# 400G Transmission of QKD-Secured 100G Data Stream over 184 km SSMF through three QKD Links and two Trusted Nodes

E. Pincemin[(1)], P. Gavignet[(1)], F. Herviou[(1)], Y. Loussouarn[(1)], F. Mondain[(1)], A. J. Grant[(2)], L. Johnson[(2)], R. I. Woodward[(2)], J. F. Dynes[(2)], B. Summers[(2)], A. J. Shields[(2)], K. Taira[(3)], H. Sato[(3)], R. Zink[(4)], V. Grempka[(5)], V. Castay[(5)], J. Zou[(4,5)]

[(1)] Orange Innovation, 2 Avenue Pierre Marzin, 22300 Lannion, France, erwan.pincemin@orange.com
[(2)] Toshiba Europe Ltd, Cambridge, UK
[(3)] Toshiba Digital Solutions Corporation, Kanagawa, Japan
[(4)] Adva Network Security GmbH, Berlin, Germany
[(5)] ADVA Optical Networking SE, Paris, France / Munich, Germany

**Abstract** *We report the transmission of a coherent 400-Gbps dual-polarization (DP) 16QAM channel that transport QKD-secured 100-GbE data stream with other fifty-four WDM channels at 100 Gbps over 184 km of SSMF through three QKD links and two trusted nodes. ©2023 The Author(s)*

## Introduction

For several years, quantum key distribution (QKD) [1] has been gaining renewed interest in improving the security of communication networks and repelling the threat of future quantum computers. QKD uses quantum properties to exchange encryption keys between remote network elements, which can be used for symmetric encryption through algorithms such as the advanced encryption standard (AES) [2]. However, QKD deployments must deal with various constraints of operational networks, such as the fiber scarcity for a QKD-dedicated fiber infrastructure, the mismatch between transmission range of QKD and WDM systems, the impossibility for a quantum key to pass through an optical amplifier. At the same time, 400Gbps is becoming the new standard for metro/regional and data-centre interconnect (DCI) transmission applications [3], both being compatible with the performance of currently proposed QKD systems [4] in particular when trusted nodes are employed.

In this paper, we report the transmission over a 184-km metropolitan link of a coherent 400G DP-16QAM channel, generated by a Nx100G muxponder (N=4), which carries a QKD-secured 100GbE data stream as OTNsec [5]. The 400G channel under study is inserted into a 54-wavelengths 100G WDM comb with a total power up to ~17 dBm. This encrypted signal is transported over three QKD links of 67 km, 50 km and 67 km of standard single-mode fiber (SSMF), respectively, which are connected to each other via trusted nodes. On the two longest QKD sections of 67 km, the 1550-nm quantum channel from one side and 1550-nm WDM channels from the other side are transmitted over two different fiber links of the same length, while on the shortest 50-km path co-propagates the quantum key at 1310 nm and the WDM signals at 1550 nm on the same fiber. This unique arrangement of the most advanced QKD and WDM technologies is, in our opinion, very new.

## Experimental Set-up

The experimental set-up is depicted in Fig.1. A 100-GbE tester generates the data flow that is converted in the optical domain by a client or ″gray″ 100GBASE-LR4 QSFP28 optic [6]. A second 100GBASE-LR4 QSFP28 interface plugged inside a 100G transponder [7] receives the data. This transponder can map and encrypt the 100-GbE data stream as OTNsec [5] thanks to the AES-256 algorithm [2]. Complying with the NIST recommendation [8], the effective 256-bit cipher key is derived from an embedded Diffie-Hellman key (″purple″ key→ DHK) exchange and a QKD ″global″ key (″red″ key → GK) delivered by a key management server (KMS), as shown in Fig. 1. At the other side of the transponder, a WDM 100G CFP digital coherent optic (DCO) that colors the signal, or a 100GBASE-LR4-CFP transceiver that keeps the signal in the ″gray″ domain can be used. This latter configuration is chosen here. The 100-GbE data stream is then mapped and encrypted in an OTU-4 [9] container before being delivered by the 100G transponder. It is then detected by a third 100GBASE-LR4 QSFP28 optic (also operating in the OTU-4 mode) plugged inside a Nx100G muxponder [7] (with N=4) that mixes the 100G QKD-secured signal with other three 100G non-encrypted data flows. At the output of the muxponder, a coherent 400G DP-16QAM signal is generated thanks to a 400G CFP2-DCO [10]. The role of the 100G transponder is thus to encrypt the signal with a ″secret″ key derived from the QKD ″global″ key (GK) provided by the KMS#1 and a Diffie-Hellman key (DHK), while the function of the muxponder is to encapsulate the 100G QKD-secured signal in a 400G WDM pipe. Note that the reverse process is performed at the receiver side to decrypt and recover the 100-GbE data flow in the 100-GbE tester.

We use one multiplexed (MU) and two long-distance (LD) QKD systems [4,11] in the experiment of Fig 1. The MU-QKD system is optimized for supporting co-propagation of quantum and WDM channels. This is achieved using a quantum channel at 1310 nm and WDM channels in the 1550-nm range, for increased spectral separation that minimizes the impact of Raman scattering [11]. On the other hand, the LD-QKD system is optimized for reaching the longest transmission distance. This is achieved using a 1550-nm quantum channel (in the window where the SSMF losses are minimal) and physically separating the propagation of the quantum key from that of WDM signals using two different fibers of the same length. Add/drop multiplexer is also included in the QKD units to multiplex /demultiplex the quantum channel, the control channels

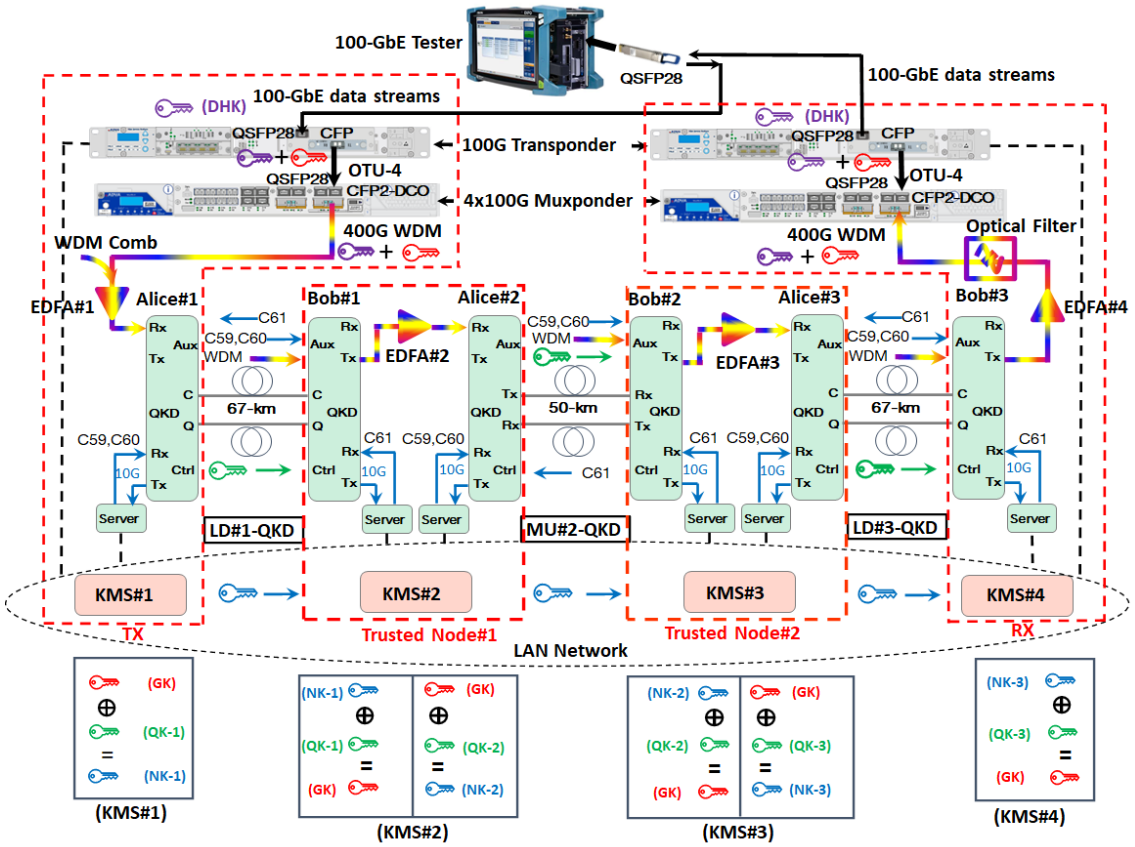


**Fig.1:** Experimental set-up with the three QKD links, the 100GbE tester, the 100G transponders, the Nx100G muxponders (with N=4), the key management servers (KMS), the two trusted nodes, and the description of key management in the set-up.

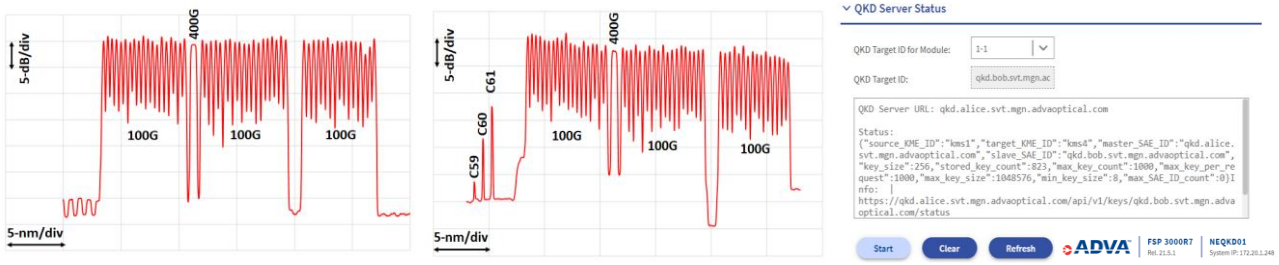


**Fig.2:** (Left) WDM comb sent at the Tx side, (Middle) WDM comb recovered at the Rx side, (Right) QKD server status recovered on the network management system (NMS) of the 100G transponder at the Tx side with all the information related to the key management [12].

of the QKD systems (for synchronization, authentication, reconciliation…) and WDM channels.

The transmission experiment (Fig. 1) is constituted of a WDM comb of 54 DP-QPSK channels at 100 Gbps ranged from 1533.6 to 1557 nm (with 50 GHz spacing) and one coherent 400G DP-16-QAM channel at 1542.3 nm carrying the 100G QKD-secured signal (as shown in the spectrum of Fig. 2 (left)). A hole is created in the WDM comb at 1550-nm by switching-off three channels: this authorizes the LD-QKD system with its 1550-nm quantum key to work without any disturbing effect. The 400G channel operating at ~64-Gbaud has two-fold more power than each of the 32-Gbaud 100G channels. After amplification in an Erbium-doped fiber amplifier (EDFA#1) with ~19-dBm output power and ~6-dB noise figure, the mixed 100G/400G WDM comb is sent to the auxiliary (AUX) Rx port of Alice#1 unit of the first LD-QKD system. From the QKD C Port of Alice#1 come out the WDM comb as well as two control channels (C59 & C60), while the QKD quantum (Q) port of Alice#1 delivers the quantum key. Two separated fibers of strictly the same 67-km length propagate the quantum channel and 1550-nm range signals (i.e., the control channels and WDM comb), respectively. Another control channel (C61) emitted by the QKD C port of Bob#1 counter-propagates with the WDM comb and C59 & C60 control channels on the same fiber, as shown in Fig. 1. At Bob#1, the quantum key is recovered on the Q port of the QKD unit while the classical channels (i.e., WDM, C59 & C60) are recovered at the C port. The demultiplexing part of Bob unit separates the WDM comb from the control channels and sends the WDM signals to the AUX Tx port. The WDM comb is re-amplified with the EDFA#2 and sent to the AUX Rx port of the Alice#2 terminal of the MU-QKD system, the second QKD system of the chain. In that case the WDM comb aggregated power in the fiber at the QKD Tx port is ~17 dBm. The operation described above for the LD-QKD system is the same for the MU-QKD units, except that the control channels (i.e., C59 & C60), WDM comb and quantum channel at 1310 nm are coupled all together and come out from the QKD Tx port of Alice#2 on a same SSMF section of 50-km. A second 50-km SSMF span is used

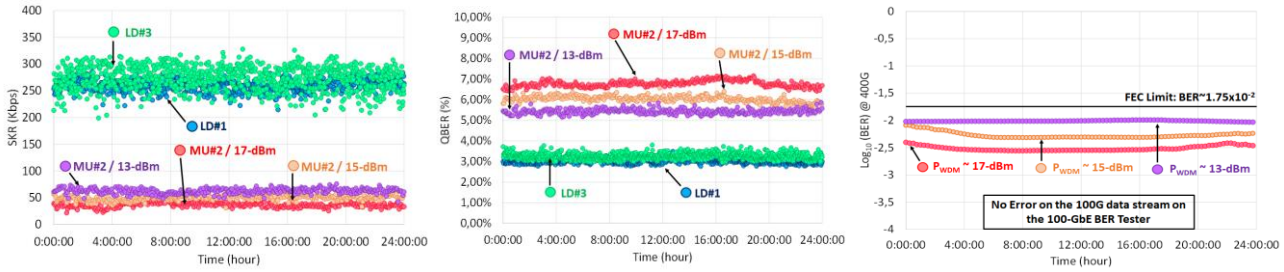


**Fig.3 :** (Left) Secret key rate (SKR) in kbps measured during 24 hours for the MU-QKD system with $P_{WDM}$ ~17, ~15 and 13 dBm, and for the LD#1 and LD#3-QKD systems with $P_{WDM}$ ~15 dBm; (Middle) Quantum BER (QBER) in % for the same configurations; (Right) Pre-FEC BER of the 400G DP-16QAM channel with $P_{WDM}$ ~17, ~15 and ~13 dBm.

to propagate the backward control channel (i.e., C61). At Bob#2, the demultiplexing unit separates the quantum key from the control channels (sent to the control (Ctrl) Tx port) and WDM comb (sent to the AUX Tx port). The WDM comb is re-amplified with the EDFA#3 and sent to the AUX Rx port of the Alice#3 terminal of the second LD-QKD system, the last of the chain. The operation inside this last QKD unit is fully identical to the first one. At the end of the link whose spectrum is depicted in Fig. 2 (middle), an 87.5-GHz flat-top tunable wavelength/bandwidth optical filter located after the EDFA#4 is used to extract the 400G channel from the received WDM comb.

## Key management

The key management servers (KMS) handle the keys inside the system and establish the link between all the elements of the set-up, all of them being connected to a local area network (LAN), as shown in Fig. 1. To establish a trusted chain between the different elements of the experiment, a ″root″ certification authority (CA) is used to create certificates to an ″intermediate″ CA that itself issues certificates to the end-entities (i.e., the equipment of the set-up) so that each element of the experiment trusts their CA and certificates issued by their CA. This constitutes a public key infrastructure (PKI). Once this certification carried out, the key exchange between the various elements of the experiment can start. The paired 100G transponders receive up to one thousand 256-bit ″secret″ keys (i.e., ″red″ keys → GK, in Fig. 1) from KMS#1 and KMS#4, for the Tx and Rx, respectively. The transponder mixes one of this 256-bit GK with a 512-bit Diffie-Hellman key (i.e., ″purple″ key → DHK) generated inside the 100G transponder through a key derivation function (KDF) [8]. The resulting key (i.e., DHK + GK) is used to encrypt the 100G OTU-4 data stream. This process is performed every 60 seconds. To establish the end-to-end key transfer, the KMS#1 executes a XOR between GK and a first ″quantum″ key (″green″ key → QK-1) to obtain a ″network″ key (″blue″ key → NK-1) that can be considered as ″public″ and transmitted through the LAN up to the KMS#2, part of the first trusted node. The KMS#2 performs a XOR between NK-1 and QK-1 (transmitted from Alice#1 to Bob#1) so that GK can be recovered. The KMS#2 carries out a XOR between GK and a new ″quantum″ key (QK-2) so that to obtain a new ″network″ key (NK-2) sent to the KMS#3. The operation is repeated until reaching the KMS#4 where GK is extracted and sent to the end-link 100G transponder where the 100G OTU-4 data stream is deciphered by a process opposite to the one described above. The successful operation of the key management process is shown in Fig. 2 (right) on the network management system (NMS) of the 100G transponder, where we can see that the ″stored key count″ at Tx side has decreased, thus demonstrating that the 100G transponder uses the keys correctly.

## Results and discussions

Fig. 3 shows the results obtained in terms of secret key rate (SKR), quantum bit error rate (QBER) and pre-forward error correction code (pre-FEC) BER of the 400G channel, for various levels of the WDM comb power ($P_{WDM}$) injected into the SSMF (i.e., ~17, ~15 and ~13 dBm). Note firstly that the pre-FEC BER limit of the OFEC [10] (used in the 400G CFP2-DCO) was measured at ~$1.75 \times 10^{-2}$ and corresponds to a required OSNR (ROSNR) in back-to-back (BtB) of ~22.2 dB in 0.1 nm. Note secondly that for the LD#1 and LD#3-QKD systems the SKR and QBER are stable when the aggregated WDM comb power is varied, as the propagation of the quantum key and WDM signals are in two different fiber spans. As expected, the mean SKR over 24 hours of the two LD-QKD systems is higher than the one of the MU-QKD system (i.e., ~260 kbps for the LD#1 and ~272 kbps for the LD#3 against ~36.5 kbps at ~17-dBm, ~48 kbps at ~15-dBm and ~63 kbps at ~13 dBm for the MU#2). The end-to-end SKR is inferred from the lowest SKR, namely the one of the MU-QKD system. Identically, the mean QBER over 24 hours is better for the LD-QKD systems than for the MU-QKD one (i.e., ~3% for the LD#1 and 3.2% for the LD#3 against ~6.7% at ~17 dBm, ~6% at ~15 dBm and 5.4% at ~13 dBm for the MU#2). In all the cases, the pre-FEC BER of the 400G channel is well below the OFEC BER threshold (as shown in Fig. 3 (right)), as well as the received OSNR measured in 0.1 nm at ~29.7 dB at ~17 dBm, ~27.7 dB at ~15 dBm and 26.2 dB at ~13 dBm, namely largely above the ROSNR in BtB, that ensures error-free transmission of the 400G and 100-GbE data flow at the receiver side.

## Conclusion

We demonstrated transmission of a coherent 400-Gbps DP-16QAM channel that transports a QKD-secured 100-GbE data stream over 184-km of SSMF with other 54 WDM channels at 100 Gbps through three QKD links and two trusted nodes. One of the QKD section co-propagates over 50-km the quantum key and the ~17-dBm WDM comb, i.e., a power level compliant with the modern WDM systems deployed in the field.

## References


[1] S. Pirandola, U. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," *Adv. Opt. Photon.* **12**, 1012-1236, 2020, DOI: 10.1364/AOP.361502

[2] S.K. Rao, D. Mahto, D. K. Yahdav, D. A. Khan , ″The AES-256 Cryptosystem Resists Quantum Attacks,″ *Intern. J. Adv. Research Comp. Sci.* **8**, 404-408, 2017, DOI: 10.26483/ijarcs.v8i3.3025

[3] "OIF Implementation Agreement 400-ZR," www.oiforum.com; "OpenROADM MSA W-Port Digital Specification (200G-400G)," www.OpenROADM.org; "OpenZR+ MSA Technical Specifications," www.openzrplus.org/documents

[4] MU-QKD and LD QKD systems specifications, https://www.global.toshiba/ww/products-solutions/security-ict/qkd/products.html

[5] ITU-T SG15, ″OTN Sec : Security for OTN beyond 100 Gbps″, https://www.itu.int/md/T13-SG15-C-0110/en

[6] IEEE 802.3cu, "Physical Layers and Management Parameters for 100 Gbps and 400 Gbps Operation over Single-Mode Fiber at 100 Gbps per Wavelength", https://standards.ieee.org/standard/802_3cu-2021.html

[7] FSP-3000 Transponders and Muxponders specifications, https://www.adva.com/en/products/open-optical-transport/fsp-3000-open-terminals/transponders-and-muxponders

[8] ″Recommendation for Key-Derivation Methods in Key-Establishment Schemes,″ 2020, https://csrc.nist.gov/publications/detail/sp/800-56c/rev-2/final

[9] ITU-T G.709.OTU-4 long-reach Recommendation," www.itu.int/ITU-T/recommendations

[10] E. Pincemin, Y. Loussouarn, A. Sotomayor, G. Losio, M. McCarthy, L. Nelson, A. Malik, I. Riggs, T. Nielsen, T. Williams, A. Gaibazzi, L. Zhang, W. Way, F. Courchesne, and M. Vasconcellos, "927-km End-to-End Interoperable 400-GbEthernet Optical Communications through 2-km 400GBASE-FR4, 8x100-km 400G-OpenROADM and 125-km 400-ZR Fiber Lines," in Optical Fiber Communication Conference (OFC) 2022, Technical Digest Series (Optica Publishing Group, 2022), paper Th4A.3, DOI: 10.1364/OFC.2022.Th4A.3

[11] P. Gavignet, F. Mondain, E. Pincemin, A. Grant, L. Johnson, R. Woodward, J. Dynes, and A. Shields, "Co-propagation of 6 Tb/s (60* 100Gb/s) DWDM & QKD channels with ~17 dBm aggregated WDM power over 50 km Standard Single Mode Fiber," in Optical Fiber Communication Conference (OFC) 2023, Technical Digest Series (Optica Publishing Group, 2023), paper Tu3H.2.

[12] ETSI GS QKD 014 v.1.1.1, ″QKD; Protocol and data format of REST-based key delivery API,″ https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_QKD014v010101p.pdf