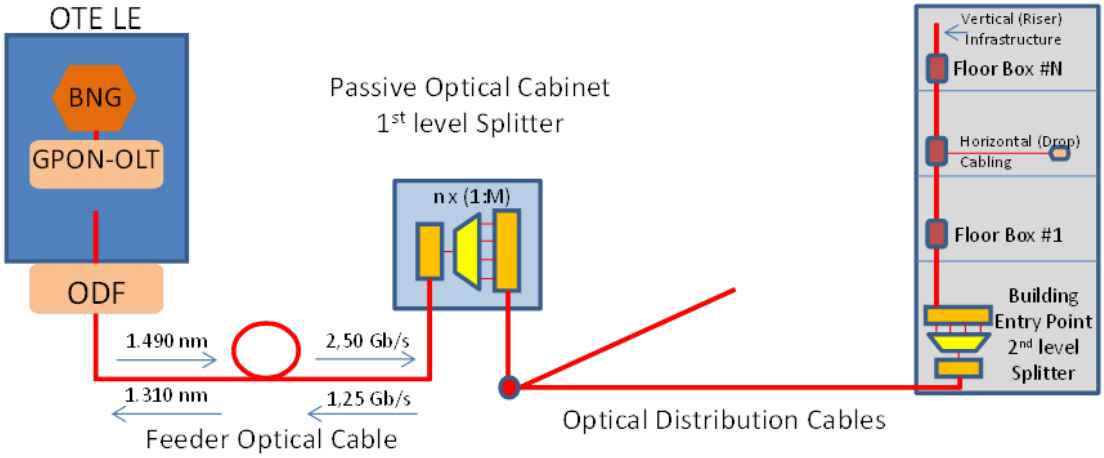


Figure 4-8. Deployed GPON topology suited for FTTH services, operated from COSMOTE

Figure 4-8 illustrates the deployed FTTH network structure of COSMOTE based on GPON topology using passive optical splitters. Through this installed topology, the active equipment is located in the central office emitting wavelengths at the 1490nm for the DS traffic and detecting the upstream from the ONTs at 1310nm. The specific lengths of feeder and distribution optical cables, combined with the class of power levels transmitting through these selected light paths will be considered for the static spectrum allocation of the DPSQKD channels. Detailed experiments will be performed to investigate the role of passive optical circuitries and possible filtering options to optimize the obtained secret key rates. In this context, mitigation techniques like time/wavelength filtering and dynamic power control will be adopted to reduce the scattering noise further [Patel-2012].

The statistics of upstream/downstream will be also explored as a key network parameter for the optimum allocation of DPSQKD channels in the GPON topology. This parameter will be also used to optimize the functional split of the classical/quantum operation of the UNIQORN DPS transmitter of each ONT in the FTTH topology by controlling the on-chip attenuation mechanism. In more detail, the appropriate TDM frames allowing for high secret key rates will be selected to exchange the key information between the centralized node at OLT and the ONTs while the DPS module can also operate as a simple, low-cost classical transmitter, which emits C-band photons, reserved for optional overlay services for currently deployed and future PON topologies [NGPON2-2018].

In parallel with the studies on integration of DPSQKD channels in support of the security of FTTH services, the 5G Mobile fronthauling will be pursued as a possible use case of the developed DPS prototypes within UNIQORN. In the era of centralized-RAN topologies of 5G, the use of quantum links to secure the optical link between the centralized BBU and the large number of fiber connected RRHs will be targeted through the use of low-cost, simple UNIQORN transmitters. Through this targeted activity, the developed DPSQKD transmitters will be integrated as a key part of the analog/digital mobile fronthaul of 5G to fortify the security layer of this fiber-based communication link. The above QKD integration concept will be investigated through mobile fronthaul links supporting both DRoF and DSP-assisted analog IFoF transport schemes [Argyris-2018].

4.5.3 Requirements and Key Performance Indicators

The following table comprises the main parameters for both targeted application of deep fiber era: installed GPON topology for FTTH services and quantum secured analog mobile fronthaul for 5G. The list also includes a set of indicative KPIs linked with the above applications.

Table 4-5. KPIs DPS-based PON

PON-based network structures in Athens test-site		
GPON topology for FTTH services		
Number of splits		1:32 optical splitter (2-stage splitting)
Feeder fiber length Distribution fiber length	Km	up to 9 up to 0.5
Classical channels (Ch-C)	nm	1490 for DS and 1310 for US
Transmission speeds	Gb/s	2.5 for DS and 1.25 for US
Optical power range (Ch-C)	dBm	Class B+ OLT modules (up to +5dBm transmit power and at least -28dBm of received power
DPSQKD channel		
Baseline system error rate (b)	%	< 1.5
QBER	%	< 5
Secret Key Rate	Kbps	1.5 -2
5G mobile fronthauling		
Dark fiber link (BBU-RRH)	Km	up to 20
Emission wavelength of analog IFoF Tx	nm	1545-1555
Launched power of classical	dBm	0-1
Radio channel bandwidth	MHz	2x400
DPSQKD channel		
Baseline system error rate (b)	%	< 1.5
QBER	%	< 4
Secret Key Rate	Kbps	0.5 - 1

Appendix A – Bibliography

[Hübel-2007] Hannes Hübel, Michael R. Vanner, Thomas Lederer, Bibiane Blauensteiner, Thomas Lorünser, Andreas Poppe, and Anton Zeilinger,“ High-fidelity transmission of polarization encoded qubits from an entangled source over 100 km of fiber“,Optics Express Vol. 15, pp. 7853-7862 (2007)

[Laudenbach-2017] Laudenbach, Fabian, et al. "A novel single-crystal & single-pass source for polarisation-and colour-entangled photon pairs." Scientific reports 7.1 (2017): 7235.

[Roehsner-2017] Roehsner, Marie-Christine, et al. "Quantum advantage for probabilistic one-time programs." arXiv preprint arXiv:1709.09724 (2017).

[Pelc-2011] J. Pelc, L. Ma, C. Phillips, Q. Zhang, C. Langrock, O. Slattery, X. Tang, M Fejer, “Long-wavelength-pumped upconversion single-photon detector at 1550 nm: Performance and noise analysis”, Optics express. 19. 21445-56 (2011)

[Herrero-2017] M. Herrero-Collantes, J. Garcia-Escartin, “Quantum Random Number Generators”, Reviews of Modern Physics 89, 015004 (2017)

[Sambo-2018] N. Sambo, K. Christodoulopoulos, N. Argyris, P. Giardina, C. Delezoide, A. Sgambelluri, A. Kretsis, G. Kanakis, F. Fresi, G. Bernini, H. Avramopoulos, E. Varvarigos, P. Castoldi, "Experimental demonstration of fully disaggregated white box including different types of transponders and monitors, controlled by NETCONF and YANG", Optical Fiber Conference (OFC'2018), San Diego, USA, March, 2018. M4A.3

[Velasco-2018] L. Velasco, A. Sgambelluri, R. Casellas , L. Gifre , J. Izquierdo-Zaragoza , F. Fresi, F. Paolucci , R. Martinez and E. Riccardi, "Building Autonomic Optical Whitebox-Based Networks", Journal of Lightwave Technology, Vol. 36, No. 15. August 2018. pp. 3097-3104

[Robinson-2018] N. Robinson, "Design and Deployment of Optical White Box", Optical Fiber Communications conference (OFC'18), San Diego, USA, March 2018. Tu3E.6

[Lyubomirsky-2016] I. Lyubomirsky, B. Taylor, H. Wolfgang Schmidtke, "An open approach for switching, routing, and transport". Facebook Code, Nov, 2016. https://code.fb.com/connectivity/an-open-approach-for-switching-routing-and-transport/

[Furrer-2018] F. Furrer, et al., “Continuous-variable protocol for oblivious transfer in the noisy-storage model”, Nat. Commun. 9, 1450 (2018).

[Erven-2014] C. Erven, N. Ng, N. Gigov, R. Laflamme, S. Wehner, and G. Weihs, “An experimental implementation of oblivious transfer in the noisy storage model,” Nature communications, vol. 5, p. 3418, 2014.

[Goldwasser-2008] S. Goldwasser, Y. T. Kalai, and G. N. Rothblum, “One-time programs,” in Advances in Cryptology – CRYPTO 2008: 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings, (Berlin, Heidelberg), pp. 39–56, Springer Berlin Heidelberg, 2008.

[Wootters-1982] W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned,” Nature, vol. 299, pp. 802–803, 1982.

[Dieks-1982] D. Dieks, “Communication by EPR devices,” Physics Letters A, vol. 92, pp. 271–272, 1982.

[Von Neumann-1955] J. Von Neumann, Mathematical Foundations of Quantum Mechanics. Investigations in Physics, Princeton University Press, 1955

[Broadbent-2013] A. Broadbent, G. Gutoski, and D. Stebila, “Quantum one-time programs,” in Advances in Cryptology – CRYPTO 2013: 33rd Annual

Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part II (R. Canetti and J. A. Garay, eds.), (Berlin, Heidelberg), pp. 344–360, Springer Berlin Heidelberg, 2013, 1211.1080

[Aaronson-2009] S. Aaronson, “Quantum copy-protection and quantum money,” in 2009 24th Annual IEEE Conference on Computational Complexity, pp. 229–242, July 2009, 1110.5353.

[Mayers-1997] D. Mayers, “Unconditionally secure quantum bit commitment is impossible,” Physical Review Letters, vol. 78, pp. 3414–3417, 1997, quant-ph/9605044.

[Lo-1998] H.-K. Lo and H. F. Chau, “Why quantum bit commitment and ideal quantum coin tossing are impossible,” Physica D: Nonlinear Phenomena, vol. 120, pp. 177–187, 1998, quantph/ 9711065

[Hayashi-2006] M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita, “(4,1)-quantum random access coding does not exist – one qubit is not enough to recover one of four bits,” New Journal of Physics, vol. 8, p. 129, 2006, quant-ph/0604061.

[Liu-2014] Y.-K. Liu, “Single-shot security for one-time memories in the isolated qubits model,” in Advances in Cryptology – CRYPTO 2014 (J. A. Garay and R. Gennaro, eds.), (Berlin, Heidelberg), pp. 19–36, Springer Berlin Heidelberg, 2014.

[Liu-2015] Y.-K. Liu, “Privacy amplification in the isolated qubits model,” in Advances in Cryptology - EUROCRYPT 2015 (E. Oswald and M. Fischlin, eds.), (Berlin, Heidelberg), pp. 785–814, Springer Berlin Heidelberg, 2015.

[Ng-2012] N. H. Y. Ng, S. K. Joshi, C. C. Ming, C. Kurtsiefer, and S. Wehner, “Experimental implementation of bit commitment in the noisy-storage model,” Nature communications, vol. 3, p. 1326, 2012.

[Yao-1982] A. C. Yao, “Protocols for secure computations,” in SFCS ’82 Proceedings of the 23rd Annual Symposium on Foundations of Computer Science, (Washington, DC, USA), pp. 160–164, IEEE Computer Society, 1982.

[Naor-1999] M. Naor, B. Pinkas, “Oblivious Transfer and Polynomial Evaluation”, Proceedings of the Thirty-first Annual ACM Symposium on Theory of Computing, 1999.

[NDFIS-2014] http://www.ndfis.org/

[Ou-2018] Y. Ou, E. Hugues-Salas, F. Ntavou, R. Wang, Y. Bi, SY. Yan, G. Kanellos, R. Nejabati, D. Simeonidou, "Field-Trial of Machine Learning-Assisted Quantum Key Distribution (QKD) Networking with SDN", European Conference on Optical Communications (ECOC'18), Rome, Italy. September, 2018. Mo3D. https://arxiv.org/abs/1807.07858

[5GAmericas-2018] Whitepaper "The Evolution of Security in 5G", October, 2018 https://2018.dc5g.com/gated-content/1779/

[Mavromatis-2018] A. Mavromatis, F. Ntavou, E. Hugues-Salas, G. T. Kanellos, R. Nejabati, D. Simeonidou, "Experimental Demonstration of Quantum Key Distribution (QKD) for Energy-Efficient Software-Defined Internet of Things", European Conference on Optical Communications (ECOC'18). Rome, Italy. September, 2018. Mo3D.6

[Fröhlich-2015] Bernd Fröhlich et al., “Quantum secured gigabit optical access networks”, Scientific Reports Volume 5, Article number: 18121 (2015)

[Fröhlich-2013] Fröhlich, B. et al. A quantum access network. Nature 501, 69-72 (2013).

[Patel-2012] Patel, K. A. Coexistence of High-Bit-Rate Quantum Key Distribution and Data on Optical Fiber. Physical Review X2, 041010 (2012).

[NGPON2-2018] On-line available presentations from NG-PON2 Council workshop OFC, 15 March 2018, San Diego, CA, USA

[Argyris-2018] N. Argyris et al., “DSP enabled fiber-wireless IFoF/mmWave link for 5G analog mobile fronthaul”, in Proc. of 2018 IEEE 5G World Forum (5GWF), 9-11 July 2018, Silicon Valley, CA, USA

Appendix B – List of Acronyms

AWG	Arrayed waveguide gratings
AI	Artificial intelligence
BBU	Baseband unit
BRW	Bragg-reflection waveguides
CV	Continuous-Variable
DPS	differential phase shift
EPR	Einstein–Podolsky–Rosen
FPGA	Field programmable gate array
HPN	High Performance Networks
IoT	Internet of Things
KPI	Key Performance Indicator
MCF	Multicore fibre
NIC	network interface card
OS	Oblivious System
ODL	OpenDayLight
OADM	Optical Add-Drop Multiplexer
PON	passive optical network
PPLN	Periodically Poled Lithium Niobate
PPKTP	Periodically Poled Potassium Titanyl Phosphate
PPLN	periodically polled lithium niobite
QRNG	quantum random number generators
QWB	Quantum White Box
QBER	Quantum-bit error rate
RAN	Radio Access Network
ROADM	reconfigurable optical add/drop multiplexers
SHG	second-harmonic generation
SPAD	single-photon avalanche detectors
SDM	Spatial Division Multiplexing
SPDC	Spontaneous parametric down conversion
TIA	Transimpedence amplifier
US/DS	Upstream/Downstream
WDM	Wavelength Division Multiplexing
WSS	Wavelength selective switches
WP	Work Package