applied sciences

MDPI

Article

On the QKD Integration in Converged Fiber/Wireless Topologies for Secured, Low-Latency 5G/B5G Fronthaul

Dimitris Zavitsanos *, Argiris Ntanos, Giannis Giannoulis and Hercules Avramopoulos

School of Electrical and Computer Engineering, National Technical University of Athens,
9 Iroon Polytechniou Str., 15780 Athens, Greece; ntanos_arg@outlook.com (A.N.);
jgiannou@mail.ntua.gr (G.G.); hav@mail.ntua.gr (H.A.)
* Correspondence: dimizavitsanos@mail.ntua.gr; Tel.: +30-210-772-2871

Received: 30 June 2020; Accepted: 27 July 2020; Published: 28 July 2020

Featured Application: The results of this paper provide a reference for the future design of a quantum-secured 5G/B5G optical edge layer, assisted by novel integration strategies of Quantum Key Distribution (QKD) technological blocks across the deployed fiber/wireless fronthaul topologies.

Abstract: A research contribution focusing on the Quantum Key Distribution (QKD)-enabled solutions assisting in the security framework of an optical 5G fronthaul segment is presented. We thoroughly investigate the integration of a BB84-QKD link, operating at telecom band, delivering quantum keys for the Advanced Encryption Standard (AES)-256 encryption engines of a packetized fronthaul layer interconnecting multiple 5G terminal nodes. Secure Key Rate calculations are studied for both dedicated and shared fiber configurations to identify the attack surface of AES-encrypted data links in each deployment scenario. We also propose a converged fiber-wireless scenario, exploiting a mesh networking extension operated by mmWave wireless links. In addition to the quantum layer performance, emphasis is placed on the strict requirements of 5G-oriented optical edge segments, such as the latency and the availability of quantum keys. We find that for the dark fiber case, secret keys can be distilled at fiber lengths much longer than the maximum fiber fronthaul distance corresponding to the round-trip latency barrier, for both P2P and P2MP topologies. On the contrary, the inelastic Raman scattering makes the simultaneous transmission of quantum and classical signals much more challenging. To counteract the contamination of noise photons, a resilient classical/QKD coexistence scheme is adopted. Motivated by the recent advancements in quantum technology roadmap, our analysis aims to introduce the QKD blocks as a pillar of the quantum-safe security framework of the 5G/B5G-oriented fronthaul infrastructure.

Keywords: quantum key distribution (QKD); phase-coding BB84; secure key rates (SKRs); advanced encryption standard (AES); 5G/B5G packetized fronthaul; low-latency; coexistence scheme; raman noise; upconverted complementary metal-oxide-semiconductor (CMOS) photon counters

1. Introduction

The 5G-enabled ultra-low-latency networks aim to open the door to the era of Internet of Actions, where things will be getting connected and becoming even more intelligent to provide service in a fully automated environment [1]. This new era of smart connectivity means that cybersecurity is expanded to physical space, with life or death situations appearing in critical services such as autopilot hacking [1]. In this context, the end-to-end distributed security strategy has been manifested as one of the key technological blocks of the research roadmaps addressing the security threats in the 5G and Beyond-5G (B5G) era [2].

Approaching the age of Quantum Computing (QC), the definition of a quantum-resistant security framework becomes a top priority for the 5G-oriented infrastructure owners and operators. This strategy relies on the use of Post-Quantum Cryptography (PQC) through unbreakable cryptosystems [3], as well on the exploitation of Quantum Key Distribution (QKD) which is based on the laws of physics only [4]. The PQC offers compatibility with the existing cryptographic infrastructure, it is only secured against known quantum attacks though [5]. In contrast, the unconditional security of QKD has been ensured through several one-time-pad demonstrations encryption across quantum networks [6]. Since the QKD is a symmetric key algorithm which cannot replicate all the functionalities of public-key cryptography [5], a joint PQC/QKD encryption scheme where quantum-resistant algorithms can have access to the secure shared key material from QKD has been manifested as the quantum-safe infrastructure layer [7]. In this direction, the development of hybrid key exchange protocols being resilient to the advances in quantum computing has emerged as an initial deployment candidate [8].

In the context of PQC, a range of algorithms is being evaluated under the NIST program [9], leading to Draft Standards in two to four years. Besides the standardization process, ADVA was recently presented through field-trials, PQC-based 100G safe optical transport over long-haul fiber links utilizing a public-key encryption system based on the variant of the Niederreiter scheme [10].

On the other hand, the major advantage of QKD is that it solves the key distribution problem in symmetric cryptosystems. Therefore, the distilled secret key can be used to encrypt a message using a symmetric algorithm, such as the Advanced Encryption Standard (AES), which is known to be quantum-resistant [11]. QKD offers a key distribution whose security is based on the most fundamental laws of nature and specifically on the laws of quantum mechanics and promises in principle unconditional security. However, even though the unconditional security of QKD has been proved for several protocols, such as the well-known BB84 [12–14], there is a gap between the ideal and the practical implementations of QKD protocols, which may lead to security loopholes, since the security proofs are commonly based on idealized setups. These security loopholes have triggered the scientific community to invent and, on a second stage, to implement more resilient schemes [4,15]. Additionally, the QKD exchange requires an initial authentication step, which requires a pre-shared secret. This initialization step can be performed by quantum-resistant algorithms. Once QKD has been performed, the security of these algorithms is no longer important, since the distilled secret key has no algorithmic link to the pre-shared key used to authenticate the QKD exchange [16]. Furthermore, the practical implementation of QKD also faces many technological challenges at the moment, such as the relatively low detection rate, the difficulty of fabricating low-noise and high-efficiency photon counters and the task of increasing the communication distance [4]. However, in the last decade, many encouraging steps have been made by quantum technology vendors and research community dealing with these limitations [17,18]. Driven by the momentum of photonic integration to meet the needs of classical photonic systems, emphasis has been placed on the integration of innovative QKD building blocks (sources, detectors) on well-established integration platforms [19], targeting compact, low-power and cheap quantum blocks.

In the era of QKD demonstrations, the integration of QKD signals into existing backbone fiber networks has been extensively studied showing the potential of co-propagation of quantum links with Tbps data channels [20]. The practicality of the quantum solutions has also been confirmed through the deployment-oriented integration of commercially available Discrete Variable-QKD (DV-QKD) with Wavelength Division Multiplexing (WDM)-enabled optical transport layer [21]. Moving towards optical edge layer, the integration of quantum channels has also been demonstrated through experiments in Passive Optical Network (PON)-segments [22]. Multiplexing of both quantum and classical streams into existing edge infrastructure remains a challenge since the presence of classical data signals in a live fibre makes the retrieval of quantum information more difficult due to excess noise generated by inelastic Raman scattering [23]. Besides the physical connectivity-oriented experiments, the QKD-enabled real-time encryption layer-1 in the field has been demonstrated using an AES-256 engine [24]. University of Bristol recently demonstrated the first end-to-end quantum secured inter-domain service orchestration by interconnecting 5G autonomous islands through quantum-enabled multiplexing nodes [25]. Very recently, a quantum-secured 5G-oriented fronthaul architecture over Multicore Fiber (MCF) was presented by assigning the quantum and fronthaul signals at different cores to prevent the contamination [26]. The potential of this MCF-based concept to meet the traffic demands of the 5G fronthaul was also verified for short fiber segments by demonstrating record coexistence transmission of DV-QKD with 11.2 Tbps classical channel traffic [27].

Welcoming the integration of quantum layer across the 5G and B5G cryptographic infrastructure, end-to-end studies targeting beyond the optimized classical/QKD coexistence scheme are still missing. More specifically, further studies are required to explore the capability of a QKD-enabled security framework to meet the strict requirements of 5G-oriented optical edge segments, such as the latency and the availability of quantum keys for AES-based encryption engines. An impressive study recently conducted emphasizing on the latency budget as well the security levels of an optical fronthaul segment operated by the evolved Common Public Radio Interface (eCPRI) [28]. Inspired by the above research, we take a step forward by presenting, for the first time to the best of our knowledge, a research study focusing on the QKD-enabled solutions assisting in the PLS of an Ethernet-based optical 5G fronthaul segment. Working towards the synergy between QKD/PQC presented above, the secure shared key resources which are available from QKD links should be also addressed in the context of the existing security infrastructure. Our research fills this gap by contributing to the definition of security parameters (quantum keys for AES encryption engines, key rotation times, attack success probabilities) of an eCPRI transport layer supported by QKD implementation. Considering the strict latency requirements imposed for 5G packetized fronthaul, performance evaluation is thoroughly discussed for Point-to-Point (P2P) topology as well as in a Point-to-MultiPoint (P2MP) scenario with a centralized Alice station supporting up to N = 64 Bob stations located at 5G terminal nodes. Emphasis has been placed on a resilient classical/QKD coexistence scheme by relying either on appropriate wavelength assignments or on the use of advanced photon detection units at the Bob stations. We also study on the security parameters by exploiting the QKD for the fiber-connected mmWave nodes, key technological blocks for the converged optical-radio infrastructure of 5G networks.

The rest of the paper is organized as follows: Section 2 describes the concept of the proposed quantum-secured eCPRI transport layer operating in both P2P and P2MP optical segments. Different fiber assignments using either dedicated or shared links for the quantum transmission are thoroughly investigated. In addition, a Fiber-Wireless topology supporting the secured P2MP distribution using mmWave nodes is proposed. The details about the physical connectivity implementation and the followed methodology for the DV-QKD layer are also discussed in this section. Section 3 presents the performance evaluation results and discusses the main outcomes and challenges for each deployment scenario. Section 4 briefly introduces a technological path in support of the QKD integration within existing deployed infrastructure in 5G/B5G-oriented topologies. Finally, Section 5 concludes this work.

2. Materials and Methods

The demand for a packet-switching-based fronthaul network has led to an enhanced version of CPRI (eCPRI [29]), which is designed for packet networks, namely Ethernet and IP. Even though Ethernet was not originally designed for delay-sensitive networks or real-time applications, intensive research efforts have been devoted [30] which are mainly based on the IEEE 802.1CM published in 2018 [31]. Apart from the above efforts towards Time Sensitive Networking for Fronthaul, eCPRI recommends that vendors optionally implement either MACsec or IPsec as security options [28]. In this context, we propose and study the use of a QKD solution to make quantum safe the key exchange which is needed for the implementation of the above security standards. We extend the study of physical layer implementation of the proposed quantum layer by considering the strict latency-related requirements of the fronthaul segments.

2.1. Dark Fiber Topology

The first part of our study focuses on the performance of a typical 5G Ethernet-based fronthaul segment operating with eCPRI interfaces, for which the Alice station for QKD layer was hosted on the Baseband Unit (BBU) node while a dark fiber link was considered for the distribution of quantum keys to the Bob station located at the 5G Terminal Node, as illustrated in Figure 1. The selection of an equal length telecom fiber for the QKD layer allows for a quantum transmission without the contamination of noise photons associated with the presence of intense classical data flows. The use of eCPRI transport layer facilitates the splitting of some of the baseband functions between the Radio Equipment Control (REC) hosted at the Baseband Unit (BBU) Node and the Radio Equipment (RE) at the 5G Terminal Node. In our study, we assumed a fixed transport line rate of 10Gbps over the dedicated fiber link.

This topology should also be subject to the 5G fronthaul latency requirements imposed for low-latency services. More specifically, the sum of transmission delays and baseband processing time at BBU must be less than 3ms [28]. In contrast to the reported methodology in [28] where the exchange of symmetric keys was realized over the classical communication channel, our proposed distribution scheme of quantum keys between the REC and RE nodes is naturally dependent on the fiber fronthaul distance. This link distance dependence appeared since the optical loss eliminates the photon detections at the Bob station, thereby lowering the available Raw Key Rate and subsequently the Secure Key Rate (SKR) for the AES-based encryption/decryption engines. Concerning the latency components of the fronthaul segment, the QKD layer introduces an additional latency component associated with the key distillation process, an essential post-processing step to guarantee the unconditional security. As calculated in Appendix A, for a round-trip processing of less than 3 ms, the fiber fronthaul distance is limited to be less than 17 km.

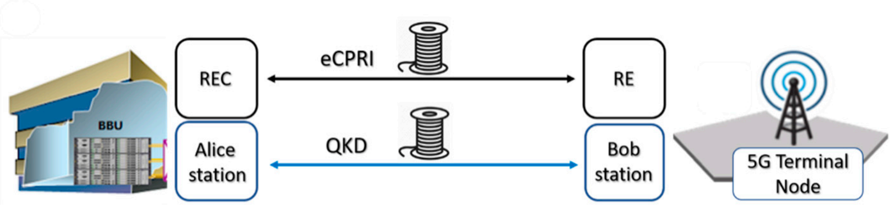


Figure 1. Quantum-secured evolved Common Public Radio Interface (eCPRI) transport layer interconnecting the Baseband Unit (BBU) and the 5G terminal nodes. A dedicated fiber link is used for quantum key exchange between Alice and Bob stations.

Moving towards networks where multiple 5G terminal nodes need to establish a secure communication link with a centralized BBU node, there exist two alternative approaches for the interconnection of the QKD stations undertaking this task. The first one lies in the one-to-one dedicated links interconnecting the number of Alice and Bob stations respectively. On the other hand, if one node hosts the source or the detection unit serving more than one link, then this could lead to significant complexity and cost reduction, at the expense of lowering the key rates. Recently, a time-division multiplexing (TDM) technique was demonstrated using a single set of photon detectors (one Bob station) to establish QKD channels with four users (four distinct Alice stations) [32]. Driven by the ongoing developments on the miniaturization of upconversion-assisted silicon photon detectors relying on the use of integrated quantum photonic chips [33], we present a scheme where one centralized transmitter (Alice) can communicate with multiple quantum receivers (Bob stations). This approach can also exploit the centralized baseband resources to efficiently perform the postprocessing modules at higher speeds for correcting the quantum-channel noise errors and distilling identical corrected keys between Alice–Bob stations.

Figure 2 shows the modification of our proposed secured fronthaul layer to support multiple 5G terminal nodes. This multi-user extension relies on the use of a centralized Alice station distributing single-photons to multiple Bob stations located at the Remote Radio nodes. In more detail, a single-photon emitter (Alice) is located in the BBU and a single and independent Bob station (quantum receiver) for each one of the 5G terminal nodes of the network. Therefore, the number of (N) Bob stations is equal to the number of (N) 5G terminal nodes assumed in our topology. In this way, each Bob (and so each 5G terminal node) is supplied with a unique, randomly selected subset of bits (1/N) from the bit string that Alice transmits at the feeder fiber [34]. These independent keys are then used for the security of each of the fiber segments connecting the BBU and the terminal nodes, through AES-based encryption/decryption engines. The independency of the multiple distilled keys lies in the fact that any single photon incident in the passive 50:50 splitter stage cannot split, but it follows only one output path in a completely random way. Even though an attenuated laser source may emit multiphoton states which could split when entering a splitter and the splitting ratio of each splitter may not be ideal (e.g., 51:49), it has been shown [34] that the level of correlation between the individual bit strings is extremely low. In our proposed topology, a single feeder is assumed to link the BBU and the splitter stage, and N terminal nodes were optically connected through drop fiber segments of equal lengths (small compared to feeder fiber length). Besides the 3 dB splitting ratio associated with each stage, an additional 0.2 dB insertion loss is assumed for each splitter to study on a more realistic scenario for the installed passive fiber segment. To combat the increased optical loss linked with the 1:N splitter stage and to increase the obtained SKR, photon counters with lower noise count rates were also considered.

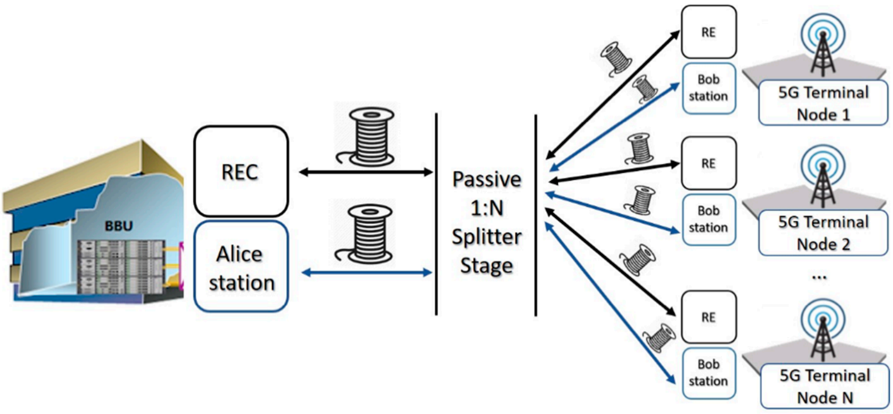


Figure 2. Quantum-secured multi-user topology with a centralized Alice station and multiple Bob stations located at the 5G terminal nodes. A passive optical distribution network based on 1:N splitter stage implements the P2MP topology with dedicated fiber segments for classical and quantum layer respectively.

The performance evaluation of the proposed secured fronthaul segments was carried out through numerical simulations based on the physical connectivity parameters as well the AES-256 security layer. For the quantum layer of P2P implementation, we considered a plug and play phase coding BB84-QKD system, based on the well-known Cerberis2 [35] and id3100 Clavis2 [36] from idQuantique [37], operating at 1550nm over a Standard Single-Mode Fiber (SSMF) with an attenuation of α_q = 0.2 dB/km and visibility set at V = 98%, where the optical pulses are generated from a highly attenuated laser source at Alice's site, with a repetition rate of f_{rep}= 5 MHz. At this low pulse repetition rate, the chromatic dispersion of fiber medium cannot significantly broaden the pulsewidth [38]. The photons were assumed to be detected at Bob's station by a pair of Single-Photon Avalanche Diodes (SPADs) operated in gated mode with a detection time-window of 1 ns. Both SPAD units were assumed to exhibit a dead time of 0.1 μs and an afterpulse probability of 0.8%. The obvious selection of photon counters at telecom wavelengths are the avalanche photodiodes working in Geiger mode, for which a dark count rate (DCR) of 5×10^{-6} ns^{-1} and a quantum efficiency of 10% were assumed. These values correspond to the typical performance of the widely used InGaAs modules photon counters for single-photon detection at telecom wavelengths [39]. The high DCR that these modules exhibit can significantly limit the transmission distance where no secure key can be distilled anymore. In order to overcome this limitation, we also considered the use of Silicon (Si) SPAD modules in Bob stations, offering significant advantages such as operation at room temperatures without the need of complex cooling mechanisms, higher values of quantum efficiency with very low timing jitter and much lower noise and dark current. To take advantage of the above benefits at telecom wavelengths where Si-based photon counters are virtually blind, an upconversion module is required to translate the wavelength of the incoming telecom single-photons into the visible range. In our study, we adopted at Bob stations an upconversion-assisted single-photon detection scheme based on an integrated periodically poled lithium niobite (ppLN) waveguide pumped by long wavelengths at 2 μm [40]. Based on the reported results in [40], a total efficiency of 10% and a dark count rate (DCR) of 6×10^{-8} ns^{-1} were assumed. Finally, the optical loss of the internal components at Bob station was fixed at 2.65 dB.

The calculation of SKR was carried out assuming general incoherent attacks in the presence of multiphoton pulses, via the theoretical treatment in [41], while adopting the approximation that the optimized average photon number per pulse is equal to the fiber link Transmittance: μ ~ T [35,41]. Following that approach, the sifted key rate can be calculated as follows

$$R_{sift} = (p_{\mu} + 2p_{dc} + p_{ap}) f_{rep} \eta_{duty} \eta_{dead}, \tag{1}$$

from which the secret key rate is derived by

$$R_{\mathrm{sec}} = R_{sift}(I_{AB} - I_{AE}), \tag{2}$$

where p_{μ}, p_{dc}, p_{ap} are the signal detection, the dark count and the afterpulse probabilities per gate duration time (=1 ns), respectively, η_{duty} captures the duty cycle imposed by the plug and play protocol synchronization requirements, η_{dead} accounts for the reduced detection rate due to SPADs dead time and I_{AB}, I_{AE} are the mutual information per bit between Alice and Bob and between Alice and Eve (a potential eavesdropper), respectively [35,41].

The secret key established from the DV-QKD protocol was then used to encrypt/decrypt the data transmitted between the BBU and the 5G terminal node via the AES-256, by exploiting a pair of Ethernet encryptors. Through our study, we specified the SKR values required for the data encryption, under three different key refresh times which, in turn, lead to different attack surfaces. As specified in [42], a very low key refresh time equal to 1.4 s can be achieved from the key management layer according to the recently reported standardization document by QKD engines providers [42], thereby guaranteeing lower attack surfaces. To achieve this rotation time which boosts the security level, a SKR of at least approximately 256 bits/1.4 s = 183 bps should be available after the post-processing steps of QKD layer. Since this SKR target significantly limits the QKD transmission range, we also considered a scenario with increased size of attack surface. More specifically, a longer refresh time equal to 1 min, which is a frequently reported order of magnitude value in bibliography [24,35,43], was also selected. To satisfy this rotation time, SKR values of at least 256 bits/1 min = 4.3 bps SKR are demanded. Lastly, we considered a longer key refresh time value equal to 5.14 min. This value corresponds to the lower bound of SKR such that Attack Success Probability (ASP) can be kept below 2^{-60}. More specifically, in [44], the ASP for a confidentiality attack was compared to the maximum amount of data that can be processed. In order to keep the ASP as low as possible, i.e., at 2^{-60}, the maximum data that can be transmitted is about 0.3887 terabytes [44]. By assuming a 10 Gbps packetized data flow over eCPRI transport layer, a key generation rate of at least

$$\frac{256 \text{ bits} \times 10 \times 10^{9} \text{ bps}}{8 \times 0.3887 \times 10^{12} \text{ bits}} \cong 0.83 \text{ bps} \tag{3}$$

is required to feed the AES-256 cryptographic engine to preserve the ASP below 2^{-60}, which corresponds to 256 bits/0.83 bps = 5.14 min refresh time.

2.2. Shared Fiber Topology

As a next step, we considered a shared fiber link for classical and quantum transmission. Specifically, the packetized classical data flow propagated from the BBU node and the 5G Terminal Node (and vice versa with symmetrical transport) and the photon transmission from Alice to Bob is performed over a shared SSMF link, as illustrated in Figure 3. This shared use of fiber installations would boost the compatibility of quantum communications with existing optical infrastructures and lead to a significant improvement in terms of cost-effectiveness and addressable market for QKD [45].

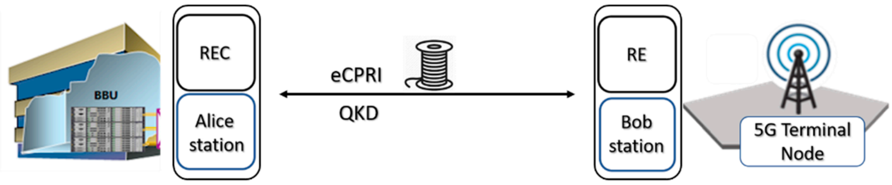


Figure 3. Quantum-secured eCPRI transport layer interconnecting the BBU and the 5G terminal nodes. One Standard Single-Mode Fiber (SSMF) link is used for both packetized classical data flow from the BBU node and the 5G Terminal Node (and vice versa) and for the photon transmission from Alice to Bob.

In this proposed coexistence setup, the performance of the quantum channels suffers mainly from the nonlinear effect of Spontaneous Raman Scattering (SpRS), arising from the inelastic scattering of the strong bidirectional classical data signal with fiber material. The forward scattered Raman power, generated by the downlink, is obtained by [46,47]

$$P_f = P_{\mathrm{dl}} \rho_{\mathrm{dl}} \Delta\lambda \frac{e^{-\alpha_q L} - e^{-\alpha_{\mathrm{dl}} L}}{\alpha_{\mathrm{dl}} - \alpha_q}, \quad (4)$$

where P_{dl} is the launch power of the downlink, ρ_{dl} is the effective Raman cross-section, $\Delta\lambda$ is the quantum receiver spectral bandwidth, which is set to 0.8 nm, L is the propagation distance and α_{dl}, α_q are the fiber attenuation coefficients for the downlink's wavelength and the quantum channel's wavelength respectively. The uplink generates backward scattered Raman photons with power given by [46,47]

$$P_b = P_{ul} \rho_{ul} \Delta\lambda \frac{\left[1 - e^{-(\alpha_{ul} + \alpha_q) L}\right]}{\alpha_{ul} + \alpha_q}, \quad (5)$$

where P_{ul} is the launch power of the uplink, ρ_{ul} is the effective Raman cross-section and α_{ul} is fiber attenuation coefficients for the uplink's wavelength. In this coexistence topology, Equation (1) has to be modified to account for the contribution of Raman noise to the SKR, by adding the Raman photon detection probability (calculated by expressing the forward and backward Raman power levels in terms of noise photons per ns (gate duration time) [23,35,48]) to the other detection probabilities. To be able to select the quantum information transmitted through the shared fiber, we considered a bandpass optical filter at Bob's side, introducing a wavelength independent loss of 2.7 dB. This filter is assumed to spectrally isolate the quantum passband, therefore no leakage photons due to classical power can be recorded due to the crosstalk. This assumption can be easily met, by keeping the channel spacing between the downlink and the quantum signal large enough (~400 GHz [38]).

Raman Scattering mechanism covers an ultra-broadband window and gets stronger as the propagation distance increases. Strictly speaking, it is maximized at a specific propagation distance, depending on the fiber attenuation value (>20 km for each wavelength allocation we encountered), longer than distances for which SKR can be established for shared topologies, after which it decreases slowly. It is also worth mentioning that in C-band topologies, besides the Raman scattering, the Kerr-based effects (e.g., FWM) should be taken into consideration, since they could contribute a significant amount of contamination photons which would increase the QBER performance [48–51].

In order to investigate in depth the magnitude of contamination of QKD links by Raman scattering photons in realistic network topologies, we considered two different wavelength allocations for the classical signals. In the first case, the quantum channel at 1550 nm is multiplexed with the classical signals at 1310 nm (downlink) and at 1490 nm (uplink). A much better system performance can be obtained by moving the uplink at the O-band too (i.e., at 1310 nm for both downlink and uplink, where the losses are assumed to be 0.35 dB/km [52]), where the impact of SpRS gets weaker on the quantum channel operated at single-photon regime at 1550 nm. By spectrally separating the quantum and classical channel between the O-band and the C-band, the Raman contamination can be significantly limited [53]. In the first configuration, the evaluation of Raman power was performed assuming $\rho_{dl} = 8 \times 10^{-10} (\text{km}{\cdot}\text{nm})^{-1}$ and $\rho_{ul} = 6.8 \times 10^{-9} (\text{km}{\cdot}\text{nm})^{-1}$, while for the second $\rho_{dl} = \rho_{ul} = 8 \times 10^{-10} (\text{km}{\cdot}\text{nm})^{-1}$ [47]. These values are typical for a single-mode fiber and correspond to the specific wavelengths that have been assigned for the classical signals. The launch power for both classical signals was set to 0 dBm, preventing the classical/quantum multiplexing scenario at C-band owing to the strong presence of Raman contamination photons [48].

The P2MP extension of our proposed coexistence scheme is depicted in Figure 4. Exploiting the existed fiber assets for transferring both classical data flows and quantum channels becomes even more essential for P2MP topologies where many mobile terminal nodes are interconnected through drop fibers. This shared strategy allows for significant cost-savings in ultra-dense mobile transport networks of 5G networks where the deployment costs for new fiber segments are a significant component of the total infrastructure cost [54].

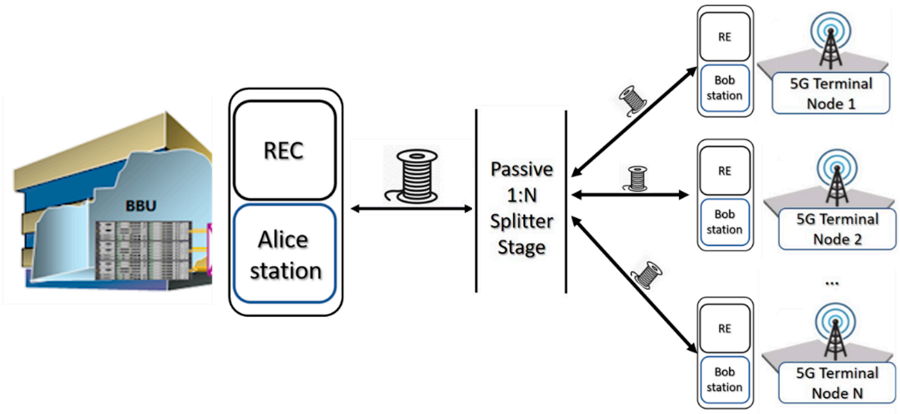


Figure 4. Quantum-secured multi-user topology with a centralized Alice station and multiple Bob stations located at the 5G terminal nodes. A passive optical distribution network based on 1:N splitter stage implements the P2MP topology with shared single-mode fiber segments for classical and quantum layer.

The Raman noise photons behave in the same way as the Alice's encoded photons while they are transmitted from the feeder to the drop fiber segment. Therefore, even though the splitter stage puts significant pressure on the quantum layer by lowering the sifted key rate due to photon loss, the same behavior is also obtained for the noise count rates due to Raman contamination photons. Consequently, we expect that, as the number of users increases, the maximum feasible transmission distance will be getting decreased to a lesser extent compared to the P2MP scenario utilizing dedicated fiber links for classical and quantum layers, respectively. The wavelength allocation of the classical signals is considered the same as described for the P2P case. In Section 3, SKR calculations are presented for the above topologies for both InGaAs and Si SPADs and for different key rotation times.

2.3. Fiber-Wireless Topology

The final part of our study aims to investigate alternative implementations of the P2MP topology, relying on the use of a mesh networking operated by mmWave wireless links. The mmWaves have been manifested as wireless fibers since they can provide reliable multiple gigabit capacity and they gain more and more ground in the field of Fixed Wireless Access (FWA) [55]. The integration of directional mmWave links over the installed Passive Optical (PON) legacy infrastructure has been recently reported [56], verifying the potential of their successful coexistence with the existing deep fiber installations. Besides the attractive properties in terms of data transport capabilities, the pencil-beam antennas as well the high free-space-loss at these frequencies ensure spatial isolation and guarantee interference-free performance. These characteristics also enhance the security of mmWave communications by protecting from passively eavesdropping and actively jamming [57]. When malicious eavesdroppers want to intercept and decode the confidential messages successfully, they need to physically be within the transmission path of mmWave signals with narrow beams. To this end, we propose a hybrid Fiber-Wireless (Fi-Wi) P2MP topology to deliver secured keys to multiple 5G terminal nodes where the optical segments can be safeguarded using QKD between the optical nodes and the wireless link is fortified through enhanced security features provided by the ultra-narrow mmWave beams.

Figure 5 illustrates the proposed Fi-Wi topology supporting the secured P2MP distribution using mmWave nodes to interconnect several 5G terminal nodes which are physically connected with mmWave mesh clients. In this topology, a shared fiber infrastructure is assumed for the interconnection of the BBU and the multiple mmWave mesh nodes. This shared fiber segment is assumed to support the secret key establishment, the classical data transmission and the communication protocols implementing the radio controller functions. For the needs of our analysis, each mesh node communicates, in turn, with four mesh clients via an Over-The-Air (OTA) link. This assumption can be easily satisfied from the radio equipment vendors providing 360-degree coverage mesh node [58]. Since the distilled secret keys at Bob stations located at mesh nodes are used to encrypt both the packetized data flow as well the Radio control and management messages, the key rate demands are significantly increased. In our study, we considered the use of parameters provided by commercially available mmWave radio nodes including the full list of their control functions involving encryption. According to the documentation provided by radio equipment vendor Siklu, the encryption of four control and management functions is based on the use of AES algorithm with maximum key lengths of 128 and 256 bits, respectively [59]). As was discussed in Section 2.1, by tuning the key rotation times to achieve different attack surfaces, a different amount of SKR is required. Regarding the latency component added by this mmWave link, the typical latency of the 10 Gbps Frequency Division Duplexing (FDD) radios is about 10 µsecs [60], leading thereby to a slightly shorter fiber distance of 17 km which satisfies the end-to-end latency budget of 3 ms for ultra-low services. The use of Time Division Duplexing (TDD) radios adding a typical latency of 350 µsecs can be considered for scenarios where delay insensitive services are targeted.

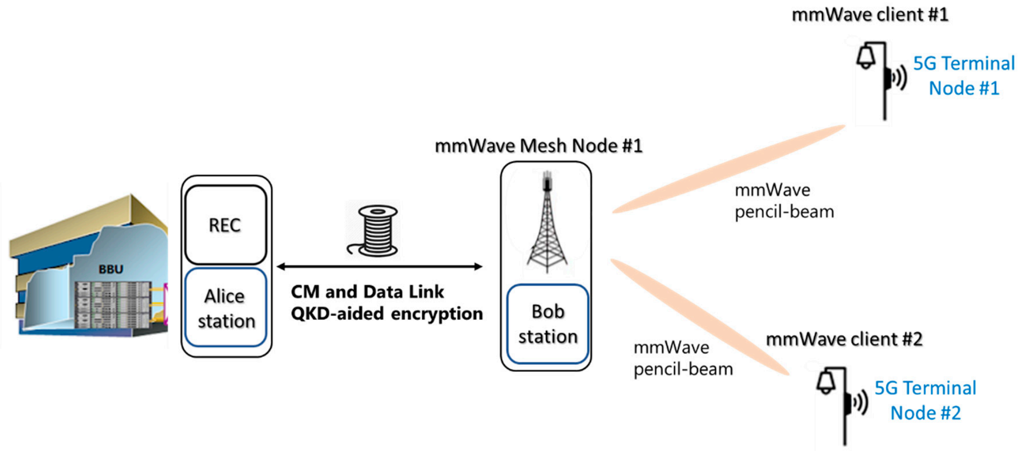


Figure 5. Fi-Wi topology supporting the secured P2MP distribution using mmWave nodes to interconnect several 5G terminal nodes which are physically connected with mmWave mesh clients.

3. Results

In this section, detailed performance evaluation results are presented. Section 3.1 provides our results from P2P and P2MP topologies using dedicated fiber links for classical and QKD links, while Section 3.2 addresses the performance of P2P and P2MP topologies using shared fiber links for the propagation of both classical and quantum channels. In Section 3.3, performance evaluation results are presented for the P2MP topology based on a mesh radio networking through wireless nodes.

3.1. Performance Evaluation of Dark Fiber Topology

Figure 6 illustrates the evaluation of SKR for the P2P link, as a function of fiber distance between the REC and RE nodes, for the case where dark fiber is used for the quantum link.

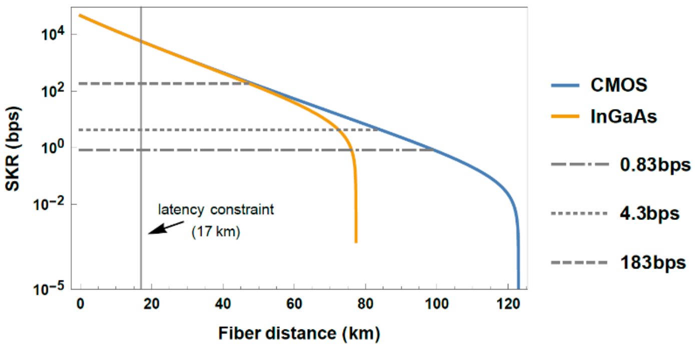
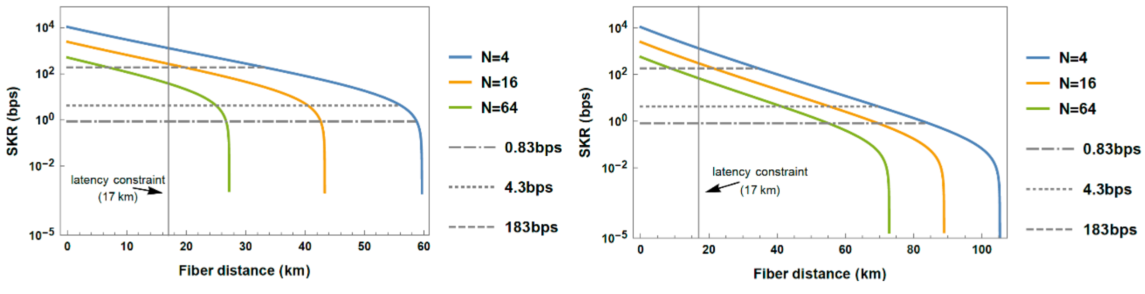


Figure 6. Secure Key Rate (SKR) as a function of fiber length, for the P2P dark fiber link, for both InGaAs and upconverted CMOS-based Quantum Key Distribution (QKD) setups. The horizontal lines with different styles correspond to the Advanced Encryption Standard (AES) limits for key refresh times equal to 5.14 min (0.83 bps), 1 min (4.3 bps) and 1.4 s (183 bps), respectively.

It is evident that in this topology the dedicated link offers a feasible transmission with sufficiently long-distance range. Both photon counters QKD setups show an identical behavior for fiber segments up to approximately 70 km. Even for the case of fast key refresh times of 1.4 s, acceptable SKR values can be achieved for both types of photon counter at ~50 km, a longer distance than 17 km, which corresponds to round-trip latency barrier as was calculated in Appendix A. Therefore, for relatively short distances, which correspond to fronthaul segments where the low-latency requirement is crucial, the InGaAs setup can offer the same performance as the upconverted silicon SPADs. The advantage of using CMOS SPADs is revealed only at distances longer than 70 km, where the difference between the DCR that the two types of photon counters exhibit, as stated in Section 2.1, causes its impact. Obviously, these long fiber lengths exceed the maximum fronthaul distances considered for 5G-oriented environments. Nevertheless, as we shall see below, the use of CMOS SPADs could benefit the QKD performance even at very short fiber lengths, in shared fiber topologies where the presence of intense classical signals can severely contaminate the quantum passband.

The SKR calculation for the P2MP scenario is depicted in Figure 7 by considering $N = 4$, $N = 16$ and $N = 64$ users, respectively.

In this P2MP scenario, as the number N of terminal users increases, the photon loss stemming from the cascaded splitter stages increases too, leading thereby to a lower SKR. This performance is resembled at the maximum key rates that can be distilled at sub-km fiber segments: the ~10 kbps/user for the case of $N = 4$ users is reduced down to ~800 bps for the case of $N = 64$ users. The SKR benefits raised using silicon SPADs are evident only at a distance longer than approximately 27 km for the case of $N = 64$ users (i.e., the maximum length at which the InGaAs QKD setup can distill secret keys) and at even longer fiber segments for the case of $N = 16$ and $N = 4$ users, respectively. At these long fiber distances of P2MP links, which could be applied to 5G-oriented services where the low-latency requirement is not critical, the silicon SPADs operating at lower DCR allow for secret key distillation with higher rate (i.e., lower key rotation times) than the InGaAs do. For shorter distances, where the low-latency requirement is met (<~17 km), the SKR behavior is almost identical for both types of detector.

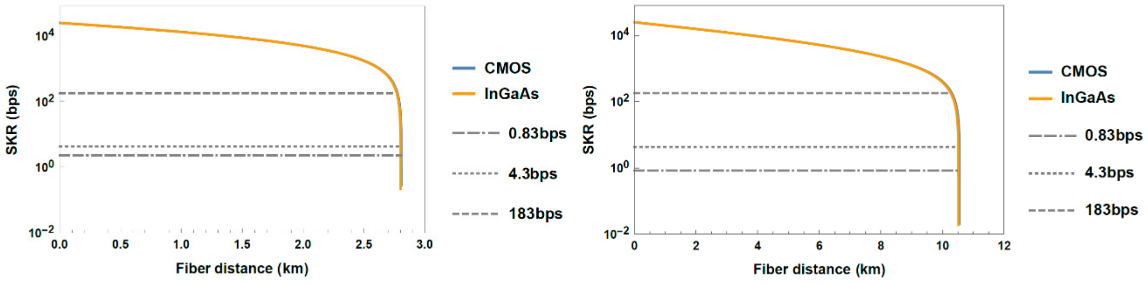


(**a**) (**b**)

Figure 7. SKR as a function of fiber length, for the P2MP dark fiber link serving $N = 4$, 16 or 64 users, for (**a**) InGaAs; and (**b**) upconverted CMOS-based QKD setups. The horizontal lines with different styles correspond to the AES limits for key refresh times equal to 5.14 min (0.83 bps), 1 min (4.3 bps) and 1.4 s (183 bps), respectively.

3.2. Performance Evaluation of Shared Fiber Topology

Moving to the shared fiber configuration, the Raman noise photons generated by the interaction of intense classical flows with the fiber medium strongly degrade the quantum layer performance, as is shown in Figure 8 for the P2P scenario.



(**a**) (**b**)

Figure 8. SKR as a function of fiber length, for the P2P shared fiber link, for both InGaAs and upconverted CMOS-based QKD setups, where: (**a**) the quantum channel at 1550 nm is multiplexed with the classical signals at 1310 nm (downlink) and at 1490 nm (uplink); (**b**) the quantum channel at 1550 nm is multiplexed with the classical signals at 1310 nm for both downlink and uplink. The horizontal lines with different styles correspond to the AES limits for key refresh times equal to 5.14 min (0.83 bps), 1 min (4.3 bps) and 1.4 s (183 bps), respectively.

In Figure 8a, SKR calculations, while the downlink is located at 1310 nm and the uplink at 1490 nm, are presented. Kbps rates are achievable but only for few km-long fiber segments, since eventually the quantum passband becomes severely contaminated with the Raman noise photons, and subsequently the SKR approaches close to zero at ~2.8 km. An improved performance can be obtained by also shifting the wavelength allocation of the uplink at 1310 nm. This enhanced version of coexistence scheme is feasible since the Raman scattering photons generated by an O-band pump has a relatively low impact to the C-band spectral windows (i.e., lower effective Raman cross-section, ρ_{ul}). For this channel allocation, the distillation of secret keys is feasible even for 10.5 km (Figure 8b), a significant improvement compared to the previous case. We can also conclude, in both the above cases, that the noise coming from the SpRS is much stronger than the noise component associated with the dark current of the photon counter, since the blue (SKR for CMOS) and the orange (SKR for InGaAs) plots exhibit practically identical performance.

In a potential case of a fully loaded optical topology, where many classical channels in WDM systems are co-transmitted along with the quantum channel, the Raman noise would be significantly increased. To mitigate the presence of these Raman contamination photons in this scenario, the realization of a quantum channel within L-band could be an option, benefited from the even lower Raman gains for these longer wavelength assignments [53].

It is worth noting that the DCR of the photon counters at Bob stations affects only the transmission distance, not the maximum key rate that can be obtained. Since we assumed, for the upconverted modules, a value of total efficiency 10% which is equal to the assumed value of quantum efficiency for the InGaAs counters, as mentioned in Section 2.1, there is no performance benefit for using the CMOS counters in this shared fiber P2P topology. To make clear how the detector's efficiency affects the SKR, we also assumed a hypothetical scenario with an upgraded CMOS counter efficiency equal to 20%. This slightly improved SKR performance is depicted in Figure 9.

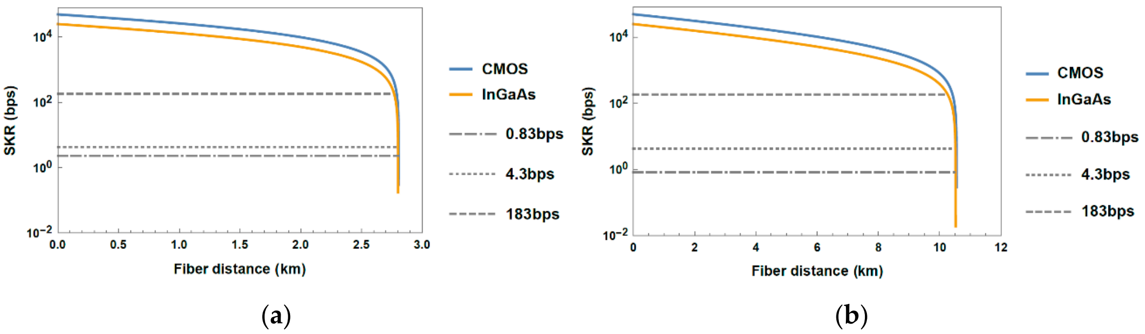


Figure 9. SKR as a function of fiber length, for the P2P shared fiber link, for both InGaAs and upgraded (i.e., with total efficiency equal to 20%) upconverted CMOS-based QKD setups, where: (**a**) the quantum channel at 1550 nm is multiplexed with the classical signals at 1310 nm (downlink) and at 1490 nm (uplink); (**b**) the quantum channel at 1550 nm is multiplexed with the classical signals at 1310 nm for both downlink and uplink. The horizontal lines with different styles correspond to the AES limits for key refresh times equal to 5.14 min (0.83 bps), 1 min (4.3 bps) and 1.4 s (183 bps), respectively.

The evaluation of SKR for the P2MP topology is illustrated in Figure 10. From this point forward, we will consider only the allocation where both classical signals are located at 1310 nm, since in this configuration the quantum passband is more resilient to the Raman scattered photons generated by the O-band pumps, as explained above.

As expected, the key rate drops significantly as the number of terminal users increases, which has an immediate impact on the key rotation times. For example, for the CMOS photon counters QKD setup coexistence scheme (Figure 10b), for 4 users a rotation time equal to 1.4 s (i.e., 183 bps low limit) can be set even at approximately 9.5 km. However, for 64 users the maximum feasible distance which allows this low-key rotation time is limited to 2 km.

On the other hand, as explained in Section 2.2, since both the encoded photons generated from Alice and the Raman noise photons suffer the same loss from the splitter stage, the maximum transmission distance for which secret keys can be distilled is not heavily compromised compared to the P2P shared fiber scenario. More precisely, for the InGaAs photon counters QKD setups, this distance is slightly reduced as the number of users increases (Figure 10a). On the contrary, for the CMOS setups, the maximum distance is almost unchanged, as can be seen from Figure 10b.

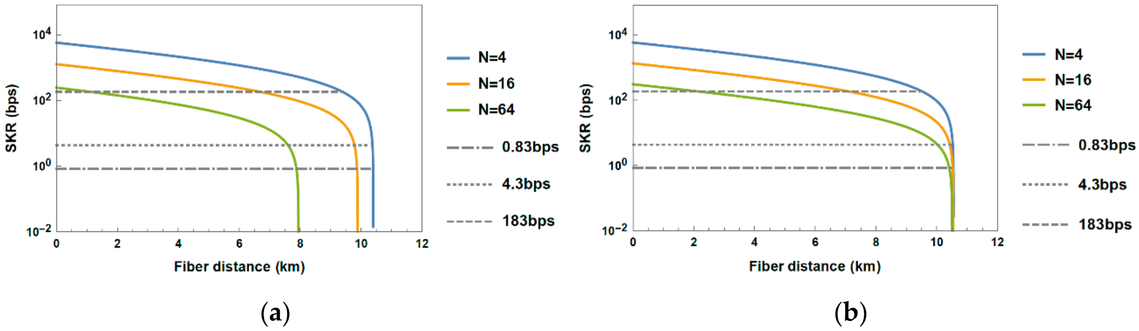


Figure 10. SKR as a function of fiber length, for the P2MP shared fiber link serving $N = 4$, 16 or 64 users, where the quantum channel at 1550 nm is multiplexed with the classical signals at 1310 nm for both downlink and uplink, for (**a**) InGaAs; and (**b**) upconverted CMOS-based QKD setups. The horizontal lines with different styles correspond to the AES limits for key refresh times equal to 5.14 min (0.83 bps), 1 min (4.3 bps) and 1.4 s (183 bps), respectively.

To emphasize on the role of the photon counter features to the overall performance of QKD layer in the coexistence scheme, we take a closer look at the contribution of dark counts and Raman noise photons to the total Quantum Bit Error Rate (QBER) recorded at the maximum fiber length (i.e., at the point where SKR approaches zero). To identify their contributions, we need to decouple the QBER into separate error components. In our topology, the main error components contributing to QBER performance are: the Raman noise photons ($\mathrm{QBER_{Raman}}$), the DCR ($\mathrm{QBER_{dark}}$), the Bob's Mach-Zehnder Interferometer's contrast ($\mathrm{QBER_{opt}}$) and the detector's afterpulsing effect ($\mathrm{QBER_{after}}$). Therefore, QBER is well approximated by [61] (pp. 134–135)

$$\mathrm{QBER} = \mathrm{QBER_{Raman}} + \mathrm{QBER_{dark}} + \mathrm{QBER_{opt}} + \mathrm{QBER_{after}}. \tag{6}$$

With our assumed setup parameters and considering the configuration where the quantum channel at 1550 nm is multiplexed with the classical signals at 1310 nm for both downlink and uplink (see Figure 10), when SKR approaches zero, QBER (calculated following [35,48]) reaches its maximum value, ~7.5%. Since $\mathrm{QBER_{opt}} = (1 - V)/2 = 1\%$ is constant and the afterpulsing effect contribution is practically negligible compared to the other error components at the maximum fiber length, we can conclude that

$$\mathrm{QBER_{Raman}} + \mathrm{QBER_{dark}} \cong 6.5\%. \tag{7}$$

In Figure 11, we have plotted the $\mathrm{QBER_{Raman}}$ and the $\mathrm{QBER_{dark}}$ for $N = 1$, $N = 4$, $N = 16$ and $N = 64$ terminal users, at the point where SKR approaches zero for each case.

For the case of using InGaAs photon detectors, the contribution of the DCR to the total QBER becomes stronger as the number of terminal users increases, since the optical losses associated to the cascaded splitter stages lead to lower number of total registered incoming photons at the Bob station. Therefore, in order for Equation (7) to be satisfied, Raman noise contribution should be lower (Figure 11a), which means that, as described in Section 2.2, the maximum propagation distance should be subsequently shorter. On the contrary, since the DCR of the CMOS photon counters is much lower compared to the InGaAs counterparts, its contribution to the total QBER is preserved practically constant as the number of terminal users increases and consequently, the same holds for the Raman noise (Figure 11b). This difference behavior between the two QKD detector setups is reflected in Figure 10a,b.

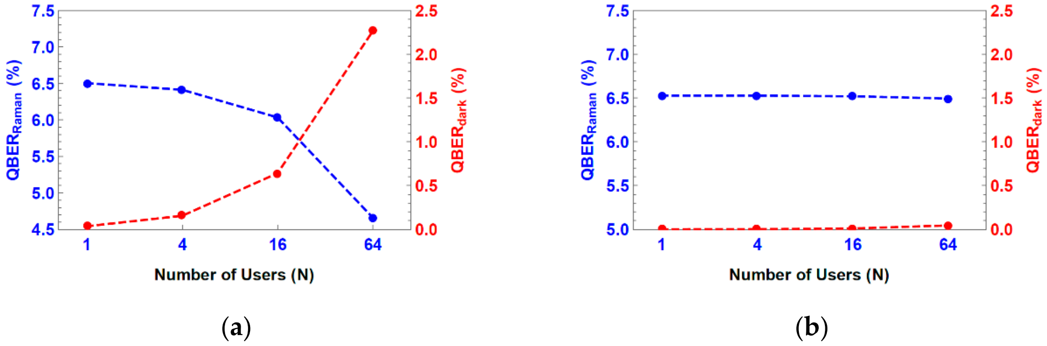


Figure 11. QBER$_{\text{Raman}}$ and QBER$_{\text{dark}}$ for 1, 4, 16 and 64 terminal users, at the maximum propagation distance (i.e., at the point where SKR approaches zero) for each case, for the configuration where the quantum channel at 1550 nm is multiplexed with the classical signals at 1310 nm for both downlink and uplink, for (**a**) InGaAs; and (**b**) upconverted CMOS-based QKD setups.

3.3. Performance Evaluation of Fiber-Wireless Topology

The performance evaluation of the converged Fiber-Wireless (Fi-Wi) topology supporting the secured P2MP distribution of symmetric keys via the use of mmWave mesh nodes is depicted in Figure 12.

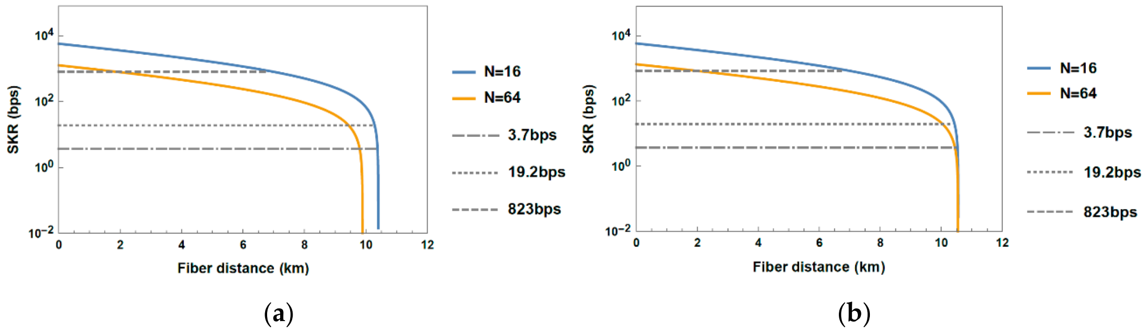


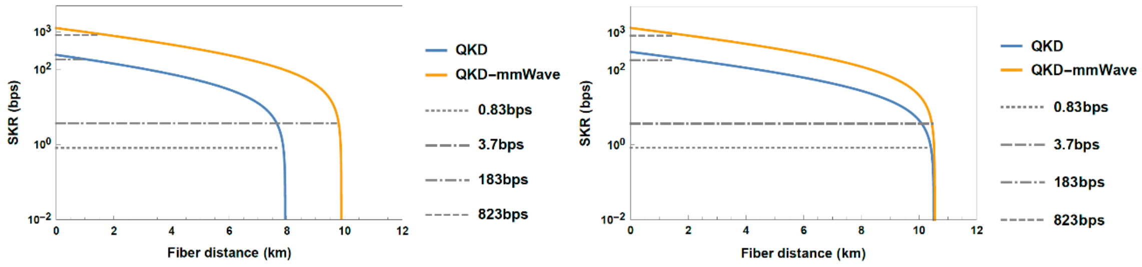
Figure 12. SKR as a function of fiber length, for the Fi-Wi topology serving N = 16 or 64 users, where the quantum channel at 1550 nm is multiplexed with the classical signals at 1310 nm for both downlink and uplink, for (**a**) InGaAs; and (**b**) upconverted CMOS-based QKD setups. The horizontal lines with different styles correspond to the AES limits for key refresh times equal to 5.14 min (3.7 bps), 1 min (19.2 bps) and 1.4 s (823 bps), respectively.

It is evident that the key rate behaves in a similar way as in the P2MP shared fiber configuration of Section 3.2, since the quantum keys are distributed to multiple mmWave nodes through identical fiber segments as in the previous case. That means that all the previous argumentation regarding the maximum transmission distance for the InGaAs- and the CMOS-based photon counters is also true for the hybrid Fi-Wi topology.

More specifically, since each mesh node communicates with four mesh clients, the SKR for the Fi-Wi topology serving 16 terminal users (blue lines of Figure 12a,b) is identical to the SKR for the P2MP shared fiber link serving four users (blue lines of Figure 10a,b). Similarly, the SKR for the Fi-Wi topology serving 64 terminal users (orange lines of Figure 12a,b) is identical to the SKR for the P2MP shared fiber link serving 16 users (orange lines of Figure 10a,b).

At first glance, this hybrid Fi-Wi topology seems preferable respecting the demands of quantum keys for a 5G fronthaul segment, since it offers a reduced number of optical Bob stations required and normally a decrease of the quantum-secured optical link distances which is translated to higher rates. Nevertheless, as described in Section 2.3, the secret keys are used to encrypt the radio controller functions besides the packetized data. According to the documentation by the radio equipment vendor providing information about the encryption in several functions of the radio, three of these functions are encrypted with AES-256 and the other with AES-128 ([59]). Following this list for the needs of our study, we allocate an additional share of the distilled keys for this layer of the controllable mesh node and to recalculate subsequently the lower SKR guaranteeing the key rotation times we have encountered. In more detail, for rotation times equal to 1.4 s, 1 min and 5.14 min, SKRs of at least $(4 \times 256 + 128)\text{bits}/1.4\ s = 823$ bps, $(4 \times 256 + 128)\text{bits}/1\text{ min} = 19.2$ bps and $(4 \times 256 + 128)\text{bits}/5.14\text{ min} = 3.7$ bps are required.

This increased SKR demands counterbalance, to some extent, the benefits of the hybrid Fi-Wi topology, as shown in Figure 13, where the performance of hybrid topology is compared with the respective of shared optical fiber P2MP link in the case of distributing keys in a secure way for N = 64 terminal users.



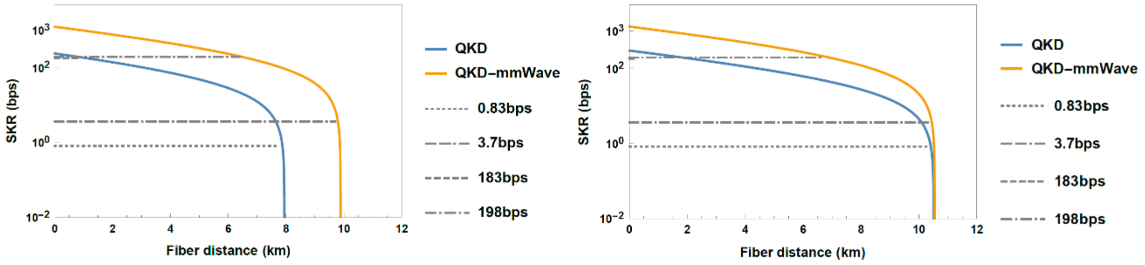
(**a**) (**b**)

Figure 13. SKR as a function of fiber length, for the P2MP shared fiber link (blue line) and for the Fi-Wi topology (orange line) serving N = 64, where the quantum channel at 1550 nm is multiplexed with the classical signals at 1310 nm for both downlink and uplink, for (**a**) InGaAs; and (**b**) upconverted CMOS-based QKD setups. The horizontal lines with different styles correspond to the AES limits for different key refresh times: 0.83 bps corresponds to 5.14 min refresh time for the data encryption for P2MP; 3.7 bps corresponds to 5.14 min refresh time for the data encryption and for the controlled functions for Fi-Wi; 183 bps corresponds to 1.4 s refresh time for the data encryption for P2MP; and 823 bps corresponds to 1.4 s refresh time for the data encryption and for the controlled functions for Fi-Wi.

According to this comparison, the Fi-Wi is slightly favored over the P2MP topology only for the InGaAs detectors and for the high key rotation time. The reason for that is twofold. Firstly, as mentioned above, apart from the SKR low limits concerning the key demands, the SKR for the Fi-Wi topology serving 64 users is identical to the SKR for the P2MP shared fiber link serving 16 users. Therefore, as explained in Section 3.2, for the InGaAs QKD setup, the maximum feasible transmission distance is longer for the Fi-Wi case (orange line of Figure 13a) compared to the P2MP configuration serving the same (i.e., 64) terminal users (blue line of Figure 13a). Secondly, the SKR values required for the data and the controller functions encryption, under a key refresh time equal to 5.14 min (3.7 bps), are not heavily increased compared to SKR needed for the data encryption only (0.83 bps). For all the other cases, we find a remarkably similar behavior between the two topologies.

However, a much better system performance can be achieved by slightly compromising on the rotation time of the secret keys required for the encryption of the radio controller functions only, while demanding the lowest key rotation time for the data encryption. More specifically, we considered a scenario where a 1.4 s refresh time is set for the data encryption and 1 min for the control layer encryption, respectively. This case demands SKR of at least $(3 \times 256 + 128)\text{bits}/1\text{ min} + 256\text{ bits}/1.4\ s = 198$ bps. The comparison between the Fi-Wi topology operated with the above settings and the shared optical fiber P2MP link serving 64 terminal users is illustrated in Figure 14.

Assuming the above combination of key rotation times, the Fi-Wi topology offers a significant improvement for both QKD implementation setups, compared to the P2MP shared fiber link case, since the SKR limits for the two configurations are almost the same (198 bps compared to 183 bps respectively). In more detail, an increase of approximately 5 km (for CMOS) to 6 km (for InGaAs) for the maximum possible fiber distance can be obtained. Finally, it should also be noted that the relative improvement is somewhat more evident for the InGaAs compared to the CMOS setup, since this QKD setup is more sensitive to the decrease in the number of optical terminal nodes which the Fi-Wi provides, respecting the maximum achievable distance, as thoroughly described previously. This behavior of the InGaAs-based QKD setup is more clearly reflected in the case of the relaxed key refresh time of 1 min for the encryption of the controlled functions, where the hybrid topology can offer 2 km extension of the maximum feasible transmission distance. On the other hand, we observe an almost identical behavior between the two topologies in the case of using CMOS detectors, for his lower key refresh time.



(**a**) (**b**)

Figure 14. SKR as a function of fiber length, for the P2MP shared fiber link (blue line) and for the Fi-Wi topology (orange line) serving N = 64, where the quantum channel at 1550 nm is multiplexed with the classical signals at 1310 nm for both downlink and uplink, for (**a**) InGaAs; and (**b**) upconverted CMOS-based QKD setups. The horizontal lines with different styles correspond to the AES limits for different key refresh times: 0.83 bps corresponds to 5.14 min refresh time for the data encryption for P2MP; 3.7 bps corresponds to 5.14 min refresh time for the data encryption and for the controlled functions for Fi-Wi; 183 bps corresponds to 1.4 s refresh time for the data encryption for P2MP; and 198 bps corresponds to 1.4 s and 1 min refresh times for the data encryption and the controlled functions, respectively, for Fi-Wi.

4. Discussion

Beyond the reported studies and outcomes, this section seeks to open the door to the future of secured 5G/B5G edge topologies, focusing on the technological options and deployment scenarios in support of the QKD integration within the 5G/B5G-oriented fronthaul infrastructure. In this direction, the roadmap of quantum communication blocks assisting in the end-to-end security of the converged optical/wireless can be built upon the following pillars:

Practical on-chip QKD blocks: Moving towards the deployment of 5G network components within street furniture such as lampposts [62], the ultra-compact size of QKD Bob stations emerges as an essential feature for this kind of metropolitan 5G/B5G terminal nodes. To satisfy the demands of the low-cost and compact on-chip circuitries for this kind of terminal node [63], upconversion assisted modules can be exploited for quantum engines, based on the use of practical CMOS SPADs for single-photon detection operated at room temperature. The advantage gained from the detection of the C-band photons with integrated CMOS SPADs instead of bulky and expensive InGaAs SPADs can be combined with advanced chip-scale photonic solutions for frequency conversion of photons, thereby allowing for miniaturized detectors. In this direction, the UNIQORN project pursues an upconversion-assisted module based on sum-frequency generation inside a waveguide inscribed ppLN crystal on the polymer platform [33].

Quantum resources as part of future WDM-PON infrastructure: The integration of QKD links within WDM-enabled architecture for securely distributing symmetric keys to 5G/B5G terminal nodes along the optical segments is also fully aligned with the strong will of the telecom operator to reuse their installed PON infrastructure as the fronthaul/midhaul connectivity layer of 5G services [64]. In this context, the QKD research community has experimentally verified that the coexistence of quantum channels with several classical channels is feasible under fully loaded modern access communication standards operating at different spectral bands [65].

QKD/PLS-assisted security for converged fiber/wireless fronthaul segments: The concept in which low-cost mmWave mesh nodes are operated as part of a network connecting access devices (e.g., WiFi hotspot, 5G RRH) has been proposed to enable flexible edge connectivity in 5G/B5G fronthaul [66]. The realization of P2MP transport nodes at above 100GHz relying on existing optical fiber infrastructure and by extending its reach has been recently demonstrated for use cases in ultra-dense environments using D-band radio equipment [67]. The end-to-end security framework of these hybrid optical/wireless mesh networks can be guaranteed through the combination of QKD-assisted AES engines in the optical fibers with the keyless secure transmission of highly directional Line-of-Sight (LOS) by mmWave/THz nodes [68].

Entering the era of Quantum Internet [69], the co-design and synergy between applications based on photonic qubits propagation over the deployed fiber infrastructure can be initiated. The presented QKD-enabled infrastructure for secured 5G/B5G topologies could potentially assist in the trusted execution of the future distributed quantum information processing tasks [70]. Exploiting the rich portfolio of Quantum PICs for generating, manipulating and measuring entangled states [71], the presented deep fiber topologies can be used as the backbone of the distributed quantum information processing at the edge. Our reported results addressing the performance of a QKD layer across deployed dark fiber segments could also be used to assist in the characterisation of the trusted/untrusted nodes along with the novel methods demonstrated in the field of Quantum Networks [72].

5. Conclusions

In this research, a QKD-aided fronthaul segment supporting low-latency 5G connectivity has been discussed. The integration of a BB84-QKD link supporting the AES-256 encryption of packetized fronthaul operating at 10Gbps has been thoroughly investigated for both P2P and P2MP topologies. In the dark fiber case, the secret keys can be distilled even at long fiber distances of P2P and P2MP links, serving up to 64 users. The shared fiber deployment option to optimize the use of fiber resources in edge optical topologies can be achieved by using the less noisy upconverted CMOS photon counters, allowing for sufficient key distillation for up to 64 Bob stations at 5G terminal nodes interconnected through fiber segments up to 10 km. We also proposed a hybrid Fi-Wi topology supporting the secured P2MP distribution using mmWave nodes to interconnect several 5G terminal nodes through wireless channels. Compared to the P2MP shared fiber link case and by letting the symmetric keys which encrypt the necessary functions for the control and management of the radio nodes to be refreshed by a slightly lower rate, the Fi-Wi topology has been verified that could offer a 5–6 km extension of the maximum feasible transmission distance.

Author Contributions: Conceptualization, D.Z., A.N., and G.G.; Data curation, D.Z. and A.N.; Investigation, D.Z., A.N., and G.G.; Methodology, D.Z., A.N., and G.G.; Supervision, G.G. and H.A.; Writing—original draft, D.Z. and G.G.; Writing—review and editing, D.Z. and G.G. All authors have read and agreed to the published version of the manuscript.

Funding: This work was funded by H2020-funded Flagship project UNIQORN (820474).

Acknowledgments: Part of the research leading to this work was also supported by the H2020-funded 5G-PPP Phase 3 project 5G-COMPLETE (871900).

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Maximum Fiber Fronthaul Distance Corresponding to Round-Trip Latency Barrier

In Section 2.1, we briefly mentioned the 5G fronthaul latency requirements imposed for low-latency services. This Appendix provides the calculation of the maximum fiber fronthaul distance which satisfies this latency constraint.

Table A1 includes the latency components considered for our study, by adopting the available parameters within [28].

Table A1. Latency components considered for our study, based on the available parameters within [28].

Latency Components	
Round-Trip Delay Components	**Typical Time**
Propagation fiber delay	10 µs/km
Radio Frequency (RF) overhead	40 µs
eCPRI overhead	10 µs
BBU	2700 µs
Fronthaul equipment processing delay	4 µs
One-way encryption/decryption	34 µs
QKD post-processing	11 µs

The additional QKD post-processing delay component was calculated by assuming the use of the high-speed postprocessing modules reported by Toshiba recently [73], to realize the operations of sifting, error correction and privacy amplification for the key distillation process of an AES-256 key. Following the methodology reported in [28], for a round-trip processing of less than 3 ms, the fiber fronthaul distance is limited to be less than

$$D = \frac{3\text{ ms} - 40\ \mu\text{s} - 10\ \mu\text{s} - 2700\ \mu\text{s} - 4\ \mu\text{s} - 2 \times 34\ \mu\text{s} - 11\ \mu\text{s}}{10\ \mu\text{s}/\text{km}} \cong 17\text{ km}. \tag{A1}$$

References

1. Sim, D.-H. Quantum Safe Communication—Preparing for the Next Era. In Proceedings of the Presentation in ITU Workshop on Quantum Information Technology, Shanghai, China, 5–7 June 2019.
2. Tomkos, I.; Klonidis, D.; Pikasis, E.; Theodoridis, S. Toward the 6G network era: Opportunities and challenges. *IT Prof.* **2020**, *22*, 34–38. [CrossRef]
3. Bernstein, D.J. Introduction to post-quantum cryptography. In *Post-Quantum Cryptography*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 1–14.
4. Diamanti, E.; Lo, H.K.; Qi, B.; Yuan, Z. Practical challenges in quantum key distribution. *NPJ Quantum Inf.* **2016**, *2*, 1–12. [CrossRef]
5. Xu, F.; Ma, X.; Zhang, Q.; Lo, H.K.; Pan, J.W. Secure quantum key distribution with realistic devices. *Rev. Modern Phys.* **2020**, *92*, 025002. [CrossRef]
6. Liao, S.-K.; Cai, W.-Q.; Handsteiner, J.; Liu, B.; Yin, J.; Zhang, L.; Rauch, D.; Fink, M.; Ren, J.-G.; Liu, W.; et al. Satellite-relayed intercontinental quantum network. *Phys. Rev. Lett.* **2018**, *120*, 030501. [CrossRef] [PubMed]
7. Community Response to the NCSC 2020 Quantum Security Technologies White Paper. Available online: https://www.quantumcommshub.net/wp-content/src/Response-to-NCSC-QSC-WP-Issue-1.1-27_5_2020.pdf (accessed on 24 June 2020).
8. Dowling, B.; Hansen, T.B.; Paterson, K.G. Many a Mickle Makes a Muckle: A Framework for Provably Quantum-Secure Hybrid Key Exchange. In Proceedings of the International Conference on Post-Quantum Cryptography, Paris, France, 15–17 April 2020; pp. 483–502.
9. Post-Quantum Cryptography. Workshops and Timeline. Available online: https://csrc.nist.gov/Projects/post-quantum-cryptography/workshops-and-timeline (accessed on 24 June 2020).
10. ADVA achieves world-first 100G Quantum-Safe Transport Over 2800 km. Available online: https://www.adva.com/en/newsroom/press-releases/20180613-adva-achieves-world-first-100g-quantum-safe-transport-over-2800km (accessed on 24 June 2020).
11. Bonnetain, X.; Naya-Plasencia, M.; Schrottenloher, A. Quantum Security Analysis of AES. *IACR Trans. Symmetric Cryptol.* **2019**, *2*, 55–93. [CrossRef]
12. Lo, H.K.; Chau, H.F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **1999**, *283*, 2050–2056. [CrossRef]

13. Shor, P.W.; Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **2000**, *85*, 441. [CrossRef]
14. Mayers, D. Unconditional security in quantum cryptography. *J. ACM* **2001**, *48*, 351–406. [CrossRef]
15. Lo, H.K.; Curty, M.; Tamaki, K. Secure quantum key distribution. *Nat. Photonics* **2014**, *8*, 595–604. [CrossRef]
16. Wright, P.; White, C.; Parker, R.C.; Pegon, J.-S.; Menchetti, M.; Pearse, J.; Bahrami, A.; Moroz, A.; Wonfor, A.; Penty, R.V.; et al. 5G Network Slicing with QKD and Quantum-Safe Security. *arXiv Preprint* **2020**, arXiv:2007.03377.
17. OIDA. OIDA Quantum Photonics Roadmap: Every Photon Counts. OIDA Report, 3; OSA Industry Development Associates (OIDA). 2020. Available online: https://www.osapublishing.org/abstract.cfm?uri=OIDA-2020-3 (accessed on 10 June 2020).
18. Chen, J.-P.; Zhang, C.; Liu, Y.; Jiang, C.; Zhang, W.; Hu, X.-L.; Guan, J.-Y.; Yu, Z.-W.; Xu, H.; Lin, J.; et al. Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km. *Phys. Rev. Lett.* **2020**, *124*, 070501. [CrossRef]
19. UNIQORN Objectives. Available online: https://quantum-uniqorn.eu/home/technology-lines/saftey-security-design-methods/ (accessed on 23 June 2020).
20. Eriksson, T.A.; Hirano, T.; Puttnam, B.J.; Rademacher, G.; Luís, R.S.; Fujiwara, M.; Namiki, R.; Awaji, Y.; Takeoka, M.; Wada, N.; et al. Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 Tbit/s data channels. *Commun. Phys.* **2019**, *2*, 1–8. [CrossRef]
21. Lai, J.S.; Lin, X.Y.; Qian, Y.; Liu, L.; Zhao, W.Y.; Zhang, H.Y. Deployment-oriented integration of DV-QKD and 100 G optical transmission system. In Proceedings of the Asia Communications and Photonics Conference, Optical Society of America. Chengdu, China, 2–5 November 2019; p. T2H-1.
22. Aleksic, S.; Winkler, D.; Franzl, G.; Poppe, A.; Schrenk, B.; Hipp, F. Quantum key distribution over optical access networks. In Proceedings of the 2013 18th European Conference on Network and Optical Communications & 2013 8th Conference on Optical Cabling and Infrastructure (NOC-OC&I), Graz, Austria, 10–12 July 2013; pp. 11–18.
23. Qi, B.; Zhu, W.; Qian, L.; Lo, H.K. Feasibility of quantum key distribution through a dense wavelength division multiplexing network. *New J. Phys.* **2010**, *12*, 103042. [CrossRef]
24. Choi, I.; Zhou, Y.R.; Dynes, J.F.; Yuan, Z.; Klar, A.; Sharpe, A.; Plews, A.; Lucamarini, M.; Radig, C.; Neubert, J.; et al. Field trial of a quantum secured 10 Gb/s DWDM transmission system over a single installed fiber. *Opt. Express* **2014**, *22*, 23121–23128. [CrossRef]
25. Wang, R.; Wang, Q.; Kanellos, G.T.; Nejabati, R.; Simeonidou, D.; Tessinari, R.S.; Hugues-Salas, E.; Bravalheri, A.; Uniyal, N.; Muqaddas, A.S.; et al. End-to-End Quantum Secured Inter-Domain 5G Service Orchestration Over Dynamically Switched Flex-Grid Optical Networks Enabled by a q-ROADM. *J. Light. Technol.* **2020**, *38*, 139–149. [CrossRef]
26. Kong, W.; Sun, Y.; Cai, C.; Ji, Y. Impact of Modulation Formats and Bandwidth on Quantum Secured 5G Optical Fronthaul over Multicore Fiber. In Proceedings of the CLEO 2020, Washington, DC, USA, 10–15 May 2020.
27. Hugues-Salas, E.; Alia, O.; Wang, R.; Rajkumar, K.; Kanellos, G.T.; Nejabati, R.; Simeonidou, D. 11.2 Tb/s Classical Channel Coexistence with DV-QKD over a 7-Core Multicore Fiber. *J. Light. Technol.* **2020**, 1. [CrossRef]
28. Cho, J.Y.; Sergeev, A.; Zou, J. Securing Ethernet-based Optical Fronthaul for 5G Network. In Proceedings of the 14th International Conference on Availability, Reliability and Security, Canterbury, UK, 26–29 August 2019; pp. 1–6.
29. Common Public Radio Interface: ECPRI Interface Specification v1.2. Available online: http://www.cpri.info/spec.html (accessed on 26 June 2020).
30. Pérez, G.O.; López, D.L.; Hernández, J.A. 5G new radio fronthaul network design for eCPRI-IEEE 802.1 CM and extreme latency percentiles. *IEEE Access* **2019**, *7*, 82218–82230. [CrossRef]
31. IEEE Standard for Local and Metropolitan Area Networks-IEEE Time Sensitive Networking for Fronthaul, IEEE Standard 802.1cm. 2018. Available online: http://www.ieee802.org/1/pages/802.1cm.html (accessed on 26 June 2020).
32. Kong, L.; Li, Z.; Li, C.; Cao, L.; Xing, Z.; Cao, J.; Wang, Y.; Cai, X.; Zhou, X. Photonic integrated quantum key distribution receiver for multiple users. *Opt. Express* **2020**, *28*, 18449–18455. [CrossRef]

33. Hübel, H. All you Need to Know about UNIQORN. Available online: https://quantum-uniqorn.eu/wp-content/uploads/2019/02/UNIQORN-summary-EQTC-Grenoble.pdf (accessed on 27 June 2020).
34. Townsend, P.D. Quantum cryptography on multiuser optical fibre networks. *Nature* **1997**, *385*, 47–49. [CrossRef]
35. Eraerds, P.; Walenta, N.; Legré, M.; Gisin, N.; Zbinden, H. Quantum key distribution and 1 Gbps data encryption over a single fibre. *New J. Phys.* **2010**, *12*, 063027. [CrossRef]
36. Jain, N. Security of Practical Quantum Key Distribution Systems. PhD Thesis, Friedrich-Alexander-Universität Erlangen-Nürnberg, Bavaria, Germany, 2015.
37. idQuantique. Available online: www.idQuantique.com (accessed on 18 June 2020).
38. Mlejnek, M.; Kaliteevskiy, N.A.; Nolan, D.A. Reducing spontaneous Raman scattering noise in high quantum bit rate QKD systems over optical fiber. *arXiv Preprint* **2017**, arXiv:1712.05891.
39. Aurea Technology Single Photon Counting Module: SPD_A_NIR Datasheet. Available online: http://www.aureatechnology.com/images/produits/AUREA_Datasheet_SPD_A_NIR_V1.1_2018_light.pdf (accessed on 26 June 2020).
40. Ma, F.; Liang, L.-Y.; Chen, J.-P.; Gao, Y.; Zheng, M.-Y.; Xie, X.-P.; Liu, H.; Zhang, Q.; Pan, J.-W. Upconversion single-photon detectors based on integrated periodically poled lithium niobate waveguides [Invited]. *J. Opt. Soc. Am. B* **2018**, *35*, 2096–2101. [CrossRef]
41. Niederberger, A.; Scarani, V.; Gisin, N. Photon-number-splitting versus cloning attacks in practical implementations of the Bennett-Brassard 1984 protocol for quantum cryptography. *Phys. Rev. A* **2005**, *71*, 042316. [CrossRef]
42. Shields, A. Performance Limits for Quantum Key Distribution Networks. In Proceedings of the Presentation in ITU Workshop on Quantum Information Technology, Shanghai, China, 5–7 June 2019.
43. Dynes, J.F.; Wonfor, A.; Tam, W.W.-S.; Sharpe, A.W.; Takahashi, R.; Lucamarini, M.; Plews, A.; Yuan, Z.; Dixon, A.R.; Cho, J.; et al. Cambridge quantum network. *npj Quantum Inf.* **2019**, *5*, 1–8. [CrossRef]
44. Luykx, A.; Paterson, K.G. Limits on Authenticated Encryption Use in TLS. 2015. Available online: https://www.isg.rhul.ac.uk/~{}kp/TLS-AEbounds.pdf (accessed on 26 June 2020).
45. Kumar, R.; Qin, H.; Alléaume, R. Coexistence of continuous variable QKD with intense DWDM classical channels. *New J. Phys.* **2015**, *17*, 043027. [CrossRef]
46. Patel, K.A.; Dynes, J.F.; Choi, I.; Sharpe, A.W.; Dixon, A.R.; Yuan, Z.L.; Penty, R.V.; Shields, A.J. Coexistence of High-Bit-Rate Quantum Key Distribution and Data on Optical Fiber. *Phys. Rev. X* **2012**, *2*, 041010. [CrossRef]
47. Fröhlich, B.; Dynes, J.F.; Lucamarini, M.; Sharpe, A.W.; Tam, S.W.B.; Yuan, Z.; Shields, A.J. Quantum secured gigabit optical access networks. *Sci. Rep.* **2015**, *5*, 1–7. [CrossRef]
48. Zavitsanos, D.; Giannoulis, G.; Raptakis, A.; Papapanos, C.; Setaki, F.; Theodoropoulou, E.; Lyberopoulos, G.; Kouloumentas, C.; Avramopoulos, H. Coexistence of Discrete-Variable QKD with WDM classical signals in the C-band for fiber access environments. In Proceedings of the 2019 21st International Conference on Transparent Optical Networks (ICTON), Université d'Angers, France, 9–13 July 2019; pp. 1–5.
49. Peters, N.A.; Toliver, P.; Chapuran, T.E.; Runser, R.J.; McNown, S.R.; Peterson, C.G.; Rosenberg, D.; Dallmann, N.; Hughes, R.J.; McCabe, K.P.; et al. Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments. *New J. Phys.* **2009**, *11*, 045012. [CrossRef]
50. Runser, R.J.; Chapuran, T.; Toliver, P.; Peters, N.A.; Goodman, M.S.; Kosloski, J.T.; Nweke, N.; McNown, S.R.; Hughes, R.J.; Rosenberg, D.; et al. Progress toward quantum communications networks: Opportunities and challenges. In *Optoelectronic Integrated Circuits IX*; International Society for Optics and Photonics: San Jose, CA, USA, 2007; Volume 6476, p. 64760I.
51. Yan, C.; Yong, S.; Guang-Zhao, T.; Hong-Xin, Z. Impact of cross-phase modulation induced by classical channels on the CV-QKD in a hybrid system. *Chin. Phys. Lett.* **2013**, *30*, 110302.
52. Kingfisher International. Optical Loss & Testing Overview. Available online: https://kingfisherfiber.com/application-notes/optical-loss-testing-overview/ (accessed on 22 June 2020).
53. Schrenk, B.; Hentschel, M.; Hübel, H. O-band differential phase-shift quantum key distribution in 52-channel C/L-band loaded passive optical network. In Proceedings of the 2019 Optical Fiber Communications Conference and Exhibition (OFC), San Diego Convention Center, CA, USA, 3–7 March 2019; pp. 1–3.
54. Oughton, E.J.; Frias, Z. The cost, coverage and rollout implications of 5G infrastructure in Britain. *Telecommun. Policy* **2018**, *42*, 636–652. [CrossRef]

55. Du, J.; Chizhik, D.; Feick, R.; Rodriguez, M.; Castro, G.; Valenzuela, R.A. Suburban fixed wireless access channel measurements and models at 28 GHz for 90% outdoor coverage. *IEEE Trans. Antennas Propag.* **2019**, *68*, 411–420. [CrossRef]
56. Kanta, K.; Pagano, A.; Ruggeri, E.; Agus, M.; Stratakos, I.; Mercinelli, R.; Vagionas, C.; Toumasis, P.; Kalfas, G.; Giannoulis, G.; et al. Analog fiber-wireless downlink transmission of IFoF/mmWave over in-field deployed legacy PON infrastructure for 5G fronthauling. *IEEE/OSA J. Optical Commun. Netw.* **2020**, *12*, D57–D65. [CrossRef]
57. Zhang, L.; Zhao, H.; Hou, S.; Zhao, Z.; Xu, H.; Wu, X.; Wu, Q.; Zhang, R. A Survey on 5G Millimeter Wave Communications for UAV-Assisted Wireless Networks. *IEEE Access* **2019**, *7*, 117460–117504. [CrossRef]
58. Butnaru, S. Siklu Announces the Multi-Gigabit MultiHaul™ Mesh Node N360. Available online: https://www.siklu.com/press-release/siklu-announces-the-multi-gigabit-multihaul-mesh-node-n360/ (accessed on 28 June 2020).
59. Siklu. Encryption & Etherhaul 7xx, Edition B1. Available online: https://www.siklu.com/wp-content/uploads/2018/12/2018-12-EH-7xx-and-Encryption-Ed.-B1.pdf (accessed on 24 June 2020).
60. Siklu. mmWave Wireless Fiber Frequently Asked Questions. Available online: https://www.siklu.com/mmwave-wireless-fiber-faq/ (accessed on 24 June 2020).
61. Benslama, M.; Benslama, A.; Aris, S. *Quantum Communications in New Telecommunications Systems*; John Wiley & Sons: Hoboken, NJ, USA, 2017.
62. Revealed: 5G Rollout is Being Stalled by Rows over Lampposts. Available online: https://www.theguardian.com/technology/2019/may/19/revealed-5g-rollout-is-being-stalled-by-rows-over-lampposts (accessed on 27 June 2020).
63. Giannoulis, G.; Tokas, K.; Poulopoulos, G.; Kanakis, G.; Toumasis, P.; Kanta, K.; Apostolopoulos, D.; Avramopoulos, H. Integrated Photonic Filters in Support of Converged 5G Mobile Fronthaul & Midhaul Transport Layers. *Fiber Integr. Opt.* **2019**, *38*, 333–348.
64. Bidkar, S.; Galaro, J.; Pfeiffer, T. First demonstration of an ultra-low-latency fronthaul transport over a commercial TDM-PON platform. In Proceedings of the 2018 Optical Fiber Communications Conference and Exposition (OFC), San Diego Convention Center, CA, USA, 11–15 March 2018; pp. 1–3.
65. Vokić, N.; Milovančev, D.; Schrenk, B.; Hentschel, M.; Hübel, H. Differential Phase-Shift QKD in a 2: 16-Split Lit PON with 19 Carrier-Grade Channels. *IEEE J. Sel. Top. Quantum Electron.* **2020**, *26*, 1–9. [CrossRef]
66. 5G-COMPLETE. Available online: https://5gcomplete.eu/ (accessed on 27 June 2020).
67. Paoloni, C.; Krozer, V.; Magne, F.; Le, Q.T.; Basu, R.; Rao, J.; Yacob, H. D-band Point to Multi-Point Deployment with G-Band Transport. In Proceedings of the EuCNC 2020, Dubrovnik, Croatia, 16–17 June 2020.
68. Federici, J.; Moeller, L. Review of terahertz and subterahertz wireless communications. *J. Appl. Phys.* **2010**, *107*, 6. [CrossRef]
69. Wehner, S.; Elkouss, D.; Hanson, R. Quantum internet: A vision for the road ahead. *Science* **2018**, *362*, eaam9288. [CrossRef]
70. Pirker, A.; Wallnöfer, J.; Dür, W. Modular architectures for quantum networks. *New J. Phys.* **2018**, *20*, 053054. [CrossRef]
71. Elshaari, A.W.; Pernice, W.H.P.; Srinivasan, K.; Benson, O.; Zwiller, V. Hybrid integrated quantum photonic circuits. *Nat. Photon* **2020**, *14*, 285–298. [CrossRef]
72. Lu, H.; Huang, C.-Y.; Li, Z.-D.; Yin, X.-F.; Zhang, R.; Liao, T.-L.; Chen, Y.-A.; Li, C.-M.; Pan, J.-W. Counting Classical Nodes in Quantum Networks. *Phys. Rev. Lett.* **2020**, *124*, 180503. [CrossRef]
73. Yuan, Z.; Murakami, A.; Kujiraoka, M.; Lucamarini, M.; Tanizawa, Y.; Sato, H.; Shields, A.J.; Plews, A.; Takahashi, R.; Doi, K.; et al. 10-Mb/s quantum key distribution. *J. Light. Technol.* **2018**, *36*, 3427–3433. [CrossRef]

© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).