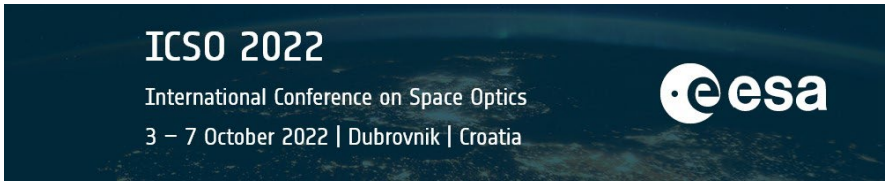
International Conference on Space Optics—ICSO 2022

Dubrovnik, Croatia

3–7 October 2022

Edited by Kyriaki Minoglou, Nikos Karafolas, and Bruno Cugny,



Hybrid BBM92 approach for GEOQKD – lab implementation and future perspectives

International Conference on Space Optics — ICSO 2022, edited by Kyriaki Minoglou, Nikos Karafolas, Bruno Cugny, Proc. of SPIE Vol. 12777, 1277724 · © 2023 ESA and CNES · 0277-786X · doi: 10.1117/12.2689968

Hybrid BBM92 approach for GEOQKD – lab implementation and future perspectives

Bob P.F. Dirks*[a], Gustavo Castro do Amaral[a], David L. Bakker [a], Luca Mazzarella[a], Ivan Ferrario[a], Sander Kossen[a], Michiel Marcus[a], B. Perlingeiro Corrêa[a], Hemant Sharma[a], Alessandro Le Pera[b], Daniele Vito Finocchiaro[b], Martina Ottavi[c], Noemi Scaiella[c], Gabriele Riccardi[c],
[a]Netherlands Organisation for Applied Scientific Research (TNO), Stieltjesweg 1, 2628 CK, Delft, The Netherlands
[b]Eutelsat SA, 32 Boulevard Gallieni, 92130 Issy-les-Moulineaux, France
[c]Thales Alenia Space Italia, Via Saccomuro, 19-21, 00131 Rome, Italy

ABSTRACT

Quantum Key Distribution (QKD) is the most mature quantum technology, having achieved on-ground applications and commercially available products. In this domain, satellite platforms are essential to achieve a communication range reaching the intercontinental scale, acting thus as enablers for the future global quantum internet operation. This paper will report on the main results of the TNO-Eutelsat-TAS Italy project aiming to evaluate a novel hybrid approach for improved QKD performance particularly suited for geostationary orbits (GEO); the Dutch TKI HTSM sponsors the overall activity. We will present the results of lab-based tests of a novel QKD free-space approach that simultaneously implements the BBM92 protocol in both trusted and trust-free mode, following a joint Eutelsat-TNO patent. The trust-free mode between two ground receivers is the standard BBM92 protocol that uses entangled photons and there is no need for further security assumptions on the satellite payload. In trusted mode operation, one of the two entangled photons is measured directly on board. Key material is generated between ground and satellite. Security measures will be needed in the space segment, which therefore needs to be trusted. Further, we will present a demonstration roadmap aiming at free space field test to validate loss and key rate models for a free space link up to 2.5km in one of the arms. We also present a perspective on potential future GEO-based quantum applications beyond QKD.

Keywords: Quantum communications, geostationary QKD, satellite quantum technology, QDK photon source.

1. INTRODUCTION

Quantum technologies promise to drastically enhance the capabilities and performance of computer and networked systems by leveraging unique quantum features such as superposition and entanglement. Quantum Key Distribution (QKD) [1][2], arguably the most mature application, can achieve secure communication between two parties by establishing a random shared secret key. It is important to note that the notion of security addressed here is stronger than the one offered by conventional classical communication as it does not rely on assumptions on the computational power of a potential adversary but, rather, on the laws of quantum mechanics [3]. In particular, the no-cloning theorem [4] ensures that the two parties distilling the key will be able to detect eavesdropping activities in which case, the key is discarded. During more than three decades, QKD research reached numerous technical milestones [5][6], culminating in the first quantum communication satellite Micius [7][8][9]. Satellite platforms are instrumental in extending the communication range of QKD to intercontinental distances [6], thus enabling large space-based quantum networks [10][11][12] and the future quantum internet [13]. Future efforts around space-based QKD have so far focused on Low Earth Orbits [14][15][16]. However, higher altitude platforms, such as those in geostationary orbits (GEO), might offer several benefits such as higher link availability, large coverage, and nearly no tracking required, but at the cost of higher link losses. Here, we focus on the experimental demonstration of a hybrid system that combines trust-free and trusted mode QKD operation, which can be operated in parallel and introduced in ref. [17]. The proportion of key material generated by either one of the two modes can be controlled such that the amount of secure key material is maximized given a certain risk-level; the latter is associated

to parts of the trusted key material being compromised by an adversary. In this paper, we explain the method of combining key material, introduce a free-space setup capable of executing ground-to-ground quantum state transfer, a detection system capable of implementing the BBM92 QKD protocol [18], and present the experimental results on secure key generation in both trust-free and trusted mode operation in a laboratory environment. While QKD will be the first foreseen application of the system, we also report on potential 'beyond QKD' applications, which may be possible using the same or slightly modified version of the system.

2. HYBRID BBM92 QKD SYSTEM

As mentioned before, we foresee a hybrid system in which trusted and trust-free mode operations are combined, as schematically shown below in Figure 2-1. In trusted mode, one photon of the entangled pair is directly measured on the satellite by receiver C while the other is sent down to ground receiver A. Key material is then generated between A and C following the BBM92 protocol. In order for A and B to obtain the same key, this procedure shall be repeated between B and C. Receiver C then holds two keys generated in trusted mode that can be combined via an XOR operation, the result of which, is sent to either A or B via an authenticated classical channel. A and B can then establish a common key by performing an XOR operation with their own original key. The term 'trusted' comes from the fact that the intermediate node C, represented by the satellite, includes the receivers which are susceptible to side-channel attacks, and stores classical key material onboard, which is no longer protected by the QKD protocol; therefore, a level of trust must be placed on the intermediate node in order to use the final key. In trust-free operation, both photons are sent to ground stations A and B, which directly generate key material following the BBM92 protocol. In this scenario, the satellite does not have to be trusted as no key material will be generated or stored on board of the satellite, i.e., the generated key is protected by the QKD protocol and A and B need not trust the security of the intermediate node. (They shall, however, be trusted nodes themselves). The advantage of the proposed hybrid system is that the two modes can be operated either separately or simultaneously with a single source of entangled photon-pairs. By means of a variable beam splitter (VBS), the entanglement resource produced by the source can be split between the intermediate node (to perform trusted-mode key generation) and the ground stations (to perform trust-free key generation). This leads to several important advantages:

1) The source can always operate at its highest pair generation rate without saturating the on-board detectors thanks to the VBS; in case of a 1GHz pair generation rate, and a maximum on-board detection rate of 10 MHz, it is sufficient to set the VBS to 1%. The other 99% is sent to B while A get the full 100% of photon rate.

2) It allows one to choose the operation mode based on link availability: if only one of the two satellite-ground links is available – say A –, the system could still operate in trusted mode, generate a key between the satellite and A, and then add trust-free mode as soon as both ground stations are again available.

3) While key material generated in trust-free mode is the most secure, the key rate is low. It can be increased by key from trusted mode by accepting a certain risk of compromise. The combination of both key can be done such that a fully secure key is generated again by sacrificing bits from trusted mode. Depending on the risk level to which the system is exposed or which is accepted by the end-user, more or less key material from trust-free mode operation can be added. It must be emphasized that combining key material of both modes to get to a final secure key can be performed in post-processing.

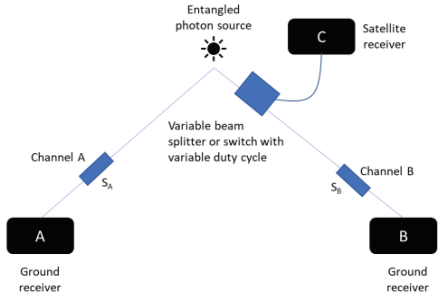


Figure 2-1: Schematic representation of the hybrid BBM92 QKD system. By changing the splitting ratio of the variable beam splitter (VBS), the ratio of photons used for trusted or trust-free operation can be selected. A and B represent the two ground stations while C is the on-board receiver where one of the photons of a pair is directly measured.

It is important to note that the trusted mode operation – within the proposed hybrid approach – differs from the case where the intermediate station produces attenuated laser pulses (i.e. as in BB84 with decoy) for the simple reason that the latter does not have the option to perform trust-free key distribution. In other words, with a single set of onboard resources, namely space-qualified single-photon detectors and an entangled photon-pair source, both operation modes can be achieved with limited complexity overhead.

Combining key material

In the experimental setup, the necessary key material is generated from trust-free and trusted mode simultaneously by varying the duty cycle of an optical switch, resulting in a splitting ratio R, similar to the behaviour of a VBS. For completeness, we identify R=0 to be trust-free operation and R=1 trusted operation. In an actual space mission with a GHz pair generation rate, using optical switch will not be possible because of detector saturation, a VBS shall then be used. In our case the source rate is significantly lower than the maximum detection rate, allowing the use of an optical switch.

For all tests described here, one of the outputs of the splitter is directly fiber-connected to the detectors of C while the other output is connected to a free-space setup that incorporates the detection apparatus of B; node A is connected directly to the other output of the source via an optical fiber.

The goal of the experimental setup is not to simulate side-channel attacks, but, rather, to demonstrate that the hybrid operation allows one to extract more key material given the same set of resources. Therefore, the proposed method of combining key material does not directly influence the experimental design or execution, as this can be done in post-processing by assuming certain attack scenarios.

Depending on the given probability that certain information of the bit string has leaked to the eavesdropper, such as the parity or a certain percentage of bit values, key material from both modes can be combined to yield a secure key of longer length than the individual keys from either mode. A potential attack scenario is associated to a malicious party that approaches the satellite and has a system capable of, for example, detecting the electromagnetic radiation emitted by the detectors, obtaining information on part of the key.

In order to help us quantify this attack, we use information variables $I_1,...,I_M$, which represent information that could be obtained by the adversary about the key through side-channel analysis. For instance, I_1 could model the compromise of the first bit (the attacker knows the value of the first bit), and I_M could model the compromise of the parity. Each of these variables has a probability of occurring, ranging from 0 to 1, described by the set of probabilities $M(I_1,...,I_M)$. The probability of information variables $M(I_1,...,I_M)$ is used to quantify the information leakage risk.

By manipulating the set M, the conditional min-entropy of the bit-string can be calculated for which this risk is relevant, namely the bit string coming from trusted mode operation. Finally, a secure key can be obtained by combining part of this key with the untrusted mode key. The goal is to combine two keys K_1 and K_2 and apply a transformation to obtain a new, shorter key, K′ with min-entropy equal to the sum of the min-entropies of the inputs. This can be generalized to a combination of multiple keys, as long as we can calculate the (conditional) min-entropy of each key. The transformation must be such that the resulting key is uniformly distributed, which can be done with cryptographic hash functions. The recipe that allows one to produce the final combined key is as follows:

1) Take a number of bit strings K_1 through K_N of lengths L_1 through L_N coming from trusted mode BBM92 with unknown min-entropies (since the set M is not known a priori).
2) Calculate the conditional min-entropies of each K_i based on the conditional probabilities of certain information variables $M(I_1,...,I_M)$ occurring for each bit string. Given the conditional probabilities over each respective I_1 through I_M, we can calculate the conditional min-entropies of each K_i.
3) Determine the final key length L′, based on the min-entropies of each K_i conditioned on their respective M(I), and a security parameter λ, representing how close the distribution of the output string is to uniform; a safe choice is λ=40. Finally, $L' = \sum_{i=1}^{N} H_\infty\left(K \mid M(I)\right) - 2\lambda$, with H_∞ the conditional binary min-entropy.
4) Take an appropriate hash function h (such as SHA3-512 or SHA3-256) with output length greater or equal to L′ and calculate the bitstring $K' = h(K_1||K_2 || ... || K_N)$ with the operator || representing binary concatenation. If L′ is

larger than 512 bits, then an appropriate extendable output function (such as SHAKE256, a hash function with custom output size) should be used.

5) Truncate K′ so that it has length L′. The resulting bit string K'_{final} can be used for cryptographic purposes.

Although numerous risk scenarios are possible, which have different impacts on the behaviour of M, we provide a generic approach. First, the capabilities of the adversary need to be accurately modelled. This requires knowledge of an adversary's instrumentation. Ideally, given any scenario where an adversary can launch a side-channel attack, we can perfectly model the information that the adversary receives through their instrumentation. We then translate that to the conditional min-entropy for the bits affected. In order to provide more insight into the calculation procedure, two distinct scenarios are presented in Examples 1 and 2, as follows.

Example 1:

For this example, we have a malicious satellite at a certain distance from our satellite. Our knowledge of the instrumentation on board that satellite states that at that distance, the adversary learns the value of each bit with a maximum probability of 0.6 (where a probability of 0.5 is perfectly random). We refer to this information as information variable I. While the satellite was at that distance, a key K with a total of L = 120 bits was generated. The conditional min-entropy of this key is then

$$H_\infty(K|\, I) = \sum_{i=1}^{120} -\log_2(0.6) > 120 \cdot 0.73 > 87$$

Following the procedure as explained before, we now calculate the final bit string length $L' = 87 - 2\lambda = 87 - 80 = 7$. Next, we calculate the bit string K' = SHA-256(K). Since the output is 256 bits-long, we truncate the output to the first 7 bits to get the cryptographically secure bitstring K'_{final}, which can be used for cryptographic purposes. We note that it is worthwhile to initially store multiple of such bit strings and their min-entropies and to apply the hash once to the concatenation of those bitstrings as explained in the procedure before. The penalty of 2λ would then only be applied once.

Example 2:

Suppose we need a final key K'_{final} to be a AES256 input string, acting as input to the AES encryption protocol. If there is no risk of side-channel attacks, then we could use a key K_1 consisting of 256 bits coming from trusted mode, as this is the fasted mode to generate a key.

However, if we take the same scenario as in example 1, then we need to combine it with an extra key, K_2, coming from trust-free mode. The question is, what is the length L_2 of K_2? The min-entropy of K_1 is 87, so in order to get a total of 256, we need L_2 to be $256 - 87 + 2\lambda = 169 + 2\lambda$. Taking $\lambda=40$, we require $L_2 = 249$.

To provide insight to the amount of key material that can be generated in different risk scenarios, we present in Figure 2-2 the result of different choices of ratios between key material coming from trust-free and trusted mode. We assume generation for exactly one hour. There is a bit rate of 1 bit/s for the trust-free mode and a bit rate of 300 bits/s for trusted mode (based on previous GEOQKD results [17]). Recall that R=0 means that we only take bits from the trust-free mode and R=1 means that we only take bits from the trusted mode. The yellow, blue, red and green lines represent the probabilities $p = 0.6, p = 0.99, p = 0.997, p = 0.998$ respectively for each bit that the value is known (through side-channel attacks).

The function used here for the key length is:

$$\tilde{L} = \lfloor (1-R) \cdot T \cdot r_{trust-free} \rfloor + \max(0, \lfloor R \cdot T \cdot r_{trusted} \cdot (-\log_2 p) \rfloor - 2\lambda)$$

Where, T is the number of seconds, $r_{trust-free}$ trust-free bit rate, and $r_{trusted}$ is the trusted bit rate. We emphasize that this function and the resulting conclusions only hold for a model where we can estimate an attackers success probability of guessing individual bits generated onboard the satellite.

We see that it is always beneficial to either use R=0 or R=1 in the provided scenario. The turning point is at $p \approx 0.99769$, which is when the rate $\frac{r_{trust-free}}{r_{trusted}} > -\log_2 p$. When $p > 0.99769$, we should only take bits from the trust-free mode and when $p \leq 0.99769$, we should only take bits from the trusted mode. If p would change over time in this scenario, it would therefore be optimal to take all bits from the trusted mode while $p \leq 0.99769$ and all bits from the trust-free mode while $p > 0.99769$. At the very end, all bits from trusted mode would then go through the process we explained before - hashing and truncation.

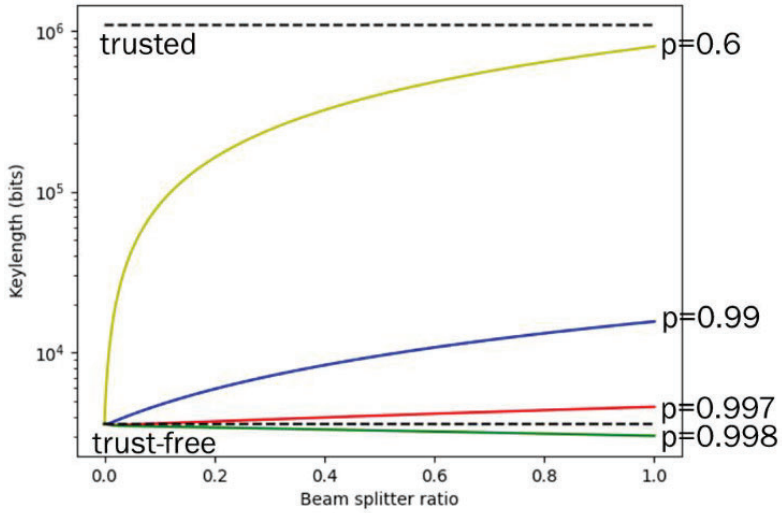


Figure 2-2: The ratio between both modes mapped to the resulting key length in bits when one hour of measurements has been done with a bit rate of 1 bit/s for the trust-free mode (R=0) and 300 bits/s for the trusted mode (R=1). The top black line corresponds to R=1 when all bits are perfectly random (no risk and no penalty of 80 bits) and the bottom black line corresponds to R=0.

3. EXPERIMENTAL SETUP

Ideally, a variable beam splitter (VBS) controls the destination of the single photon from the source. Acting on the VBS, one manipulates the ratio of incoming photons that go to C and B and, thus, the proportion of photons used for trusted and trust-free operation. To implement this, we opted to use an optical switch (OS) as a variable beam splitter since the pair rate produced by the source is low enough so that the detectors are not saturated. Although the OS cannot directly control the ratio of photons for each path, it has a high extinction ratio, and the outputs have a similar insertion loss, making them almost symmetric, allowing one to multiplex the outputs in time, effectively controlling the mean number of pairs used for either mode in a given period. To select the operation period, we considered the electronic and mechanical time delays of the OS. From the specifications of the device used in practice, it takes roughly 3 ms to switch outputs so the operational period of 1 second is chosen so the transition period can be neglected

We can divide the experimental setup into three segments, as shown in Figure *3-1*: the source segment, measuring stations, and synchronization electronics. The first segment contains the entangled photon pair source (EPPS), in which we used the benchtop Polarization-entangled photon-pair source, Emerald, from OzOptics, and the optical switch. Its function is to generate and send polarization-entangled photons at 810 nm through optical fibers to A, B, and through the free-space setup to C (see Figure 6-1 and Figure *6-2*). In addition, it controls whether the photons go to B or C by operating the OS, as discussed before.

The EPPS generates pairs at 810 nm via type 2 spontaneous parametric down-conversion (SPDC), producing, ideally, the following Bell state:

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|H,V\rangle + |V,H\rangle)$$

Where H (V) indicates a photon with horizontal (vertical) polarization. After either the fiber or free-space link, the photons reach the second stage of our setup, the measuring station, as shown in Figure 3-2. First, the photons pass through a polarization controller manually adjusted to compensate for polarization transformations along the link, since the measurement bases must match for correct protocol execution. Then, they arrive at a free space optical system developed to perform random projective measurements on two mutually non-orthogonal bases, e.g., the rectilinear basis (with eigenvalues H, V) and the diagonal basis (with eigenvalues D, A). More specifically, for a given pair of photons generated within a time window, upon arriving at the measurement station, they can either be projected on the rectilinear or diagonal basis if the individual photons are transmitted or reflected at a symmetric beam splitter, i.e., a passively random choice.

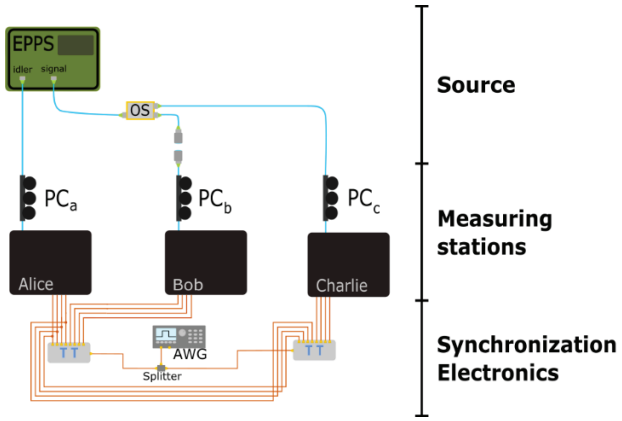


Figure 3-1: Scheme for the experimental setup for the Hybrid BBM92 with the three experimental segments highlighted. The source segment contains the entangled photon pair source (EPPS) and the optical switch (OS). The measuring stations segment includes the polarization controllers (PC) and the free-space measuring systems for Alice, Bob, and Charlie. The synchronization electronics contain the time taggers (TT) and the arbitrary waveform generator (AWG), which produces and distributes the clock signal.

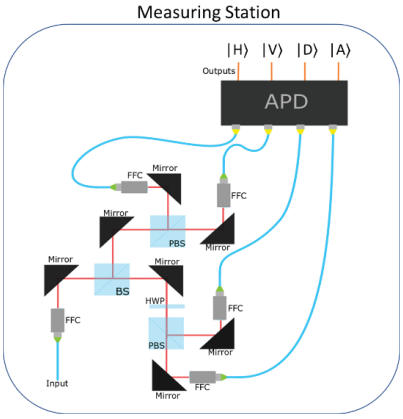


Figure 3-2: Illustration of the measuring systems inside Alice, Bob, and Charlie's station. A fixed focus collimator couples the incoming photons to free-space. After that, a beam splitter (BS) splits the beam into two arms, effectively choosing the projective measurement in a intrinsically random fashion. On the outputs of the PBSs, we couple the light back to fibers and into the photodetectors. Here, we make use of silicon-based avalanche photodetectors (APD).

Finally, we get to the last stage, the synchronization electronics, where the detections from the silicon APDs are routed to a time tagger (TT). This device will very accurately (34 ps RMS jitter) provide a timestamp associated to each detection event. The TT will also receive a clock signal which is used to synchronize the detections between two remote stations. We use an arbitrary waveform generator (AWG) to produce a square-wave signal for the clock and distribute it to the TT with RF cables (to A and C) and through a multiplexed telecom channel via free-space (to B). By using the accurate timestamping of the TT in combination with the clock signal, correlations between two stations can be recovered.

4. SOURCE CHARACTERIZATION

An ideal polarization-entangled photon-pair produces a distinct pattern of coincidences as the projective measurement performed on the individual photons change. This so-called visibility of entanglement metric allows one to determine whether a certain source is producing entangled pairs, given certain assumptions: namely the fact that the density matrix of the bi-partite quantum state that models the pairs can be represented in the Werner form: $\rho_{AB} = \alpha\Psi_{AB} + (1-\alpha)\, I/4$, where Ψ_{AB} is a maximally entangled Bell state, I represents the 4x4 identity matrix, and α is the convex sum parameter associated to the fidelity of the state ρ_{AB} with respect to Ψ_{AB}. In case the visibility of entanglement, measured and averaged over two mutually non-orthogonal bases, exceeds 0.5, the state is said to be entangled; above 0.707, it is said to be non-local.

In practice, the visibility of entanglement is calculated by measuring the coincidence events that occur between the detectors of two measurement nodes (in our case, either A and C or A and B); without loss of generality, we will consider A and B throughout the explanation. This leads to 4 possible detection combinations, associated to detectors A1, A2 and

B1, B2: A1-B1, A1-B2, A2-B1, and A2-B2. Using the TimeTagger devices, it is possible, first, to determine the time delay between the detectors with the help of the clock signal distributed between the measurement nodes. With that information at hand, the correlation peaks associated to each channel combination can be measured: the correlation peaks translate the energy-time entanglement between photons generated via spontaneous parametric down-conversion. By actively changing the measurement basis (which is practically achieved via a half-wave plate mounted on an automated rotation stage), the height of the correlation peaks change, which is plotted, in Figure 4-1 as a function of the half-wave plate angles of A and B.

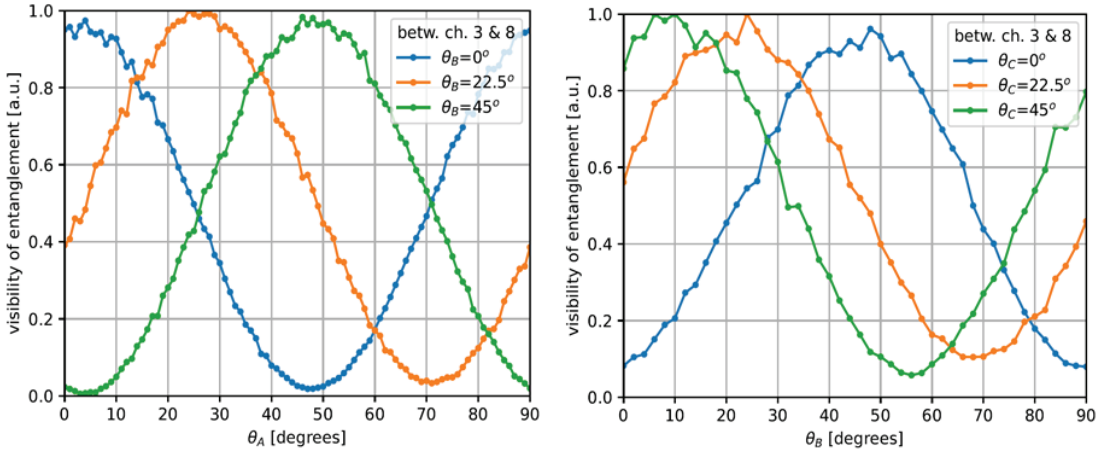


Figure 4-1 The visibility curves measured during the source characterization procedure for trusted (left) and trust-free (right); the latter incurs into an overall extra loss of 17dB with respect to the former due to free-space propagation and fibre coupling efficiencies. At every point in the curves, the correlation peaks were measured for 90 seconds, which are then used to calculate the visibility of entanglement by integrating over a coincidence window centred at this peak. These measurements were then repeated for different settings of the HWP angles at Alice and Bob. Channels 3 and 8 correspond to A1 and B2, respectively.

From a visibility curve, the visibility of the quantum state produce by the source can be calculated as follows,

$$V = \frac{\mathcal{V}_{max} - \mathcal{V}_{min}}{\mathcal{V}_{max} + \mathcal{V}_{min}},$$

where $\mathcal{V}_{min}$ and $\mathcal{V}_{max}$ are the minimum and maximum of the entanglement of visibility curve. The visibility V can then be used to calculate the entangled photon state fidelity with respect to a maximally-entangled bi-partite state $\mathcal{F} = \frac{3V+1}{4}$. To determine the overall visibility, we measure several visibility of entanglement curves, each with a fixed the HWP angle θ_B at Bob and varying HWP angles θ_A of Alice. At each pair of angles (θ_A, θ_B), we measure all four correlation peaks between the D/A and H/V channels at Alice and Bob and calculate the visibility of entanglement $\mathcal{V}_{\theta_B}^{(i,j)}$ (with i the D/A or H/V channel from Alice and j the D/A or H/V channel from Bob) –Figure *4-1* only depicts one of these curves. We then calculate the visibility $V_{\theta_B}^{(i,j)}$ using the above equation and taking the average over all:

$$V = \frac{1}{N} \sum_{\theta_B, i, j} V_{\theta_B}^{(i,j)}$$

A coincidence rate of 142 per second could be achieved in the current experimental setup for trusted mode operation. The experimentally determined values of coupling efficiencies within the measurement setup and detection efficiencies are 0.6 and 0.46, respectively. Using the curve presented in Figure 5, a total average visibility was calculated of $97.1 \pm 2.6\%$. The entangled photon state fidelity is then found to be $97.8 \pm 0.7\%$. For the trust-free operation, the visibility corresponds to $85.4 \pm 4.3\%$.

5. EXPERIMENTAL RESULTS

In this section, we discuss the key extraction method and the resulting key-rate following the BBM92 protocol [18]. The steps to extract the key from the coincidence counts the following: Alice and Bob measure the received entangled photons

in the X or the Z bases randomly. Then they share their measurement bases, whereby only the results corresponding to projections onto the same basis are kept and the rest discarded; this results in the so-called sifted key. Alice and Bob then convert their measurement results into a bit string by assigning to the counts in H and D (V and A) the value 0 (1); due to the properties of the state generated by the source, which approximates a Ψ^+ Bell state, Bob applies a logical NOT gate on all his bits. Alice and Bob both sacrifice a part of the key to estimate the quantum bit error rate (QBER) of the key; in our protocol, the measurements in the diagonal basis are used for QBER estimation and the ones in the rectilinear basis are kept for key extraction; this estimation is based on the trust-free operation of the experiment. If the QBER is larger than a certain threshold value (11% for the BBM92 protocol) Alice and Bob abort the protocol, otherwise they perform error correction using the Winnow corrector [19], as chosen in our case. During the error correction process, Alice and Bob communicate classically, and information about the key is naturally leaked to a potential eavesdropper. Therefore, error correction is followed by privacy amplification, a step in which Alice and Bob attempt to minimize the information that any eavesdropper could have about the key. Our privacy amplification protocol uses the SHAKE256 hash function [20] to produce an final output key whose length is equal to the entropy of the error-corrected key. The resulting rate of secrete key is shown in Figure *5-1* together with its theoretical estimation taking into account all experimentally determined parameters: source pair rate, detector dark count rate, detector efficiency, detector and electronics combined jitter, and coupling efficiency in the measurement stations.

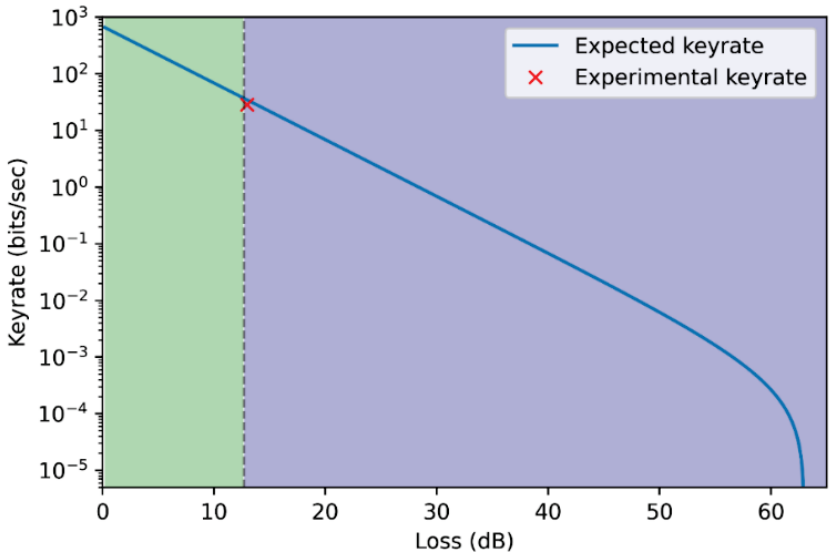


Figure 5-1: Expected (blue line) and experimental (red cross) key rate vs overall losses. The green region represents the system losses (single path free-space), while the purple one represents the link losses.

We were able to achieve a secure key rate of 28.5 bits per second with a QBER of 3.9 % at an overall loss of 12.7 dB in the configuration where one path is free-space connected to the receiver while the other is fiber connected. This quantity is in good agreement with the expected value of 34.6 bits per second obtained using the BBM92 key rate model [21].

6. FUTURE TESTS

The results presented in the previous sections show that parallel operation of trusted and trust-free mode can be realized with our system and that it is a promising way forward for an actual implementation of GEOQKD. As a next step, we would like to extend the distance between the sender and receiver to operate the system in a more representative environment. We currently aim for a 2.5 km free-space link between two towers in The Hague in the Netherlands. This will allow us to compare the expected link losses and secure key rates using our models with actual experimental results in an environment with varying atmospheric conditions, such as turbulence and background light, but also exposed to vibrations of the towers on which we will mount the system.

We have designed and built an optical system to keep the link losses below 30 dB for the 810 nm QKD channel. At this loss, we should still obtain a positive key rate. The system's design is shown below in Figure 6-1Figure 6-2. The three

optical signals in red, yellow, and green propagate in free space, while the blue lines represent optical fibers. The red line represents the transmitter(Tx)-to-receiver(Rx) beacon, while yellow is the Rx-to-Tx beacon, both at 1550 nm. The green line represents the entangled photon signal.

The Tx-to-Rx beacon is responsible for transmitting the clock signal from the source station to the measuring station and is used to align the fine steering mirror (FSM) at Rx. For this, a laser source emits light in the C band (around 1550 nm), which goes to an electron-optical amplitude modulator (AM). We tune an arbitrary waveform generator to produce the clock signal and modulate the Tx-to-Rx beacon via the AM. Then, we use a fiber collimator (FC) to couple the modulated light into free space. The beam impinges onto two mirrors for alignment. After that, it passes through an HWP adjusted for maximum transmission on the following PBS. A quarter-wave plate (QWP) rotates the polarization from linear to circular. Next, a dichroic mirror merges the 1550 nm and the 810 nm beams. Before transmitting the beam through the beam expander (BEX) with a magnification of 10, the Tx-to-Rx beacon and the entangled photons impinge on an FSM and a silver mirror (SM). In the receiver Rx, the beam is collected by a telescopic system with a magnification factor of 3, after which the beams impinge on the FSM, then a dichroic mirror (DM), which splits the 810 nm from the 1550 nm beam. A QWP rotates the signal from circular to linearly polarized light, maximizing the Tx beacon signal on the following PBS. An optical relay (OR) followed by an optical filter are responsible for reducing the background noise and matching the spatial mode. Next, a 90:10 beam splitter (BS) splits the Tx beacon: the 10% arm goes to a quadrant detector which feeds-back the receiver FSM control. Finally, the 90% arm goes to the free space detector, which recreates the clock signal to synchronize the time tagger.

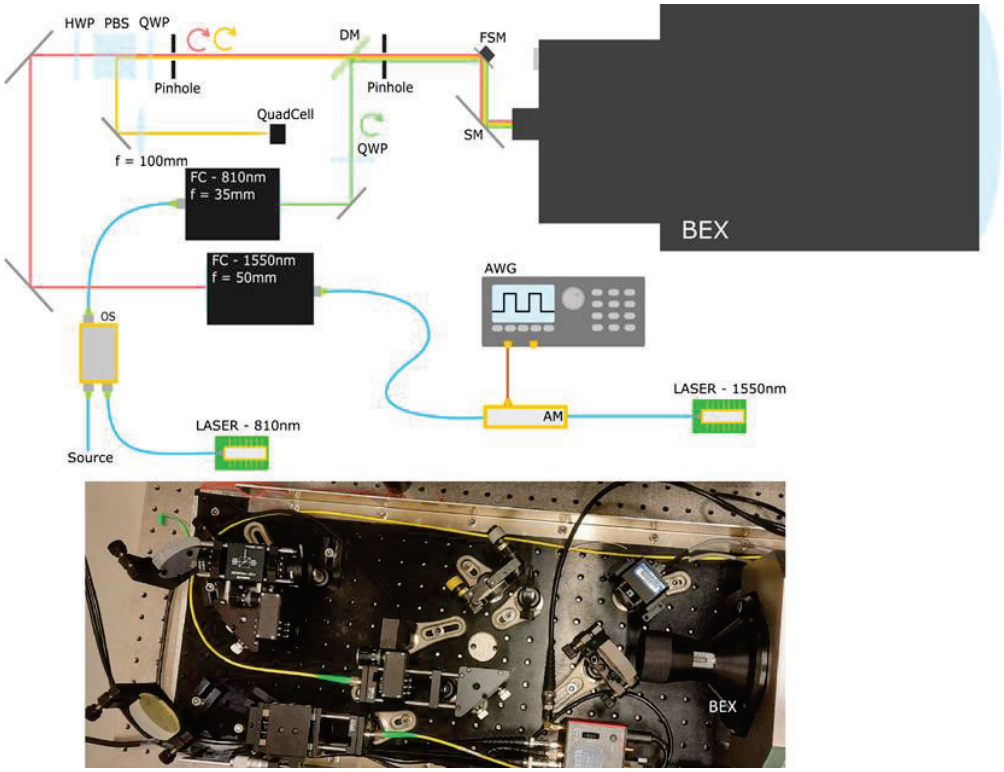


Figure 6-1: a) Transmitter (Tx) side of the system designed to perform BBM92 QKD over 2.5km free space. b) Transmitter setup in the laboratory. The AWG, OS, lasers and AM are not in the picture, because they are spread in the lab.

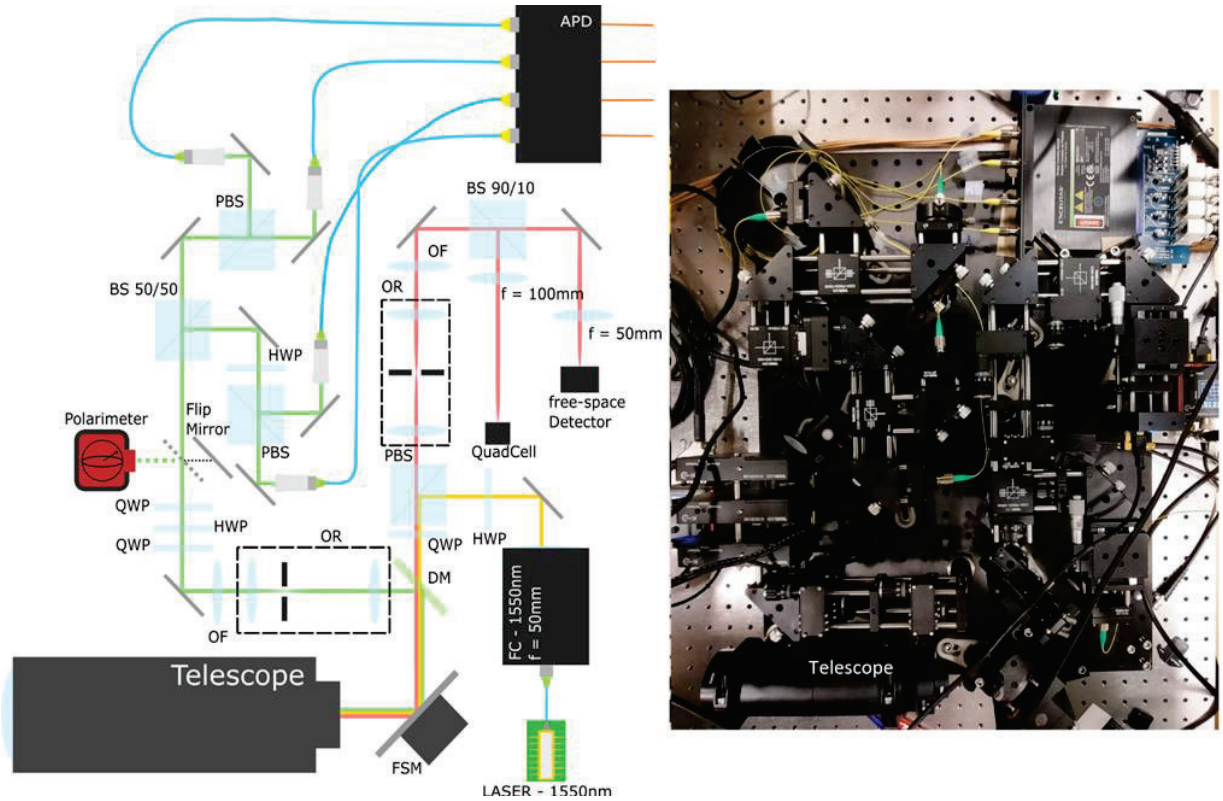


Figure 6-2 a) Schematic drawing of the receiver side (Rx) of the system. b) Receiver setup developed in the lab.

The system for 810 nm is responsible for: transmitting the entangled photons; adjusting the polarization on the receiver; and measuring the photons. The first element of this system is an optical switch (OS) in the transmitter. This changes between the input from the source or the laser at 810 nm. For key distribution, we set the OS path such that the entangled photons are transmitted. In the other mode, it switches to the laser so that the polarimeter at the receiver can measure the polarization transformation along the channel and the measurement bases of A and B can be co-aligned. After the OS, a fiber collimator couples the 810 nm beam to free space. A QWP rotates the polarization from linear to circular. The DM merges the 810 nm and the 1550 nm. The optical path is the same for 1550 nm until the next DM at the receiver. Similar to the previous system, an OR followed by an OF filters the background noise. For the 810 nm channel, we designed the OR to have a magnification of 1/3 to reduce the beam width so that they can be directly coupled into fiber without the need of an extra collimation device. Before the measuring system, we have the polarization control structure, which contains three wave plates (two QWP and an HWP) attached to motorized rotation stations, a flip mirror, and a polarimeter. The polarization controller acts when the flip mirror directs the beam to the polarimeter, and the OS switches the output for the laser (on this order, so it cannot harm the APDs). The polarimeter feeds the rotors so they can act on the wave plates to align the incoming light to the desired polarization state. After compensating for the polarization transformations on the channel, the OS switches the output then the flip mirror is moved away from the beam. Therefore, we automatically control the polarization on the receiver.

The last system provides the Rx-to-Tx beacon signal. This setup is responsible for aligning the FSM at Tx in such a way that the Tx *tracks* the position of the Rx, allowing one to maximize the antenna gain, thus minimizing the losses on the quantum channel. We use another laser at the C band as the source for the Rx beacon. A FC couples the light into free space. An HWP maximizes the output on the reflected port of the following PBS. Then, a QWP rotates the polarization from linear to circular. Since the beam is in the C band, it transmits through the DM. Then, it reflects at the FSM and goes to the Rx telescope. Thus, the BEX receives the beam on the transmitter side. The beam reflects on the silver mirror and the FSM and passes through a DM and a QWP. The QWP rotates the polarization from circular to linear, so the beam reflects on the following PBS. Finally, the beam reaches a quadrant detector that feeds the control loop for the Tx FSM.

Currently the system is integrated with the QKD setup in our laboratory and is used for all lab tests. Before moving to the demonstration at 2.5km, an interbuilding link of ~150m link between the TNO and TU Delft is currently running for functionality tests. Results of this test were not yet available at the time of writing of the paper.

7. BEYOND QKD APPLICATIONS

This article focuses on the experimental results of a future space-based quantum communication system. In this context, the aim is to establish a secret key between two parties. QKD is an established technology that was implemented using both weak coherent pulses and entangled photons. However, it is worth noting that single and entangled photons are the critical components for many quantum technology applications different from QKD. For example, present-day single photon sources realized with weak coherent pulses can be used to implement quantum digital signature [22] and measurement device independent QKD [23]. Furthermore, entangled photons are required for teleportation [24], quantum secret sharing [25], distributed quantum computing [26], remote clock synchronization [27], conference key agreement [28], and quantum-enhanced interferometry [29]. These applications leverage the quantum properties of entangled states to achieve advantages compared to classical protocols and have been implemented in proof of principle experiments. Blind quantum computation is an important application with a potentially high impact for the future quantum internet. Therefore, we now briefly discuss this case to show the potential role of our hybrid system in applications beyond QKD [30].

In blind quantum computing, a party, the client, might want to exploit the computational capabilities of a server to perform a certain computational task without the server gaining knowledge of the actual computation being performed. This can be done by using shared entangled states as a resource. More precisely, the client will prepare qubits with a random relative phase, not shared with the server. After entanglement is generated between the client and server qubits, the client teleports the states to the server. Then the client instructs the server to perform certain operations, namely certain rotations and measurements on the received state. We must assume here that the server has a quantum memory available to store the quantum state for the duration of the operation. Still, because of the unknown initial relative phase, the server cannot reconstruct the client desired operation. One can show that the client can verify the actual “blindness” of the protocol provided that the fidelity of the teleportation operation, the entanglement rate, and the memory time meet certain thresholds. In particular, following [30], we can show that for an entanglement distribution rate between the client and the server of 10 Hz and a memory time of 10 s, the blindness can be verified if the fidelity of the entangling operation is above 0.85, a value achievable with present-day technology. An entanglement rate of 10 Hz is possible using a 10 GHz source rate, even considering a double channel loss of 41 dB, a value compatible with GEO [17]. A 1 GHz source would achieve a 1 Hz entanglement rate; this scenario could still meet the blindness threshold of 0.85 provided that a 100 s memory is available. There is a trade-off between the entanglement rate and memory time. It is also worth noting that the threshold on the teleportation fidelity increases if the product between the entanglement rate and the memory time decreases. Our hybrid system can achieve performance compatible with the requirements for blind quantum computing, provided that suitable quantum memory will be available; the storage time requirements on the latter will probably be achieved in the short term [31]. It is also worth noting that quantum memories will have a fundamental role in implementing the protocol mentioned above and enhance the performance of future quantum networks [11].

In general, multi-parties applications require multipartite entangled states such as the Greenberger–Horne–Zeilinger (GHZ) state as a resource. Currently, there are no reliable sources of multipartite entangled states, and it seems unlikely that this will change in the near future. Multipartite entangled states can be distilled starting with Bell states. Thus, entangled photon sources are key components for implementing future quantum technologies applications and for developing the future quantum internet.

The experimental results presented in this paper are meant to be included in a broader picture, consisting of the countless national and international QKD initiatives that are being carried out all over the World. As the technology necessary to take QKD to the space level is evolving, the hybrid approach used in GEOQKD is intended to provide a stepping stone towards the development of a space-grade entangled-photon source without the need to sacrifice potentially high secret key rates because of the high double-channel losses. In this respect, we have already worked on the definition of a demonstrator mission based on a LEO satellite. In preparation for an in-orbit test, the mission feasibility study has been performed (including the assessment of the obtainable performances in terms of secret key rates and volumes), the platform category has been selected, and the payload accommodation study has been carried out. While a LEO demonstrator is not fully representative of the final GEO mission, and the differences in terms of both required performances and overall impairments between a GEO and a LEO mission are well known, a LEO-based demonstrator could provide a way toward

a fast validation of the technology and a confirmation of the models used in the definition of the losses and secret key rate. It would also lead to the analysis and mitigation of loss sources that typically generate more stringent requirements in LEO-based quantum communications than in the GEO case, such as the pointing performances. The assessment of the latter has an interest that goes beyond quantum communications, as the topic is of great interest for virtually every satellite-based optical communication system (because of the strong impact of pointing losses on the overall link budget).

One of the goals of GEOQKD is thus fostering the European product chain positioning in the Worldwide market. Once the technology has reached a high level of maturity, the final goal of a fully operative system based on hybrid constellations with LEO and GEO satellites can be achieved. To this aim, the system should be developed by accounting for integration and full compatibility with the European initiatives carried out in the European Quantum Communication Infrastructure framework by the European Commission and the European Space Agency. Finally, one of the key focus areas of GEOQKD is the analysis of security aspects, which will turn out to be crucial in every future communication system.

8. CONCLUSIONS

In this paper, we have presented a new hybrid scheme that can combine operations in trusted and trust-free modes. Our hybrid system can enhance the performance and, therefore, the commercial value of a quantum communication system based on entangled photons by increasing its overall key rate. We have also shown how to combine bit strings from the trusted and trust-free modes to form a secure key given a risk scenario. We report an entanglement visibility of 97.1 ± 2.6 and an entangled state fidelity of $97.8 \pm 0.7\%$. Furthermore, we report a preliminary secret key of $28.5\ \mathrm{bits/s}$; this value agrees with our theoretical prediction based on the BBM92 protocol. We believe that the parallel operation of trusted and trust-free mode is a promising way forward for an actual implementation of GEOQKD. Future development plans include a free space test over 2.5 km. Our hybrid system has the potential to enhance the performance and widen the operations scenarios of space-based quantum communication and to be employed for applications beyond QKD.

9. REFERENCES

[1] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” *Theor. Comput. Sci.*, vol. 560, pp. 7–11, 2014, doi: https://doi.org/10.1016/j.tcs.2014.05.025.

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, Mar. 2002, doi: 10.1103/RevModPhys.74.145.

[3] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, “The security of practical quantum key distribution,” *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301–1350, Sep. 2009, doi: 10.1103/RevModPhys.81.1301.

[4] W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned,” *Nature*, vol. 299, no. 5886, pp. 802–803, 1982, doi: 10.1038/299802a0.

[5] S. Pirandola *et al.*, “Advances in quantum cryptography,” *Adv. Opt. Photonics*, vol. 12, no. 4, pp. 1012–1236, 2020, doi: 10.1364/AOP.361502.

[6] J. S. Sidhu *et al.*, “Advances in space quantum communications,” *IET Quantum Commun.*, vol. 2, no. 4, pp. 182–217, Dec. 2021, doi: https://doi.org/10.1049/qtc2.12015.

[7] J. Yin *et al.*, “Satellite-based entanglement distribution over 1200 kilometers,” *Science (80-.).*, vol. 356, no. 6343, pp. 1140–1144, Jun. 2017, doi: 10.1126/science.aan3211.

[8] S.-K. Liao *et al.*, “Satellite-to-ground quantum key distribution,” *Nature*, vol. 549, no. 7670, pp. 43–47, 2017, doi: 10.1038/nature23655.

[9] J.-G. Ren *et al.*, “Ground-to-satellite quantum teleportation,” *Nature*, vol. 549, no. 7670, pp. 70–73, 2017, doi: 10.1038/nature23675.

[10] S. Khatri, A. J. Brady, R. A. Desporte, M. P. Bart, and J. P. Dowling, “Spooky action at a global distance: analysis of space-based entanglement distribution for the quantum internet,” *npj Quantum Inf.*, vol. 7, no. 1, p. 4, 2021, doi: 10.1038/s41534-020-00327-5.

[11] M. Gündoğan *et al.*, “Proposal for space-borne quantum memories for global quantum networking,” *npj Quantum Inf.*, vol. 7, no. 1, p. 128, 2021, doi: 10.1038/s41534-021-00460-9.

[12] M. Polnik, L. Mazzarella, M. Di Carlo, D. K. L. Oi, A. Riccardi, and A. Arulselvan, “Scheduling of space to ground quantum key distribution,” *EPJ Quantum Technol.*, vol. 7, no. 1, 2020, [Online]. Available:

https://doi.org/10.1140/epjqt/s40507-020-0079-6
[13] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," *Science (80-.).*, vol. 362, no. 6412, p. eaam9288, Oct. 2018, doi: 10.1126/science.aam9288.
[14] A. Villar *et al.*, "Entanglement demonstration on board a nano-satellite," *Optica*, vol. 7, no. 7, pp. 734–737, 2020, doi: 10.1364/OPTICA.387306.
[15] H. Podmore *et al.*, "QKD terminal for Canada's Quantum Encryption and Science Satellite (QEYSSat)," in *Proc.SPIE*, Jun. 2021, vol. 11852, p. 118520H. doi: 10.1117/12.2599162.
[16] L. Mazzarella *et al.*, "QUARC: Quantum Research Cubesat—A Constellation for Quantum Communication," *Cryptography* , vol. 4, no. 1. 2020. doi: 10.3390/cryptography4010007.
[17] B. Dirks *et al.*, "GEOQKD: quantum key distribution from a geostationary satellite," in *Proc.SPIE*, Jun. 2021, vol. 11852, p. 118520J. doi: 10.1117/12.2599164.
[18] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Phys. Rev. Lett.*, vol. 68, no. 5, pp. 557–559, Feb. 1992, doi: 10.1103/PhysRevLett.68.557.
[19] W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. H. Nickel, C. H. Donahue, and C. G. Peterson, "Fast, efficient error reconciliation for quantum cryptography," *Phys. Rev. A*, vol. 67, no. 5, p. 52303, May 2003, doi: 10.1103/PhysRevA.67.052303.
[20] N. Sha, "standard: Permutation-based hash and extendable-output functions. Federal Information Processing Standards Publication 202, 2015." 3AD.
[21] X. Ma, C.-H. F. Fung, and H.-K. Lo, "Quantum key distribution with entangled photon sources," *Phys. Rev. A*, vol. 76, no. 1, p. 12307, Jul. 2007, doi: 10.1103/PhysRevA.76.012307.
[22] P. J. Clarke, R. J. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G. S. Buller, "Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light," *Nat. Commun.*, vol. 3, no. 1, p. 1174, 2012, doi: 10.1038/ncomms2172.
[23] H.-K. Lo, M. Curty, and B. Qi, "Measurement-Device-Independent Quantum Key Distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, p. 130503, Mar. 2012, doi: 10.1103/PhysRevLett.108.130503.
[24] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, "Experimental quantum teleportation," *Nature*, vol. 390, no. 6660, pp. 575–579, 1997, doi: 10.1038/37539.
[25] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Phys. Rev. A*, vol. 59, no. 3, pp. 1829–1834, Mar. 1999, doi: 10.1103/PhysRevA.59.1829.
[26] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, "Demonstration of Blind Quantum Computing," *Science (80-.).*, vol. 335, no. 6066, pp. 303–308, Jan. 2012, doi: 10.1126/science.1214707.
[27] E. O. Ilo-Okeke, L. Tessler, J. P. Dowling, and T. Byrnes, "Remote quantum clock synchronization without synchronized clocks," *npj Quantum Inf.*, vol. 4, no. 1, p. 40, 2018, doi: 10.1038/s41534-018-0090-2.
[28] M. Proietti, J. Ho, F. Grasselli, P. Barrow, M. Malik, and A. Fedrizzi, "Experimental quantum conference key agreement," *Sci. Adv.*, vol. 7, no. 23, p. eabe0395, Aug. 2022, doi: 10.1126/sciadv.abe0395.
[29] E. T. Khabiboulline, J. Borregaard, K. De Greve, and M. D. Lukin, "Optical Interferometry with Quantum Networks," *Phys. Rev. Lett.*, vol. 123, no. 7, p. 70504, Aug. 2019, doi: 10.1103/PhysRevLett.123.070504.
[30] G. Avis *et al.*, "Requirements for a processing-node quantum repeater on a real-world fiber grid," *arXiv e-prints*. p. arXiv:2207.10579, Jul. 01, 2022. [Online]. Available: https://ui.adsabs.harvard.edu/abs/2022arXiv220710579A
[31] C. E. Bradley *et al.*, "A Ten-Qubit Solid-State Spin Register with Quantum Memory up to One Minute," *Phys. Rev. X*, vol. 9, no. 3, p. 031045, Sep. 2019, doi: 10.1103/PhysRevX.9.031045.