Brunner et al. *EPJ Quantum Technology* (2023) 10:38
https://doi.org/10.1140/epjqt/s40507-023-00194-x

EPJ Quantum Technology
a SpringerOpen Journal

EPJ.org

RESEARCH Open Access

Demonstration of a switched CV-QKD network

Hans H. Brunner[1*], Chi-Hang Fred Fung[1], Momtchil Peev[1], Rubén B. Méndez[2], Laura Ortiz[2], Juan P. Brito[2], Vicente Martín[2], José M. Rivas-Moscoso[3], Felipe Jiménez[3], Antonio A. Pastor[3] and Diego R. López[3]

*Correspondence:
hans.brunner@huawei.com
[1]Munich Research Center, Huawei Technologies Duesseldorf GmbH, Munich, Germany
Full list of author information is available at the end of the article

Abstract

A quantum channel is a physical media able to carry quantum signals. Quantum key distribution (QKD) requires direct quantum channels between every pair of prepare-and-measure modules. This requirement heavily compromises the scalability of networks of directly connected QKD modules. A way to avoid this problem is to introduce switches that can dynamically reconfigure the set of connections. The reconfiguration of a quantum channel implies that the modules using it can adapt to the new channel and peer.

The maturity and flexibility of continuous-variable QKD (CV-QKD) qualifies it as a strong contender for integration into optical communication networks. Here we present the implementation of a switched CV-QKD network embedded in the Madrid quantum testbed. The optical switching of the quantum paths significantly reduces the amount of required QKD modules and facilitates the scalability of the network. This demonstration highlights the flexibility and ease of integration of this emerging technology.

Keywords: QKD; CV-QKD; Quantum cryptography; Quantum communications; Quantum networks

1 Introduction

QKD is a family of protocols that generate a shared secret key between two mutually trusting parties. In the specific case of prepare-and-measure protocols, these are the transmitter (Alice) and the receiver (Bob). The generated key is information-theoretically secure (ITS), which can be proven using quantum information theory [1, 2]. QKD protocols are superior to state-of-the-art key exchange protocols as the security of the latter is based on computational complexity assumptions, which could be broken as soon as sufficiently powerful computers (quantum or classical) and/or algorithms are available [3, 4]. While limited in reach and bound to hardware, QKD protocols have also a higher security compared to *post-quantum cryptography* (PQC) protocols. Being ultimately founded on assumptions about quantum and classical computation complexity, PQC protocols can be demonstrated secure only under assumptions about computational security.

CV-QKD protocols, such as, e.g, GG02 [5], are based on modulated continuous-wave lasers and coherent detection, but unlike classical communication the optical power is ex-

© The Author(s) 2023. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

Springer

tremely attenuated. Protocol security is analysed under the assumption that all power lost between the transmitter and the receiver, a fraction typically close to unity, is collected by the eavesdropper. All noise on top of the unavoidable shot noise, which is a manifestation of the uncertainty principle in the measurement of a light state, might as well originate from an adversary. The no-cloning principle dictates that any attempt by the eavesdropper to obtain information on Alice and Bob's data inevitably results in loss and noise [6]. As long as the eavesdropper's information is below a threshold, it is still possible to distil a secure key [7, 8].

A general obstacle to practical utilisation of QKD based on optical communication is the inherently limited key-generation distance. QKD is realised by very weak optical signals that are ultimately absorbed in any physical medium. Periodic amplification, which is a standard practice in optical telecommunication technology, cannot be used for QKD. Amplification, which can be seen as an attempt of cloning unknown quantum states, has to introduce noise on the channel. This noise trace has to be regarded as eavesdropping and usually prohibits key generation. Instead, the reach of quantum signals may be extended by means of special quantum communication devices, known as quantum repeaters (see [9–11] for an overview of the state of the art). Such devices would not obliterate the described level of security, but the development of quantum repeaters is still in an early experimental stage. For this reason it is not straight-forward to design and deploy QKD networks that are analogous to telecommunication ones.

As of today, the standard approach to QKD networking is the "trusted repeater" principle. This amounts to stitching together finite distance QKD links, a link being a pair of a sender and a receiver, by trusted locations. QKD keys are generated in the individual links and then retransmitted by means of classical, albeit ITS, cryptographic methods (see [12, 13] for details). The majority of present-day QKD links are fixed links with a sender permanently connected to a receiver over a given quantum channel, typically an optical fibre. A fully meshed QKD network with N nodes would require approximately N^2 fixed links. In view of the availability and cost of current QKD technology, such an exponential grow in the number of required devices limits the size of QKD networks.

For this reason, switching of quantum channels has been proposed. The first approaches were done by selecting different fibres to connect several senders and receivers in a time multiplexing scheme [14–16]. In this manuscript we extend this approach, capitalising on the potential greater flexibility of CV-QKD over discrete-variable QKD (DV-QKD), by allowing also wavelength multiplexing for a significant increase of versatility. Abstract or small-scale wavelength switching has also been proposed earlier [17, 18]. Moreover, by utilising also the CV-QKD inherent higher tolerance to co-propagation with classical (much stronger) signals in optical fibres [19] we demonstrate a substantial scaling-up of switching.

It should be noted that switching can significantly reduce the number of required QKD devices that are situated within metropolitan-area locations but cannot increase the finite reach of QKD. This means that long-distance QKD still requires, as of today, trusted repeaters. Without going into too much detail, we note that switching of quantum channels will be used in future end to-end quantum communication networks, sometimes popularly dubbed "the quantum internet" [9, 10, 20]. Such networks will require end-to-end entanglement realised by quantum repeaters. For cost reduction and to avoid massive over-

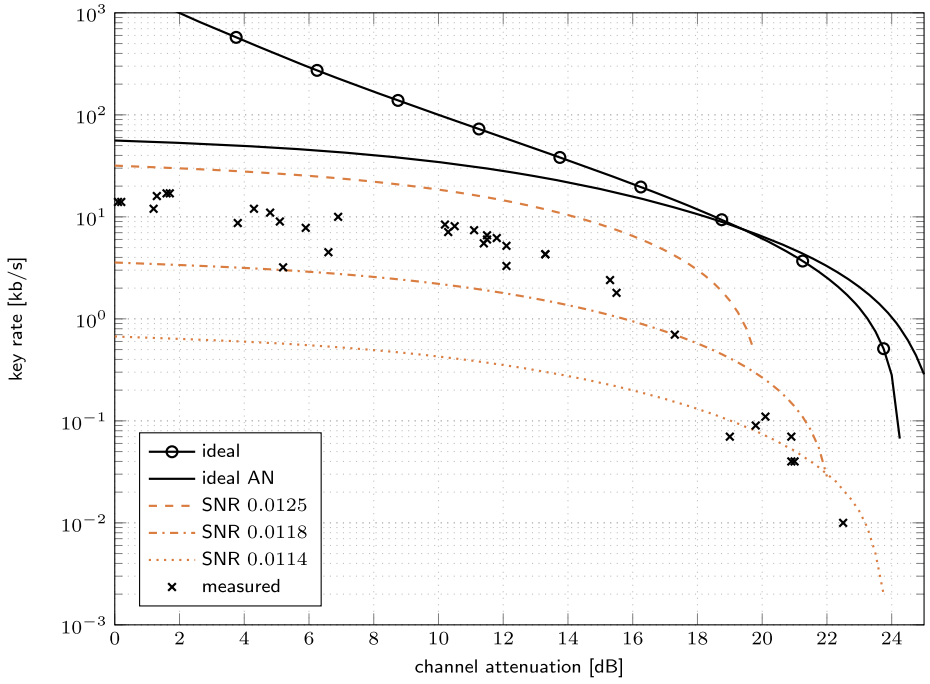


Figure 1 Key rate over channel loss with a 12.5 MHz bandwidth quantum channel. "ideal AN" and "ideal" refer respectively to ideal error correction with and without artificial noise added at the receiver. It can be seen that the addition of artificial noise reduces the key rate in the low to medium loss regime but extends the reach. The curves labelled with "signal-to-noise ratio (SNR) *x*" are upper bounds for the key rate with the SNR target *x* of the artificial noise set to 0.0125 (–19.0 dB), 0.0118 (–19.3 dB), and 0.0114 (–19.4 dB), respectively. These curves are calculated with a fixed-rate code and decoding failure probability corresponding to the target SNR. The transmit power and target SNR of the artificial noise are adapted to the channel situation for each measurement individually to maximise the key rate. The measured key rates suffer from a limited processing power available for the post-processing and can have a wide confidence interval

utilisation of resources, these repeaters could rely on optical switching for the distribution of entanglement.

The investigation of the switched CV-QKD network presented in this paper is embedded in the Madrid quantum network, which is a continuously growing environment for testing and developing quantum communication technologies [14, 21, 22].

2 CV-QKD prototypes

The demonstrated switched QKD network is based on a 12.5 MHz-bandwidth low-noise and low-complexity CV-QKD system with Gaussian modulation. The system has evolved from the setup described in [23] to a phase- and polarisation-diverse modulation and receiver structure.

The CV-QKD systems have an in-band synchronisation, only one dense wavelength division multiplexing (DWDM) channel[1] in the C-band in one direction is needed for the QKD operation. Additionally, a bidirectional, standard internet protocol (IP)-based reconciliation link is required. This link does not rely on a purely-optical point-to-point connection, it can be transported over any existing network infrastructure, e.g., Ethernet.

[1]Without loss of generality, here and in the following we refer to the 100 GHz grid in the C-band defined by ITU-T G.694.1.

The devices can be configured to transmit with any figure between 0.0004 and 40 photons per symbol on average in the quantum band. This corresponds to a transmit power range of approximately −122 dBm to −72 dBm at a carrier frequency of 193.4 THz. The in-band synchronisation signals are typically 30 dB to 40 dB stronger than the quantum signal. The error correction runs with a single fixed-rate code, which supports a SNR down to −19.5 dB. This is a receiver sensitivity of approximately −105 dBm with 2.5 dB of receiver loss and heterodyne detection [24]. Excess noise powers smaller than 50 dB below the shot noise can be detected (−141 dBm in the signal bandwidth at 193.4 THz). With trusted detector noise [25] and an inherent system noise as low as 0.15 mSNU,[2] the system supports up to 23 dB of channel loss. The inherent system noise is attributed to the eavesdropper.

Simulated and measured key rates are depicted in Fig. 1 *vs.* the channel attenuation, in principle proportional to the fibre-link length. In a metropolitan-area scenario the insertion loss of connectors and passive optical equipment and the state of the fibre are likely to dominate the losses. All calculated curves in the plot follow [26] and assume optimistic values with 23 mSNU of trusted detector noise, 0.15 mSNU of untrusted system noise, and 2.5 dB of insertion loss in the receiver. These optimistic values are tight bounds to the span of actual values measured in the deployed devices.

The utilized error-correction code has a low error-correction efficiency at high SNR, but artificially added noise allows reducing the SNR to the efficient regime [27, 28]. The artificially generated noise is added at the receiver after detection. It can reduce the information of the eavesdropper and extend the reach. While the error-correction efficiency improves linearly with an SNR reduction, the probability of an unsuccessful decoding increases rapidly close to the SNR limit. A careful selection of the target SNR for the artificially added noise is necessary to maximise the key rate depending on the channel situation (see Fig. 1).

The final key rate is several orders of magnitude smaller compared to the initial symbol rate of 12.5 MBd. This is a consequence of devoting most symbols to parameter estimation, of a low code rate, and of privacy amplification. The limited amount of computational resources in the prototypes is also a major bottleneck for the final key rate. The probability of a successful decoding depends on the amount of computational resources allowed for each decoding block. While more resources per block improve the probability of a successful decoding they reduce the number of blocks that can be processed per time with a fixed amount of computational resources and a compromise has to be found.

Vulnerability to side channel attacks and possible counter measures [2] are currently not considered.

3 Optically-switched QKD network

The switched QKD network is embedded in the larger Madrid QKD network [21]. A satellite map of the network can be found in [29]. The full sub-network configuration with a focus on the switching and multiplexing setup is shown in Fig. 2. The seven nodes of the QKD-switching network are located all over the metropolitan area of Madrid and are interconnected with previously deployed fibres. Quirón, Quintín, Quijote, and Quevedo and

[2] milli shot-noise unit (SNU), *i.e.*, normalised with respect to the shot-noise power. In this contribution, all excess-noise figures are referred to the receiver.

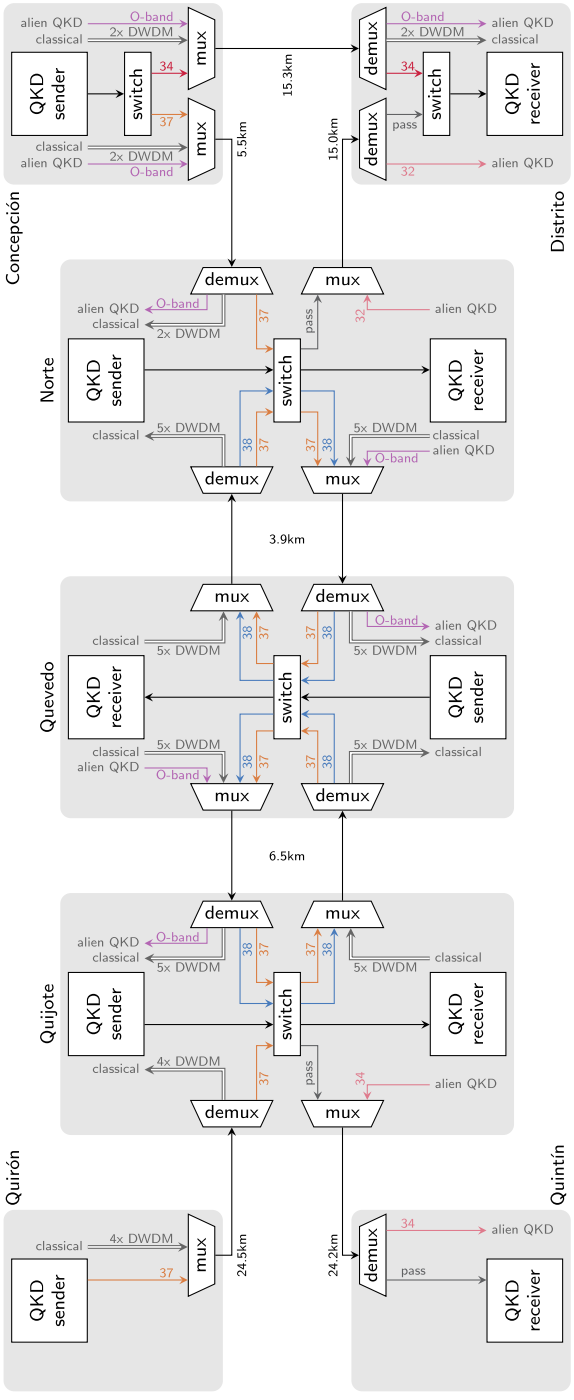


Figure 2 Full configuration of the switched QKD network with a focus on the QKD modules and reconfigurable optical add-drop multiplexers (ROADMs) interconnecting them. At least one lightpath can be created between any of the five senders and any of the five receivers, respectively. The arrow directions indicate the input and output ports of the switches, fixed (de)multiplexers, and QKD devices. The number of occupied DWDM channels and the presence of an O-band channel are indicated for each multiplexer (mux) and demultiplexer (demux) with the arrows at the client side. A double-line arrow stands for multiple fibres, the attached label indicates the number of occupied DWDM channels. "pass" refers to the pass-through lightpath of a (de)mux for all not-listed DWDM channels, e.g., all wavelengths but DWDM channel 34 in the link between Quijote and Quintín. Other classical and quantum communication infrastructure which does not intermingle with the switched QKD signals is omitted from the figure, e.g., the classical connection between Quintín and Quijote

the fibres between them belong to the RediMadrid academic communication network. Concepción, Norte, and Distrito and the fibres between them belong to Telefónica. All of the locations are production sites.

Five QKD senders and five QKD receivers are distributed across seven nodes. The QKD modules are linked through amplifier-free, low-loss ROADMs, which can switch the optical path for the QKD channels in a non-blocking fashion. A lightpath between any QKD sender and any QKD receiver can be established on at least one DWDM channel. While the QKD modules can be tuned to any wavelength in the C-band, the fixed multiplexers constrain most QKD links to the DWDM channels at 193.4 THz (channel 34), 193.7 THz (channel 37), and 193.8 THz (channel 38).

Figure 4 in [30] shows a photograph of the setup at one of the nodes. The top six height units in the picture are filled with two QKD modules and the associated servers used for the experiments described in this contribution. In the same picture, one can find the employed add-drops, optical switch, and OTN equipment among other things.

With the following three stages the ROADMs are adapted to the specific requirements of the respective node. In the first stage, the classical and quantum signals not relevant for this experiment are dropped and the different QKD wavelengths split into different paths for each incoming direction, respectively. This is implemented with demultiplexers, e.g., at Quevedo's inputs from Quijote and Norte in Fig. 2. The direct input from the QKD sender does not need this stage. In the second stage, a non-blocking, all optical $N \times N$ switch routes the different QKD signals towards their respective destination, e.g., the optical switch at Quevedo. In the third stage, the different QKD wavelengths are combined and added to the non-QKD signals for each direction, respectively. This is implemented with multiplexers, e.g., at Quevedo's outputs towards Quijote and Norte in Fig. 2. The direct output into the QKD receiver does not need this stage.

As an example for a switched optical path, the QKD link between Quijote and Norte is described in the following. The QKD sender at Quijote would be configured to a supported DWDM channel, channel 37 or 38. The output signal of this sender would then pass through the optical switch at Quijote, which needs to connect this QKD input towards the appropriate multiplexer port towards Quevedo. At Quevedo, the QKD signal would be dropped by the demultiplexer into the optical switch at Quevedo. This switch needs to connect this input signal to the appropriate multiplexer port towards Norte. At the other end of the line, at Norte, the QKD signal would be dropped again by the demultiplexer and fed into the optical switch. Finally, the optical switch at Norte would connect the QKD signal to the input port of the QKD receiver. As long as the total loss along such a path is supported by the QKD devices, a QKD link for key generation can be established.

The QKD links are multiplexed with classical communication links in most fibres between the different nodes. Most of these fibres carry also QKD links from other vendors in the O-band or C-band. The reconciliation links of the QKD devices are transported jointly with the control signals and encrypted data through a packet-switched network with network switches at every node. This dedicated network is not depicted in detail in Fig. 2, but it accounts for most of the classical channels between the different nodes.

The multiplexing between Quijote, Quevedo, and Norte is established with two consecutive multichannel optical add-drop multiplexers (OADMs). The five classical channels are combined in a first OADM before they are added in a second OADM to the two quan-

tum channels 37 and 38 and the alien QKD signal in the O-band. This is depicted with a single multiplexer in Fig. 2. The same is true vice versa for the demultiplexing side.

In the link between Quirón and Quijote the quantum channel is fixed to channel 37 as it is simply connected as an alien wavelength to a free multiplexing port of the previously existing optical transport network (OTN) equipment. This link has three active classical channels plus our reconciliation link as a second alien wavelength. In the links Quijote to Quintín and Norte to Distrito the QKD channel is combined with the QKD channel of another vendor also in the C-band with single channel OADMs. Here, the QKD channel could be on any wavelength in the C-band except the single DWDM channel occupied by the alien QKD.

The multiplexing in the links Concepción to Distrito and Concepción to Norte is also implemented with two-stage multiplexers. In contrast to the central links, the QKD signals here are first multiplexed with a classical signal before they are added with an OADM to the alien QKD quantum and synchronisation channels. This first multiplexer fixes the QKD link Concepción to Distrito to DWDM channel 34 (193.4 THz). The QKD link Concepción to Norte is on the DWDM channel 37.

4 Trusted transmit loss

The deployed CV-QKD prototypes support the configuration of a trusted transmit loss. The idea of a trusted transmit loss is to allow the system operator to shift the trusted boundary within the trusted transmit perimeter. By default the trusted boundary is the output port of the QKD transmitter. Additionally configured trusted transmit loss can shift this, e.g., to the output of a multiplexer and/or optical switch the output of the QKD transmitter is connected to within the trusted node perimeter.

Ideally, the trusted transmit loss is calibrated by comparing the optical output power of the QKD transmitter before and after the additionally trusted devices. Since such a calibration would lead to a possibly unwanted interruption of other traffic passing the same devices and adds an extra step when building the network, it is also acceptable to take conservative (secure) guesses about the insertion loss. Only the insertion loss that is certainly absorbed within the trusted transmit perimeter should be configured as trusted loss. In a multi-hop link only the insertion loss of the switch and/or multiplexer at the transmit node might be trusted, whereas the insertion loss of the switches, demultiplexers and multiplexers of the nodes in-between or at the receiver must not be regarded as trusted transmit loss.

In the demonstrated network, each node is assumed to operate inside a trusted perimeter (indicated by the grey boxes in Fig. 2) and the trusted boundary is always shifted to the boundary of the node. The trusted losses configured in the network at hand are listed in Table 1 and explained in more detail in the following. All assumed insertion losses have been checked to be lower than the actual insertion losses.

The 16-channel multiplexer at Quirón has more than 3.3 dB of insertion loss. Any connection from Quirón is configured with this figure as the trusted transmit loss.

For the optical switches at Quijote, Quevedo, and Norte an insertion loss of 0.5 dB each is used. The back-to-back links at Quijote, Quevedo, and Norte are each configured with this insertion loss as trusted transmit loss. The single-channel OADMs at Quijote towards Quintín and at Norte towards Distrito are assumed to have an insertion loss of 0.6 dB, respectively. The multi-channel OADMs between Quijote, Quevedo, and Norte have more

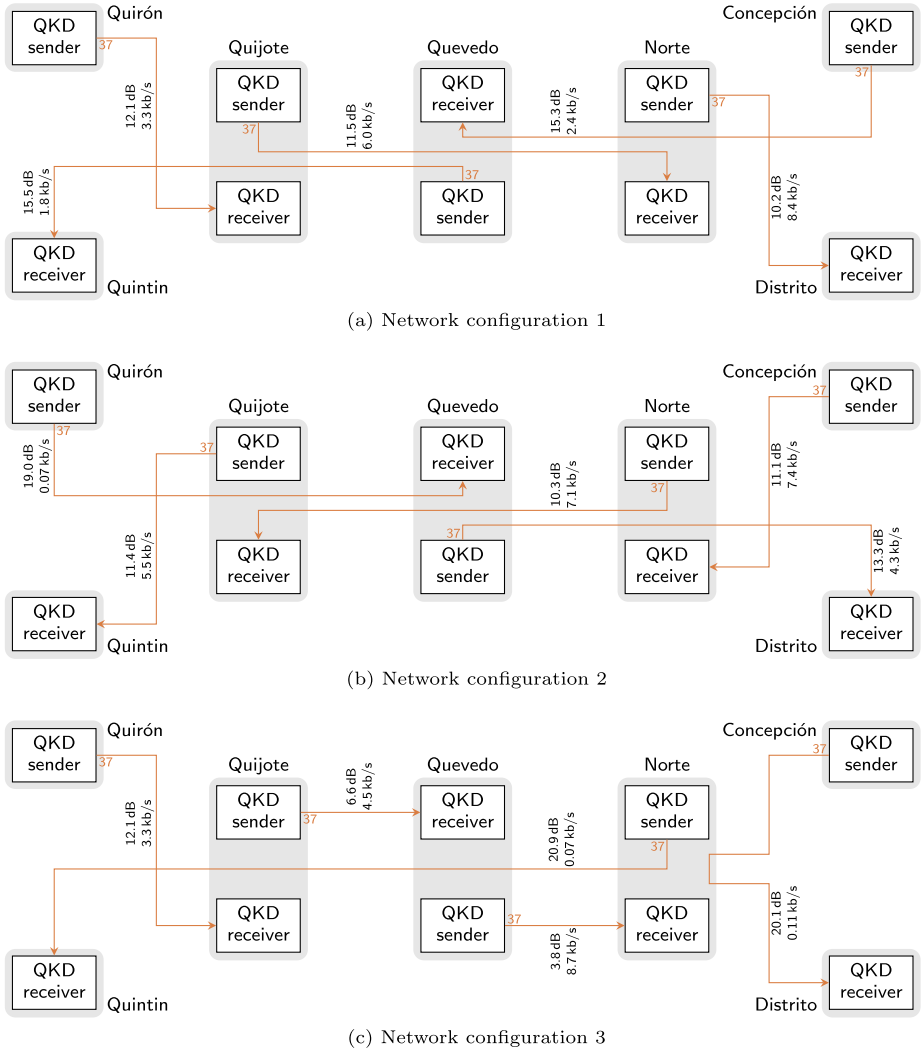
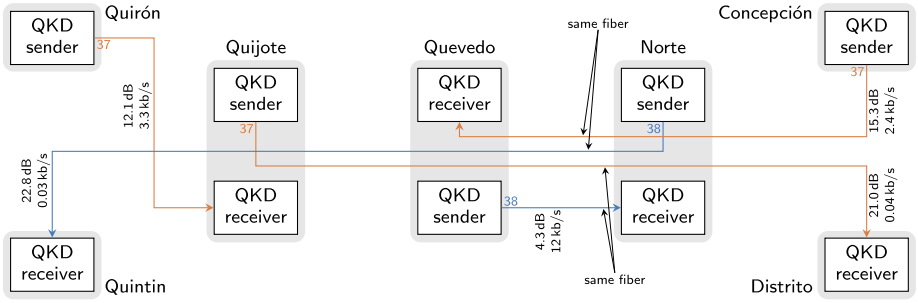


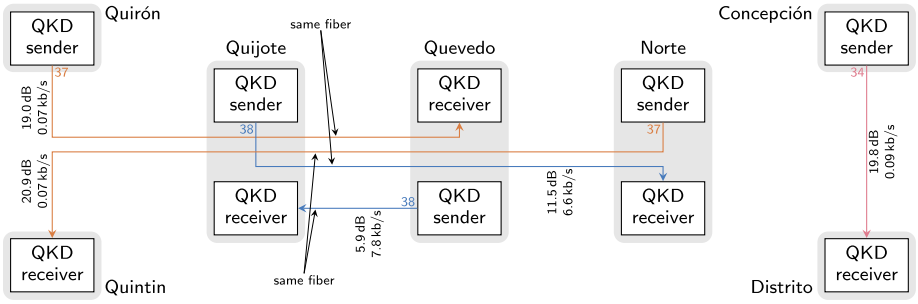
Figure 3 Exemplary network configurations with all QKD senders and all QKD receivers active on the same DWDM channel 37. The given numbers are the measured channel loss and key rate handed over to the local key manager

than 0.9 dB of loss each. Except for the back-to-back links, the trusted transmit loss of all links from Quijote, Quevedo, and Norte are configured to 1.1 dB or 1.4 dB each, which is the sum of the insertion losses of the respective OADM and switch.

For the optical switch at Concepción an insertion loss of 0.3 dB is used. The connection between Concepción and Norte is equipped at Concepción with a 40-channel multiplexer with an assumed insertion loss of 4.1 dB followed by a multi-channel OADM with an assumed insertion loss of 0.9 dB. This concatenation is depicted as a single “mux” in Fig. 2. All links using this connection are configured with a trusted transmit loss of 5.3 dB. The connection towards Distrito is equipped with an 8-channel multiplexer followed by a multi-channel OADM. Insertion losses of 2.1 dB and 0.9 dB are configured, respectively. Again, this concatenation is depicted as a single “mux” in Fig. 2. The link Concepción to Distrito is configured with a trusted loss of 3.3 dB.



(a) Network configuration 4



(b) Network configuration 5

Figure 4 Exemplary network configurations with all QKD senders and all QKD receivers active on either DWDM channel 34, 37, or 38. Note that multiple QKD links can be active at the same time on the same fibre in such a configuration (only two fibres connect different nodes). The given numbers are the measured channel loss and key rate handed over to the local key manager

5 Experimental results

Figures 3 and 4 show several of the possible switching configurations, which can be achieved by online reconfiguration of the switches and DWDM channels of the QKD modules. All QKD links are on DWDM channel 37 in the configurations in Fig. 3, while some of the QKD links are in DWDM channels 34 or 38 in the configurations in Fig. 4. Note that there are four different QKD links active in the fibre pair between Quevedo and Norte in Fig. 4(a) and Quijote and Quevedo in Fig. 4(b), respectively. Taking the alien QKD links in the O-band into account, there are five different QKD links active in these fibre pairs.

Table 1 lists the configured trusted transmit loss, measured channel loss, and measured key rate for all links possible in the network configuration described in Fig. 2. The given key rates are all within the range supported by the employed QKD devices, but they are preliminary figures as finite-size effects could not be considered to their full extent for all scenarios. Although the systems were installed and running during a very long time period (close to three years), no long-term measurements of the key rate have been systematically done. There is no one-to-one mapping between the measured channel loss and the measured key rates because the receiver devices experience different system noise and insertion loss. On the one hand this is because the receivers are different modules and on the other hand the receivers are situated in differently air-conditioned environments since these are production facilities and not controlled laboratories. Some of the reported key rates are at the very edge of the rates supported by the modules and cannot be guaranteed in general. They might not be feasible if the receivers were swapped or the environmental conditions in the facilities changed.

Table 1 List of supported key rates and measured channel loss

Sender node	Receiver node	Optical channel [THz]	Trusted loss [dB]	Channel loss [dB]	Key rate [kb/s]
Concepción	Distrito	19**3.4**	3.3	19.8	0.09
	(via Norte)	19**3.7**	5.3	20.1	0.11
	Norte	19**3.7**	5.3	11.1	7.4
	Quevedo	19**3.7**	5.3	15.3	2.4
	Quijote	19**3.7**		too high	0
	Quintín	19**3.7**		too high	0
Norte	Distrito	19**3.7**	1.1	10.2	8.4
		19**3.8**	1.1	10.5	8.1
	Norte	19**3.7**	0.5	1.6	17
		19**3.8**	0.5	1.7	17
	Quevedo	19**3.7**	1.4	5.1	9.0
		19**3.8**	1.4	5.2	3.2
	Quijote	19**3.7**	1.4	10.3	7.1
		19**3.8**	1.4	12.1	5.2
	Quintín	19**3.7**	1.4	20.9	0.07
		19**3.8**	1.4	22.5	0.01
Quevedo	Distrito	19**3.7**	1.4	13.3	4.3
		19**3.8**	1.4	13.3	4.3
	Norte	19**3.7**	1.4	3.8	8.7
		19**3.8**	1.4	4.3	12
	Quevedo	19**3.7**	0.5	0.1	14
		19**3.8**	0.5	0.2	14
	Quijote	19**3.7**	1.4	4.8	11
		19**3.8**	1.4	5.9	7.8
	Quintín	19**3.7**	1.4	15.5	1.8
		19**3.8**	1.4	17.3	0.7
Quijote	Distrito	19**3.7**	1.4	21.0	0.04
		19**3.8**	1.4	20.9	0.04
	Norte	19**3.7**	1.4	11.5	6.0
		19**3.8**	1.4	11.5	6.6
	Quevedo	19**3.7**	1.4	6.6	4.5
		19**3.8**	1.4	6.9	10
	Quijote	19**3.7**	0.5	1.2	12
		19**3.8**	0.5	1.3	16
	Quintín	19**3.7**	1.1	11.4	5.5
		19**3.8**	1.1	11.8	6.2
Quirón	Distrito	19**3.7**		too high	0
	Norte	19**3.7**		too high	0
	Quevedo	19**3.7**	3.3	19.0	0.07
	Quijote	19**3.7**	3.3	12.1	3.3
	Quintín	19**3.7**		too high	0

Since the launch powers into the fibres of the classical channels are rather weak (< 0 dBm) and the distances are mostly below 10km, there is only negligible Raman noise to be expected (< 0.05 mSNU) [31]. Especially the links towards Quintín and over the connection Norte to Distrito experience very little Raman noise as they only copropagate with very weak alien-QKD signals in the last hop. The variation in the channel losses between different DWDM channels is mostly due to the different insertion losses of the optical connections.

With five senders and five receivers there are up to twenty-five different, loop-free links in a fully meshed network on the same DWDM channel. In contrast, with fixed point-to-point QKD only five links could be established with five QKD pairs. Twenty out of these twenty-five links are operational in the demonstrated network on DWDM channel 37. The other five have a too-high channel loss. Three of the twenty operational links are back-to-

back links in the same node, which are useful for maintenance and testing purposes. There are fifteen operational links on DWDM channel 38, again three of them are back-to-back links, and one operational link on DWDM channel 34. All together thirty-six loop-free links could be operated successfully.

6 Conclusion

An elaborate switched QKD network implementation, which was demonstrated in the Madrid quantum testbed, is described in detail. The switching is enabled by specialised ROADMs and online configurable DWDM channels in the QKD modules. The QKD modules support any-to-any connectivity and promptly adapt to changing link characteristics, allowing 36 different, loop-free QKD links to be established in a small-sized network with only five QKD senders and five QKD receivers. Avoiding intermediate trusted nodes and the need to have static fibre links for the quantum channel between any two nodes in the network demonstrates the relevance of switching on the path to large-scale QKD networks.

Funding
We would like to thank the project MadQ-CM (Madrid Quantum de la Comunidad de Madrid) funded by the European Union (NextGenerationEU, PRTR-C17.I1) and by the Comunidad de Madrid (Programa de Acciones Complementarias), the project Quantum Information Technologies in Madrid (QUITEMAD-CM S2018/TCS-4342), and the European Union's Horizon Europe research and innovation funding program under the project "Quantum Secure Networks Partnership" (QSNP, grant agreement No 101114043).

Abbreviations
CV-QKD, continuous-variable QKD; demux, demultiplexer; DV-QKD, discrete-variable QKD; DWDM, dense wavelength division multiplexing; IP, internet protocol; ITS, information-theoretically secure; mux, multiplexer; OADM, optical add-drop multiplexer; OTN, optical transport network; QKD, quantum key distribution; ROADM, reconfigurable optical add-drop multiplexer; SNR, signal-to-noise ratio; SNU, shot-noise unit.

Availability of data and materials
Not applicable.

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
Not applicable.

Competing interests
The authors declare no competing interests.

Author contributions
H. H. Brunner, M. Peev, J. P. Brito, V. Martin, A. A. Pastor, and D. R. Lopez conceived the idea for the study. H. H. Brunner, C.-H. F. Fung, and M. Peev developed the QKD devices. R. B. Mendez, J. P. Brito, L. Ortiz, and V. Martin developed the key management and network layer. H. H. Brunner, C.-H. F. Fung, R. B. Mendez, J. P. Brito, L. Ortiz, V. Martin, J. M. Rivas-Moscoso, and F. Jimenez installed the field deployment as well as operated the QKD devices and network layer. H. H. Brunner performed the measurements and created the figures, then wrote the manuscript with feedbacks from all authors. All authors contributed to the extensive discussions of the results.

Author details
[1]Munich Research Center, Huawei Technologies Duesseldorf GmbH, Munich, Germany. [2]Center for Computational Simulation, Universidad Politécnica de Madrid, Madrid, Spain. [3]Telefónica gCTIO/I+D, Madrid, Spain.

Received: 13 June 2023 Accepted: 7 September 2023 Published online: 21 September 2023

References

1. Diamanti E, Lo HK, Qi B, Yuan Z. Practical challenges in quantum key distribution. npj Quantum Inf. 2016;2:16025. https://doi.org/10.1038/npjqi.2016.25.
2. Diamanti E, Leverrier A. Distributing secret keys with quantum continuous variables: principle, security and implementations. Entropy. 2015;17(9):6072–92. https://doi.org/10.3390/e17096072.

3. Kaplan M, Leurent G, Leverrier A, Naya-Plasencia M. Breaking symmetric cryptosystems using quantum period finding. In: Robshaw M, Katz J, editors. Advances in cryptology—CRYPTO 2016. LNCS. vol. 9815. Berlin: Springer; 2016. p. 207–37.
4. Shor PW. Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th annual symposium on foundations of computer science. 1994. p. 124–34.
5. Grosshans F, Grangier P. Continuous variable quantum cryptography using coherent states. Phys Rev Lett. 2002;88(5):057902. https://doi.org/10.1103/PhysRevLett.88.057902.
6. Wootters WK, Zurek WH. A single quantum cannot be cloned. Nature. 1982;299:802–3. https://doi.org/10.1038/299802a0.
7. Leverrier A. Composable security proof for continuous-variable quantum key distribution with coherent states. Phys Rev Lett. 2015;114(7):070501. https://doi.org/10.1103/PhysRevLett.114.070501.
8. Leverrier A. Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction. Phys Rev Lett. 2017;118:200501. https://doi.org/10.1103/PhysRevLett.118.200501.
9. Azuma K, Economou SE, Elkouss D, Hilaire P, Jiang L, Lo HK et al. Quantum repeaters: from quantum networks to the quantum Internet. 2022. Preprint.
10. Azuma K, Kato G. Aggregating quantum repeaters for the quantum Internet. Phys Rev A. 2017;96:032332. https://doi.org/10.1103/PhysRevA.96.032332.
11. Briegel HJ, Dür W, Cirac JI, Zoller P. Quantum repeaters: the role of imperfect local operations in quantum communication. Phys Rev Lett. 1998;81:5932–5. https://doi.org/10.1103/PhysRevLett.81.5932.
12. Mehic M, Niemiec M, Rass S, Ma J, Peev M, Aguado A et al. Quantum key distribution: a networking perspective. ACM Comput Surv. 2020;53(5):96. https://doi.org/10.1145/3402192.
13. Cao Y, Zhao Y, Wang Q, Zhang J, Ng SX, Hanzo L. The evolution of quantum key distribution networks: on the road to the qinternet. IEEE Commun Surveys Tuts. 2022;24(2):839–94. https://doi.org/10.1109/COMST.2022.3144219.
14. Lopez DR, Martin V, Lopez V, de la Iglesia F, Pastor A, Brunner H et al. Demonstration of software defined network services utilizing quantum key distribution fully integrated with standard telecommunication network. Quantum Rep. 2020;2(3):453–8. https://doi.org/10.3390/quantum2030032.
15. Yang YH, Li PY, Ma SZ, Qian XC, Zhang KY, Wang LJ et al. All optical metropolitan quantum key distribution network with post-quantum cryptography authentication. Opt Express. 2021;29(16):25859–67. https://doi.org/10.1364/OE.432944.
16. Martinez-Mateo J, Ciurana A, Martin V. Quantum key distribution based on selective post-processing in passive optical networks. IEEE Photonics Technol Lett. 2014;26(9):881–4. https://doi.org/10.1109/LPT.2014.2308921.
17. Ciurana A, Martínez-Mateo J, Peev M, Poppe A, Walenta N, Zbinden H et al. Quantum metropolitan optical network based on wavelength division multiplexing. Opt Express. 2014;22(2):1576–93. https://doi.org/10.1364/OE.22.001576.
18. Wang R, Tessinari RS, Hugues-Salas E, Bravalheri A, Uniyal N, Muqaddas AS et al. End-to-dnd quantum secured inter-domain 5G service orchestration over dynamically switched flex-grid optical networks enabled by a q-ROADM. J Lightwave Technol. 2020;38(1):139–49. https://doi.org/10.1109/JLT.2019.2949864.
19. Karinou F, Brunner HH, Fung F, Comandar L, Bettelli S, Hillerkuss D et al. Towards the integration of CV quantum key distribution in deployed optical networks. IEEE Photonics Technol Lett. 2018;30(7):650–3. https://doi.org/10.1109/LPT.2018.2810334.
20. Kimble HJ. The quantum Internet. Nature. 2008;453:1023–30. https://doi.org/10.1038/nature07127.
21. García Cid MI, Ortiz Martín L, Ayuso M, Madrid V. Quantum network: a first step to quantum Internet. In: 16th int. conf. Availability, reliability and security—ARES 21. Association for Computing Machinery; 2021.
22. Martin V, Aguado A, Salas P, Sanz AL, Brito JP, Lopez DR et al. The Madrid quantum network: a quantum-classical integrated infrastructure. In: OSA advanced photonics congress (AP) 2019. Optica Publishing Group; 2019.
23. Brunner HH, Comandar LC, Karinou F, Bettelli S, Hillerkuss D, Fung CHF et al. A low-complexity heterodyne CV-QKD architecture. In: 19th int. conf. Transparent optical networks—ICTON 2017. New York: IEEE Press; 2017.
24. Kikuchi K. Fundamentals of coherent optical fiber communications. J Lightwave Technol. 2016;34(1):157–79. https://doi.org/10.1109/JLT.2015.2463719.
25. Brunner HH, Bettelli S, Fung CHF, Peev M. Precise noise calibration for CV-QKD. In: 22nd int. conf. Transparent optical networks—ICTON 2020. New York: IEEE Press; 2020.
26. Laudenbach F, Pacher C, Fung CHF, Poppe A, Peev M, Schrenk B et al. Continuous-variable quantum key distribution with Gaussian modulation—the theory of practical implementations. 2017. Preprint.
27. Fung CHF. inventor; Huawei Technologies Duesseldorf GmbH, assignee. Quantum key distribution communication devices, methods and systems. EP3656079A1; 2022.
28. Usenko VC, Filip R. Trusted noise in continuous-variable quantum key distribution: a threat and a defense. Entropy. 2016;18(1):20. https://doi.org/10.3390/e18010020.
29. Hübel H, Kutschera F, Pacher C, Achleitner M, Strasser W, Vedovato F et al. Deployed QKD networks in Europe. In: Optical fiber communication conference (OFC). Optica Publishing Group; 2023.
30. van Deventer O, Spethmann N, Loeffler M, Amoretti M, van den Brink R, Bruno N et al. Towards European standards for quantum technologies. EPJ Quantum Technol. 2022;9:33 https://doi.org/10.1140/epjqt/s40507-022-00150-1.
31. Karinou F, Comandar L, Brunner HH, Hillerkuss D, Fung F, Bettelli S et al. Experimental evaluation of the impairments on a QKD system in a 20-channel WDM co-existence scheme. In: Photonics society summer topical meeting series (SUM). New York: IEEE Press; 2017. p. 145–6.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.