DELIVERABLE 2.3

Alternative path(s) for each realization of applications in D2.1

COST Action:	**CA15220**
Project acronym:	**QTSpace**
Project title:	**Quantum Technologies in Space**
Funding scheme:	**COST Association**
Start date of project:	**20 October 2016**
End date of project:	**19 April 2021**
Due date of the Deliverable:	**December 2019**
Deliverable issued:	**December 2019**
Dissemination Level:	**Public**
Version:	**1.0**

TABLE OF CONTENT

INTRODUCTION

In the deliverables D2.1 and D2.2, we described promising applications of quantum technology in space and their respective technical requirements. In particular, we focused on Quantum Key Distribution and Quantum Sensing. Here, we will describe alternative routes towards implementing these applications.

IMPLEMENTATION

We describe requirements that need to be met in order to implement the two applications chosen.

Quantum Key Distribution

The most straightforward satellite QKD link configuration is for the satellite to act as a trusted node. The satellite assumes the role of one of the trusted parties (Alice or Bob) in a prepare-and-measure QKD protocol and establishes independent secure keys with individual ground stations. The satellite stores all the keys and upon request for connection between two ground stations it broadcasts a bitwise parity of keys established with respective stations. Given that both keys are independent secret strings, and their bit-parity is a uniformly random binary sequence, the announcement of the latter does not reveal any actual information to any unauthorized third party. On the other hand, the key stored at the ground station and the broadcasted sequence is sufficient to infer the key stored at another station [1].

Depending on the role assumed by the satellite, the connection can be established as an uplink or a downlink [2]. In the former, the ground station prepares and sends quantum signals to the receiver passing by in orbit (also referred to as ground-to-space link), while in the latter the quantum signals are prepared and sent from the satellite to the ground station (space-to-ground link). Naturally, the trusted party occupying the ground station will be flexible and can upgrade or replace components, while the hardware configuration at the satellite must be space-qualified and will not be adapted or changed after launch.

The flexibility is especially important for continuous security maintenance of the prepare-and-measure protocol setup and prevention of potential side channel attacks. More specifically, theoretical models used for security analysis may not necessarily faithfully describe actual equipment used in a practical QKD setup, thus opening side channels and loopholes in security, that can be exploited by a malicious third party. Moreover, active attacks aim to intervene and temper with the operation of QKD setup creating new vulnerabilities and side channels. Closing loopholes and protection of the operation requires suitable countermeasures. In the best case scenario, this implies improving the models, adapting the security proofs and/or post-processing, all of which would require modification of the software component of the implementation. Some of the issues can only (or more efficiently) be fixed by modifying or introducing additional physical components to the setup. Examples of two distinct solutions to the same security threat, posed by the photon-number-splitting attack on multiphoton signal pulses in BB84, are: introduction of decoy states that can directly detect such an attack [3], or SARG04 modification of data processing at the cost reduced performance of the protocol [4]. Furthermore, active attacks such as Trojan-horse [5], faked-state [6], detector efficiency mismatch [7], wavelength-dependency [8], and many more can be prevented hardware-wise, by adjusting the design of the protocol setup, including additional isolators, filters and detectors, monitoring the nominal performance.

The hardware on the QKD satellite node cannot be updated after deployment, which leaves the protocol vulnerable to potential novel attacks. Even the viability for future software

updates can potentially leave a backdoor to the system open and compromise the protocol. On the other hand, conducting an active attack requiring precise targeting of a distant and moving satellite-based trusted station presents a significant challenge for an adversary with today's technology [9,10]. In addition, trusted stations can verify the absence of complex devices within the direct line of sight between them [11].

The main difference between uplink and downlink is the amount of atmospheric attenuation. In the uplink scenario, the atmospheric effects (occurring in the troposphere and lower parts of the stratosphere) such as absorption, scattering, and scintillation contribute to beam spot spreading, deformation and wandering which at higher altitudes are enforced due to further diffraction-induced spreading [12]. In the downlink scenario, the beam first travels through the vacuum enduring only diffraction-induced spreading, and the atmospheric influence occurs only at the very end of the path, resulting in lower overall signal loss. One can expect 10-20 dB of additional loss in the uplink, compared to a downlink under the same conditions [13,14].

The downlink can also be simulated using a powerful light source at the ground station and retroreflectors on a satellite. The mean photon number of the light pulses emitted from the ground station is scaled [15] according to uplink channel transmissivity so that the mean photon number of the pulse reflected (and modulated) from the satellite would be 1 or less, i.e., in accordance with the requirements to the source of the decoy-state BB84 protocol [3].

If the trusted parties employ entanglement-based QKD protocol [16,17], then the requirement to trust the satellite can be alleviated. In such a configuration, the trusted parties reside at ground stations, while the satellite carries a source of entangled states and establishes a double downlink to two separate stations (Alice and Bob). Upon successful collection and measurement of both entangled subsystems, the measurement results of Alice and Bob will be correlated. In the BBM92 (DV) QKD protocol [17], the sequence of such symmetrical measurements will form a sifted key, that, similarly to the one in the (prepare-and-measure) BB84 protocol [18], can be distilled and corrected for errors, thus resulting in a secure key. The security of the key is based on the inevitable appearance of errors in the raw key if an unauthorized party will try to become entangled to the signal entangled system.

On the other hand, the security of E91 protocol [16] stems from the violation of Bell inequalities. While this forces trusted parties to measure in more polarization bases, after a successful violation of the inequality, Alice and Bob can be confident there was no eavesdropping. This is also the security foundation for device-independent (DI) QKD protocols. Such protocols make no assumptions regarding used equipment (thus eliminating all possible side channels), and only test classical inputs (measurement bases) and outputs (measurement results) of the protocol to verify randomness and integrity of shared binary strings. The implementation of DI QKD protocols is challenging and imposes strict requirements on detection efficiencies to close the detection loophole [19].

Alternatively, measurement-device-independent (MDI) QKD protocols lift trust assumptions regarding the detection devices only [20,21]. This is achieved by delegating the Bell measurement to a third party, with the trusted parties preparing and sending the states, but not receiving any. This corresponds to a double uplink with satellite carrying Bell-measurement station and acting as an untrusted node. The announcement of Bell measurement results and consequent post-selection allows to create strong correlations

between data sets of remote trusted parties. Combining the protocol with the decoy-state method circumvents the multi-photon emission issue of weak coherent sources [22,23]. The main challenges of the implementation are losses and the required synchronization of the signals in both uplinks.

Another practical concern for satellite-based QKD is link availability. Aside from weather dependence [14], a foremost factor is the orbital altitude of the satellite: Low Earth Orbit (LEO), Medium Earth Orbit (MEO), and Geostationary Orbit (GEO). LEO is the most common orbit up-to-date due to its proximity to the surface which implies lower diffraction induced losses, lower exposure to ionizing radiation from the Sun, as well as lower launch costs than for orbits of higher altitudes. The downsides of LEO are the high speed of the satellite relative to the ground station and the limited line-of-sight window during a flyover. The former presents a challenging requirement for an accurate and fast pointing system, while the latter prevents continuous communication and allows to distribute keys only once every one or two hours for a few minutes when the satellite is above 10 degrees of elevation above the horizon [24,25]. Reaching MEO would support a significantly longer communication window [33], while the satellite at GEO would be permanently accessible. However, increasing the altitude also increases the channel loss and the exposure to ionizing radiation. Crucially, it also decreases the eclipse fraction of the total orbital period [26], which curtails the link access time with minimal background radiation, which can be five orders of magnitude lower than during day-time operation [27,28]. The presence of scattered sunlight has confined current QKD tests to night-time operation only, and a day-and-night link availability requires advanced acquisition, tracking and pointing systems, filtering, and precise temporal synchronization [29].

CV QKD protocols can be potentially operated during the day due to its reliance on the coherent detection of the signal where the signal is matched with a narrow-band local oscillator that serves as a phase reference. This approach can efficiently filter out background radiation [30]. However, CV QKD protocols (as well as some DV encodings such as orbital angular momentum [31]) are sensitive to turbulent fluctuations of refractive index within the air mass [32]. Such fluctuations induce untrusted excess noise, proportional to the size of the encoding alphabet and variance of channel transmittance fluctuations [33], and bounds the range of atmospheric conditions and zenith angles that support secure key distribution. Sub-channel post-selection and data clusterization has been suggested to suppress fading noise influence [33,34]. Furthermore, squeezed states can provide substantial improvement to the performance of the protocol, although require optimization in accordance with the shape of the transmittance distribution profile [35]. Latter requires accurate channel estimation [34] which also allows for noise suppression via adaptive optics [36] or beam-spot size optimization [37]. Overall feasibility studies admit considerable challenges in satellite-based CV QKD [19,38–41], yet do not present fundamental limits for the realization.

Modelling of satellite link transmissivity provides an opportunity for preemptive optimization of protocol parameters, but must account for altitude-dependent atmospheric conditions, geographical position of the observer, variations of the slant range and refraction within the communication window, etc. [12]. Lastly, other relevant effects for all long-range space-based QKD protocols include space-time curvature [42] and gravity [43].

Communication time determines the raw data block size, that can be accumulated, and consequently the length of the key. Furthermore, the size of the block influences the confidence intervals on estimated security parameters with given composite probability of protocol failure that encapsulates probabilities of successful error correction, parameter estimation, privacy amplification, etc. In other words, the longer time the communication link was established for, the more confident trusted parties can be that actual values of security parameters do not significantly deviate from their most probable values, and therefore that the lower bound on the key rate is correctly assessed [44]. Various approaches has been developed to ensure correct evaluation of the smooth min-entropy bounds obtained from the finite raw key, such as exponential de Finetti theorem [45,46], post-selection technique [47], virtual entanglement distillation [48], entropic uncertainty relations [49,50], or entropy accumulation [51]. Finite-size effects can be reduced by merging measurement results from different satellite passes to enhance block size thus creating keys more reliably at expense of additional time needed for data accumulation [52].

Natural progression for space QKD, that eliminates the issue of link unavailability, is development of global quantum networks. Such networks would consist of satellite constellations that could share a secure key between any two ground terminals. Space QKD networks can be deployed for global, targeted or local coverage, differ in amount of employed satellites, their orbit types and altitudes, constellation geometry, etc. [53]. Within an embassy LEO constellation model, aimed at delivering a message from one ground station to a number of other stations, enabling intra-planar space-to-space links have been shown to drastically increase the key size for all ground stations [54]. Connecting MEO or GEO relay satellites to a LEO network can improve connection stability, handover management and network control, as well as, decrease latency [53,55]. Investigations into networking design, optimization of orbits, inter-satellite links and QKD protocols are pending and will pave way towards global quantum-secured communication [56].

Quantum Sensing

Without focussing on space-based systems, quantum sensors could be deployed in earthbound systems. Especially if larger missions appear infeasible, more complex setups could be loaded into transport vehicles, such as cars or ships, or deployed stationary as in atomic fountains.

Atom interferometric experiments exist both in fountains and in transportable form. For both of these options, additional investigations on increasing the sensitivity and the particle flux appear the necessary next step. This path allows the development of systems with increased sensitivity, which are important in their own rights and could be deployed for specific uses, where the complexity, volume, and mass are less of a concern. This development, additionally, supports miniaturization efforts, which could then deliver similar performance due to the technology developed in stationary or transportable devices.

Optomechanical devices using optically trapped particles may also benefit from fountain-like set-ups, where individual trapped particles are launched upwards in order to increase the effective free-fall time. Currently, systems are developed increasing interrogation times in ground-based experiments, which also serve as precursors to microgravity missions, such as MAQRO [57,58]. In this context, it may be possible to follow the path of atom interferometric

experiments and to develop transportable sensor heads and focus on the adaptation to novel environments as opposed to miniaturizing the system from the start. Similar to atom optics, this leads to further technologies and techniques being developed to increase interrogated particles per time frame or prolong the interrogation time for individual particles. Clamped optomechanical systems, on the other hand, may play an important complementary role. While they may not be as sensitive in some respects, they can be readily miniaturized [59,60], and the higher resonance frequencies of these systems and their potential to achieve high optomechanical coupling could allow for faster interrogation times and to cover a complementary parameter regime in sensing. The large variety of architectures for optomechanical sensory may allow covering a large parameter range [61], and the potential for optimizing the design of optomechanical systems for particular applications. Optomechanical systems also promise the possibility of increased sensitivity via distributed sensing [62].

CONCLUSIONS

We discussed several distinct protocols to realize Quantum Key Distribution (QKD), ranging from trusted-node QKD based on the prepare-and-measure distribution of secret keys to entanglement-based device-independent QKD, where it is not required to trust intermediary nodes. In addition, we presented discrete-variable and continuous-variable QKD protocols. In a future quantum network, different techniques may be used in order to best harness the advantages of the individual protocols.

REFERENCES

[1] M. Polnik *et al.*, EPJ Quantum Technol. **7**, 3 (2020).
[2] C. Bonato *et al.*, New J. Phys. **11**, 045017 (2009).
[3] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[4] V. Scarani *et al.*, Phys. Rev. Lett. **92**, 057901 (2004).
[5] N. Jain *et al.*, New J. Phys. **16**, 123030 (2014).
[6] V. Makarov and D. R. Hjelme, J. Mod. Opt. **52**, 691 (2005).
[7] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006).
[8] H.-W. Li *et al.*, Phys. Rev. A **84**, 062308 (2011).
[9] S.-H. Sun *et al.*, Phys. Rev. A **92**, 022304 (2015).
[10] V. Makarov *et al.*, Phys. Rev. A **94**, 030302 (2016).
[11] T. Vergoossen *et al.*, Entropy **21**, 387 (2019).
[12] D. Vasylyev, W. Vogel, and F. Moll, Phys. Rev. A **99**, 053830 (2019).
[13] M. Aspelmeyer *et al.*, IEEE J. Sel. Top. Quantum Electron. **9**, 1541 (2003).
[14] C. Liorni, H. Kampermann, and D. Bruß, New J. Phys. **21**, 093055 (2019).
[15] G. Vallone *et al.*, Phys. Rev. Lett. **115**, 040502 (2015).
[16] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[17] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[18] C. H. Bennett and G. Brassard, in *Proc. IEEE Int. Conf. Comput. Syst. Signal Process.* (Bangalore, India, 1984), pp. 175–179.
[19] S. Pirandola *et al.*, Adv. Opt. Photonics **12**, 1012 (2020).
[20] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[21] S. Pirandola *et al.*, Nat. Photonics **9**, 397 (2015).
[22] H.-K. Lo, M. Curty, and K. Tamaki, Nat. Photonics **8**, 595 (2014).
[23] H.-L. Yin *et al.*, Phys. Rev. Lett. **117**, 190501 (2016).
[24] R. Bedington, J. M. Arrazola, and A. Ling, Npj Quantum Inf. **3**, 30 (2017).
[25] O. Lee and T. Vergoossen, ArXiv190913061 Quant-Ph (2019).
[26] W. J. Larson and J. R. Wertz, (1992).
[27] M. Er-long *et al.*, New J. Phys. **7**, 215 (2005).
[28] M. T. Gruneisen *et al.*, Opt. Express **23**, 23924 (2015).
[29] S.-K. Liao *et al.*, Nat. Photonics **11**, 509 (2017).
[30] K. Günthner *et al.*, Optica **4**, 611 (2017).
[31] Z. Wang, R. Malaney, and B. Burnett, Phys. Rev. Appl. **14**, 064031 (2020).
[32] R. Dong *et al.*, Phys. Rev. A **82**, 012312 (2010).
[33] V. C. Usenko *et al.*, New J. Phys. **14**, 093048 (2012).
[34] L. Ruppert *et al.*, New J. Phys. **21**, 123036 (2019).
[35] I. Derkach, V. C. Usenko, and R. Filip, New J. Phys. **22**, 053006 (2020).
[36] G. Chai *et al.*, New J. Phys. **22**, 103009 (2020).
[37] V. C. Usenko *et al.*, Opt. Express **26**, 31106 (2018).
[38] S. P. Kish *et al.*, Quantum Eng. **2**, e50 (2020).
[39] I. Derkach and V. C. Usenko, Entropy **23**, 55 (2021).
[40] N. Hosseinidehaj, N. Walk, and T. C. Ralph, Phys. Rev. A **103**, 012605 (2021).
[41] D. Dequal *et al.*, Npj Quantum Inf. **7**, 1 (2021).
[42] D. E. Bruschi *et al.*, Phys. Rev. D **90**, 045041 (2014).
[43] R. Pierini, Phys. Rev. D **98**, 125007 (2018).

[44] Z. Zhang *et al.*, Phys. Rev. A **95**, 012333 (2017).
[45] R. Renner, Int. J. Quantum Inf. **06**, 1 (2008).
[46] A. Leverrier, Phys. Rev. Lett. **118**, 200501 (2017).
[47] M. Christandl, R. König, and R. Renner, Phys. Rev. Lett. **102**, 020504 (2009).
[48] M. Hayashi and T. Tsurumaru, New J. Phys. **14**, 093014 (2012).
[49] M. Tomamichel *et al.*, Nat. Commun. **3**, 634 (2012).
[50] F. Furrer *et al.*, Phys. Rev. Lett. **109**, 100502 (2012).
[51] F. Dupuis, O. Fawzi, and R. Renner, Commun. Math. Phys. **379**, 867 (2020).
[52] J.-P. Bourgoin *et al.*, New J. Phys. **15**, 023006 (2013).
[53] Y. Zhang, editor, *Internetworking and Computing Over Satellite Networks* (Springer US, 2003).
[54] T. Vergoossen *et al.*, Acta Astronaut. **173**, 164 (2020).
[55] Biswas, Sanat K., Abhijit, Mitra, and Srivastava, Anand, in *IAC-18B2110x44754* (International Astronautical Federation, Bremen, n.d.).
[56] J. S. Sidhu *et al.*, ArXiv201207829 Quant-Ph (2020).
[57] R. Kaltenbaek *et al.*, EPJ Quantum Technol. **3**, 5 (2016).
[58] *ESA Science & Technology - CDF Study Report: QPPF - Assessment of a Quantum Physics Payload Platform* (2019).
[59] A. G. Krause *et al.*, Nat. Photonics **6**, 768 (2012).
[60] T. Liu *et al.*, Nat. Commun. **11**, 2407 (2020).
[61] D. Carney *et al.*, Quantum Sci. Technol. **6**, 024002 (2021).
[62] Q. Zhuang, J. Preskill, and L. Jiang, New J. Phys. **22**, 022001 (2020).