The Evolution of Free-Space Quantum Key Distribution

Tamas Bisztray and Laszlo Bacsardi

***Abstract*—In this paper we are looking at the milestones that were achieved in free−space quantum key distribution as well as the current state of this technology. First a brief overview introduces the technical prerequisites that will help to better understand the rest of the paper. After looking into the first successful demonstrations of short range free space QKD both indoor and outdoor, we are examining the longer range terrestrial QKD experiments. In the next step we look at some experiments that were aiming to take free space QKD to the next level by placing the sender or the receiver on moving vehicles. After the terrestrial demonstrations we focus on satellite based experiments. Finally, we explore hyper-dimensional QKD, utilising energy−time, polarization and orbital angular momentum (OAM) degrees of freedom.**

***Index Terms*—free−space quantum communication, quantum key distribution**

I. INTRODUCTION

QUANTUM key distribution (QKD) is an emerging technology which was born to solve one of the biggest information security issues, namely the obsoletion of conventional public key cryptography. Although public key cryptographic primitives such as RSA (Rivest−Shamir−Adleman protocol) and DH (Diffie−Hellman protocol) are still used today, in the near future when quantum computers reach quantum supremacy these protocols will not provide any security since the algorithms to break them are already developed, we are just waiting for quantum computers to catch up. However, information security is not only endangered in the future but in the present as well. Messages that are recorded today can be deciphered when a quantum computer becomes available. Quantum key distribution therefore, should be implemented in advance before quantum computers arrive. But what is exactly quantum key distribution and how does it solve this problem. In short, it replaces the conventional public key algorithms and establishes a perfectly secure secret pair of keys between the communicating parties. This shared secret key than can be used in symmetric cryptographic protocols to encrypt secret messages and this can be sent through a regular channel same as today. The security of this technology is based on the principles of quantum physics, unlike in public key algorithms where the security relies on assumptions such that a certain mathematical problem is hard, like discrete logarithm or prime factoring. There are two major obstacles in the way of implementing QKD on a large scale. The first on is that this technology is expensive and still not perfectly mature and a lot of things needed to be developed, such as quantum memory or quantum repeaters. The second is that in a network we would like to establish secure communication between every node, therefore a secure key−exchange between every node. To achieve this, we need to have a direct cable connection without breakpoints if we want to achieve maximum security. This is not possible in most of the cases since if we would like to describe a network it is usually a k-vertex or edge connected graph so if some parts of the network fail the other nodes can still reach each other. A subgraph of the network might be complete but the whole network is usually not. Moreover, it might not be even possible to establish direct connection between some of the nodes with optical cable, due to geographical separation. This is a major problem that needs a solution. Free space quantum key distribution can be the answer to this challenge, where instead of optical cables all we need is line of sight. The nodes moreover are not fixed to work in one pair. After the secret key is established between two they can turn in other directions. This area is further important for satellite communication which is an absolute necessity for building a global quantum encryption networks. It also has a lot of challenges as the weather or day and night cycles can influence the key exchange rate to name a few.

T. Bisztray is with the Department of Networked Systems and Services, Budapest University of Technology and Economics. E-mail: t.bisztray@gmail.com L. Bacsárdi is with the Institute of Informatics and Economics, University of Sopron. E-mail: bacsardi@inf.uni-sopron.hu The research was supported by the Hungarian Scientific Research Fund – OTKA PD-112529. The research is connected to COST Action CA15220 Quantum Technologies in Space. The research was further supported by the National Research Development and Innovation Office of Hungary (Project No. 2017-1.2.1-NKP-2017-00001).

II. TECHNICAL BACKGROUND

In classical information technology information is encoded in bits, zeros and ones. In quantum communication the information is encoded in qubits [1]. These can contain information about zero and one at the same time. An example of such can be photon polarization or magnetic moment. Figure 1. shows a simple visualisation for the following experiment that will help the reader to understand the nature of qubits. Here the line represents the path of the photons (from left to right) while the boxes are the polarizers. In the first experiment we polarize light vertically with the first box. Then we apply another vertical polarizer and what we see is that all of the light comes through and the intensity remains unchanged. In the second experiment we change the second box to a horizontal polarizer, and this time we see that no light comes through. The third time a diagonal polarizer is used that has a $45°$ angle with the vertical polarizers reference frame. Now we see that light comes through but only with 50% intensity, meaning that for the individual photons there is a 50% chance of passing

DOI: 10.36244/ICJ.2018.1.4

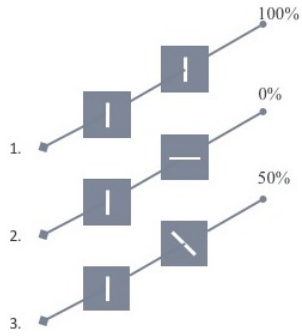

Fig. 1: Experiment with photon polarization. 1. First light is polarized vertically and then it goes through another vertical polarizer (measurement). Here the light comes through with unchanged intensity. 2. After being vertically polarized now a horizontal measurement is performed. In this case no light comes through. 3. Here the second measurement is diagonal with 50% of the light coming through.

Fig. 2: Schematic overview of the BB84 protocol. Alice sends random bit values to Bob encoding the information into photon polarization. She is randomly alternating between the rectilinear and diagonal bases as each bit value can be represented in both. $\longleftrightarrow = \nearrow = 0$ *and* $\updownarrow = \nwarrow = 1$. *Bob is also randomly alternating between the measurement devices when detecting the incoming photons.*

or not passing the second polarizer. To be precise the actual probability of successfully measuring a photon in a β state which was prepared in an α state can be described with the following simple formula

$$|\langle\beta|\alpha\rangle|^2 = cos^2(\Theta),$$

where Θ is the angle difference between the shared reference frame [2]. It is easy to see now that in the first experiment both polarizer was vertical so the angle between them was zero. Thus $cos^2(0) = 1^2 = 1$ which means that the light will pass through with probability 1. The bra–ket $\langle .|.\rangle$ notation is the standard notation for describing quantum states. Ket $|.\rangle$ is a column vector while bra $\langle .|$ is a row vector. This is known as the Dirac notation. Bra and ket are each others Hermitian conjugate.

A. BB84 protocol, a prepare and measure approach

The question is now how can we use this property of light to establish a shared secret between the communicating parties. The BB84 protocol [3] was the first one to implement this. The schematic overview of the following steps is shown in Figure 2.

1) Alice encodes her random sequence of bits in horizontal, vertical, diagonal and anti−diagonal polarization where $\longleftrightarrow = \nearrow = 0$ and $\updownarrow = \nwarrow = 1$ (Alternating randomly between the bases)
2) Bob chooses randomly between rectilinear and diagonal measurement bases for each event
3) Bob will have a binary sequence as the result of the measurements. (It might be less then the amount Alice sent)
4) They compare their measurement bases
5) Alice and Bob keep the results only if they used similar bases
6) This binary sequence is called the shifted key

The security of this communication builds on Heisenberg's uncertainty principle which says that measuring one of these properties such as rectilinear or diagonal polarization, randomizes the value of the other property. It can be also proven that both of these measurements cannot be performed at the same time. The eavesdropper has a probabilistic chance to get information on this key but by performing an intermediate measurement on the transmitted information she introduces errors. The first challenge is that the results by default can contain some errors due to the imperfection of physical components, but this error rate can be determined and the protocol should allow to recover from this. The eavesdropper further increases this and to discover her presence Alice and Bob can compare a random subset of they shifted key with the assumption that the errors are evenly distributed. If the error rate is high the whole key is discarded, otherwise Alice and Bob will perform post processing steps to exclude all errors and further reduce the probabilistic information Eve might possess to arrive to their private shared secret. These post processing steps as well as the error estimation is communicated through a conventional public communication channel with a strong assumption on it's authenticity, such that Eve cannot perform a man in the middle attack nor can compromise the integrity of the messages. The second challenge is that it's difficult to produce single photons whose arrival times are not randomly distributed. Therefore, one approach is to use incoherent weak light pulses. The problem with this is that Eve can split the pulse into two or more photons measuring only one and letting the others arrive to Bob. This way she will introduce no additional error and can gain significant amount of partial information. Alice and Bob can estimate Eve's partial information on the string both from the detected error frequency and the optical pulse intensity. The post processing steps therefore must include privacy amplification [4] to further reduce Eve's partial information. During the error correction step which is usually done by LDPC algorithms (low density parity check) the key string is divided into chunks with the assumption that the errors are evenly distributed and each chunk contains only one error with very high probability. The parties compare these parities until they can do 5 round without finding any error. Of course after each round the string is permuted and new chunks are selected. When the parity of two chunks are compared one random bit has to be discarded so Eve cannot gain information on the parities. Unfortunately, this means that a lot of key−bits are discarded.

During these steps together with the privacy amplification Eve's actual information on the secret key becomes negligible.

For summary the key that the users get by simply detecting the incoming transmission is called the raw key. This contains detection events even from not compatible bases. Next during the shifting step, when only measurements performed in the compatible bases are kept, is when we acquire the shifted key. If there were no eavesdropper and no errors these would be identical, but even without an eavesdropper this contains errors. The rate of this error is significant not only for eavesdropper detection but if it is high the error correction would take a lot of rounds discarding a lot of key−bits. For this it is important to differentiate between the shifted key and the secret key which we get from the shifted key after the post processing steps.

It is also important to note that over large transmission distances the fibre attenuation can be very significant and this effect cannot be mitigated by amplifying the weak signals since quantum information cannot be amplified and thus no repeaters can be built to prolong the coverable distance.

B. Entanglement based key establishment

There is a spooky quantum physical phenomena called entanglement that can be also used to securely establish a secret key between Alice and Bob [5]. To obtain entangled pairs a strong laser shoots at a nonlinear crystal. This shooting is periodical with a certain pump frequency. The majority of the photons pass through the crystal but some of them undergo spontaneous parametric down conversion and two weaker pulse will leave the crystal. By the law of conservation of energy and the law of conservation of momentum, the pair have combined energies and momenta which is equal to the energy and momentum of the original photon. The laser has to be adjusted such that after the down conversion the average photon number in the weaker pulses must be between 0.1 and 0.5. Depending on the crystal used the correlation between the polarization can be Type I, where the photons share the same polarization or Type II where they have perpendicular polarization. But what do we mean by entanglement? The polarization of pairs is not determined, it is neither horizontal, vertical or in any other well definable state. If we send the pairs far apart from each other and we perform a measurement on one of them, in case of a Type I pair the polarization of the other half will be instantaneously determined to be polarized in the same way as the result of the measurement on the other half. Meaning if we perform the same measurement we will get the same result 100% of the time. The strange thing about this phenomena is that the pairs can be space like separated in a way that when the measurement is performed on one half, the same measurement is performed on the other before light could reach from one half to the other. However, information cannot be transmitted with this method faster than the speed of light since the parties need to communicate to choose the same measurement base in order to extract information out of this phenomena. This entangled state can be written as

$$|\Psi\rangle = \frac{1}{\sqrt{2}} |H\rangle_A |V\rangle_B - \frac{1}{\sqrt{2}} |H\rangle_A |V\rangle_B ,$$

for a Type II correlation with probability amplitudes $\frac{1}{\sqrt{2}}$, meaning there is a 50% chance to measure either horizontal or a vertical result but then the state of the other half is determined to be the opposite.

The photons are now anti−correlated. To test their entanglement, we can preform a Bell−experiment. To understand how that works lets do a game between Alice and Bob. They first get an input from the set $\{0,1\}$ (randomly). Then they output 0 or 1 as they wish. Let's call Alice's input A and output a, while Bob's input is B and output is b. The rules are the following:

- If $A \vee B = 0$ they win if $a = b$ // $(A \cdot B = 0) \rightarrow$ win if the answers are correlated
- If $A = B = 1$ they win if $a \neq b$ // $(A \cdot B = 1) \rightarrow$ win if answers are anti−correlated

If they win they get +1 coin if they loose they get nothing. We can write down the expected value of their winnings by looking at the probabilities of correlation

$$S = P_c(A_0B_0) + P_c(A_0B_1) + P_c(A_1B_0) + P_a(A_1B_1).$$

Here A_0 denotes that $A = 0$ and P_c stands for the probability of a correlated answer while P_a is for anti−correlated. Alice and Bob cannot communicate during the game. If they play randomly they win only 50% if the time so they previously agreed on making a 0 output no matter what the input is. Then the previous equation becomes: $S = 1{+}1{+}1{+}0$. From this it is obvious that classically $1 \leq S \leq 3$.

Note: In the most common Bell test called the CHSH inequality they get -1 for an uncorrelated answer. With that the equation is

$$P_c(A_iB_i) = P(a = 1, b = 1|A_iB_i) + P(a = 0, b = 0|A_iB_i)$$
$$P_a(A_iB_i) = P(a = 1, b = 0|A_iB_i) + P(a = 0, b = 1|A_iB_i)$$
$$E(A_iB_i) = P_c(A_iB_i) - P_a(A_iB_i).$$

In this case, the expected winnings are

$$S = E(A_0B_0) + E(A_0B_1) + E(A_1B_0) - E(A_1B_1),$$

with $S \leq 2$.

Alice and Bob would like to do better than that so although they cannot communicate classically they can share a Bell state (Type I). $|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. The measurement they perform on this will be the random input A and B. For Alice $A_0 = 0°, A_1 = 45°$ are the measurement angles, for Bob $B_0 = 22,5°, B_1 = -22,5°$. Now we would like to get correlated outcomes for A_0B_0, A_1B_0, A_0B_1 but uncorrelated results for A_1B_1. In the cases of A_0B_0, A_1B_0, A_0B_1 the angle is $\pi/8$ between the reference frames. For A_1B_1 it is $3\pi/8$.

In the case : $A \vee B = 0$ they win if $a = b$. According to the experiment in Figure 1, and our formula: $|\langle\beta|\alpha\rangle|^2 = cos^2(\Theta)$, we know that the probability that they win is $cos^2(\frac{\pi}{8})$.

In case of: $A = B = 1$ they win if $a \neq b$. Getting the same result is $cos^2(\frac{3\pi}{8})$. But now they win if the answers are anti−correlated. The probability of that is $1 - cos^2(\frac{3\pi}{8})$ which can be show to be equal to $cos^2(\frac{\pi}{8})$.

This gives

$$S = P_c(A_0B_0) + P_c(A_0B_1) + P_c(A_1B_0) + P_a(A_1B_1) \leq$$

$$\leq 4 \cdot cos^2(\pi/8).$$

Since $cos^2(\pi/8) \approx 0.85$ it follows that $S \leq 3.4$.

If an experiment is conducted and from the collected data we see that the coincidences (winnings) are greater than what a classical experiment would allow and the classical inequality is violated than we can be sure that indeed the incoming photons were entangled since we previously showed that classically $1 \leq S \leq 3$. This requires a large number of measurements with relatively high detection efficiency to successfully determine the violation. In case of the CHSH inequality a value grater than 2 is needed to prove the violation. The most commonly used protocol for entanglement based QKD is the Ekert protocol. In this case the coincident detections where the parties used the same measurement bases is used for the key establishment. In the case of not compatible measurement angles the results are recorder and used for the CHSH inequality or another Bell test.

III. ACHIEVEMENTS IN THE 1990'S

The first implementation of a quantum key distribution system that used free air as the optical path took place in 1991 [6]. Here the authors used a prepare and measure protocol to transmit the information from Alice to Bob. The bases that the information is encoded in are the rectilinear basis (horizontal vs vertical polarization) and the circular basis (left circular vs right circular) which can be used instead of the diagonal base in an equivalent way. Incoherent pulses are produced by a green LED that is filtered and directed on a horizontal polarizer. This light is then modulated Pockels Cells $-$(an optical component that can change the light's polarization direction as a function of applied voltage)$-$ to achieve one of the four polarization states which is then detected by Bob. The intensity of this light is around 0.1 photon per pulse. This disallows the eavesdropper to further split the pulse into more photons. In this scenario the quantum channel was 32 cm free air.

This light intensity was good for demonstration and the given short distance, but such weak pulses would be lost due to noise and channel attenuation over larger distances. The low efficiency of detectors (9%) used in the experiment further limited the key rate of transmission. As a result, over 715.000 pulses were sent and only around 4000 were detected. This means that the laser has fired 715.000 times but due to channel attenuation or because of imperfection in the physical components combined with the low detection efficiency the detectors fired only 4000 times. Approximately half of the detections took place in the correct basis and the process took 10 minutes of real time. Without an eavesdropper the parties ended up with 754 bits of shared secret. With an active eavesdropper this was reduced to 105 bits leaving a lot of room for improvement.

The first demonstration for a successful free space quantum key$-$exchange in an outdoor environment was published in 1996. [7] The approach was similar to the previous one in terms of information encoding but instead of circular polarization a diagonal base state were used by adding a second Pockels cell. The experiment was conducted under bright daylight conditions over a 75m distance. After traveling through the air the single photon was focused back into an optical fiber. The small fibre diameter $(3 - \mu m)$ limited the angle through light could arrive which prevented background light coupling into the system. Using two silicon avalanche photodiodes with (50%) efficiency the achieved transmission rate was 1 kHz.

The next big step in free space QKD was the experiment done by a group of physicists at University of California, Los Alamos National Laboratory in 1998 [8]. Similarly to the previous experiments a prepare and measure protocol was used namely the B92. The maximal distance achieved was 950m under nighttime. An average photon number of ≤ 0.1 were used per pulse for transmission. The achieved BER with this setup was 1.5% which was lowered to 0.7% at a 240m distance. Here a laser was used to generate a large number of photons (10^5) with a $\sim$ 1-ns optical pulse which was then attenuated in such a way to reach a 2-photon probability of less then 0.5% and this implies that less than 6 of every 100 detectable pulses could contain 2 or more photons. The laser was temperature adjusted to get a wavelength of 772 nm, which is good against depolarizing effects of atmospheric turbulence. On the transmitter side a beam expander is used to magnify the beam that is directed into a telescope in the receiver side. With the transmitter pulsed at a 20 kHz the achieved bitrate was 50 Hz. The authors further argue that this experiment shows the feasibility of a ground station to satellite transmission. They suggested that under nighttime conditions a 35-450 Hz key generation rate is possible. To mitigate the effects of background photons narrow time windows within which we look for the incoming photons are important. To accurately determine the photon arrival time a bright (classical) precursor reference pulse was used which allows the receiver to set a 1-ns time window.

IV. THE EARLY 2000'S

In 2002 the Los Alamos National Laboratory took their experiment a step further making a quantum key$-$exchange over a 9.81 km free air channel [9]. The experiment was conducted both during daylight and nighttime conditions. During the day the average photon number (μ) was between $0.2 < \mu < 0.8$ and $0.1 < \mu < 0.2$ during the night since the probability that the photon will be successfully detected also depend on the atmospheric transmission efficiency. The other important factor is the detection efficiency which is dependent on the physical apparatus on the receiver side and it's sensitivity towards noise and other interfering factors that makes the system deviate from an ideal setup. These factors can be however calculated to a degree by conducting an experiment with $\mu = 0$ transmission and comparing the results for day and night background generated noise. In this experiment the BB84 protocol was used. Some of the parameters such as the wavelength was unchanged from the previous experiment. The background radiance was mitigated by using spectral, spatial and temporal filtering. In this experiment however no polarization switching techniques were used. Here cryptographic monolithic randomizer generates two random bits to determine

which of the four temperature−controlled diode laser should fire. Each laser corresponds to a state either in the rectilinear or diagonal basis. The lasers will emit a $\sim$ 1-ns, 772-nm optical pulse. On each cycle a 1-ns 1550-nm timing pulse was sent. The authors claim that this setup serves both simplicity and security. The malfunction of the random number generator could however sabotage the security of the system. Moreover, if the adversary manages to determine through some means, which laser fired she will not only know the base but the exact key bit that is transmitted. The photon detectors are silicon avalanche photodiodes cooled to $-20\ C^{\circ}$ operation temperature, with a single-photon detection efficiency of η_{det} $\sim$ 0.61 and a dark count rate of $\sim$ 1.6 kHz. After a 1 s transmission of 10^6 bits for each transmission a 6 second post processing step is necessary only to produce the shifted key resulting in 100 − 2,000 sifted key bits per 1-s quantum transmission. During this experiment 207 1-s transmission was performed during daylight with $\mu = 0.49$ and a $\sim 5.0\%$ BER. This resulted in 394,004 shifted key−bits from which 50,783 secret key−bits was constructed. In comparison 236 1-s transmission was done during nighttime conditions but with $\mu = 0,14$. This decreased the number of shifted key−bits to 192,925. However, since the BER was only $\sim 2,1\%$ the error correction steps discarded much less from the shifted key producing 118,064 bits of secret key. In a practical crypto−system this is sufficient to feed an AES encryption or for very short messages in OTP communication.

A huge stepping stone in free space QKD came in 2006 [10]. This experiment exceeded all previous ones in terms of transmission distance by more than one order of magnitude. The polarization entangled photons were generated at Alices's side 2400 m above sea level. A picosecond−pulsed laser used with a special crystal created energy degenerate entangled photon pairs of 710 nm wavelength. Using the Ekert protocol, −(an entanglements based key sharing protocol)− the photons are detected in the rectilinear or diagonal bases. The singlet state as previously is written as

$$|\Psi\rangle = \frac{1}{\sqrt{2}} |H\rangle_A |V\rangle_B - \frac{1}{\sqrt{2}} |H\rangle_A |V\rangle_B ,$$

where $|H\rangle$ and $|V\rangle$ are the horizontal and vertical polarizations states while the lower indices indicate the spatial modes. One pair is detected by Alice right after generation since the source was located at her side. The other half is transmitted to Bob via a telescope over a 144 km long free space path. The alignment is automatically adjusted with a beacon laser based tracking system to mitigate beam drifting. The optical link efficiency is further attenuated by diffraction, absorption and imperfections in the physical components. The atmospheric losses are around 0.07 dB/Km at these altitudes. Adding up the various factors the attenuation of the whole channel was −25 dB in the best case with 25% single photon detector efficiency that is equivalent to a −6 dB attenuation. On both sides each detection event is labelled with a time tag that Bob sends to Alice who can see which subset of the transmissions arrived to Bob. To check for the presence of entanglement the evaluation of the CHSH inequality is necessary and it's violation was confirmed with a value of 2,5. The experiment however violates the locality loophole to some degree since the detection of the first photon took place with the other photon being still a few meters away, nevertheless the measurement of the other photon was space−like separated. As a result over a 75-s time period key−generation procedure 178 bits of distilled secure key was established which is ∼2.3 bit/s. Such key−rates are not sufficient to feed a modern crypto−system however it shows the feasibility of key exchange over large distances. Considering that over a satellite to earth communication the minimal distance is 400 km, the overall atmospheric thickness is about one order of magnitude less than in this experiment.

Satellite to ground station communication is now becoming a closer reality with these experimental results, however there are still challenges that needs to be solved such as how to aim a narrow beam from a moving object to a fixed station. The feasibility of the latter was demonstrated in 2012 [11], with an aircraft−to−ground downlink experiment from a fast moving airborne platform using the BB84 protocol with $\mu = 0.5$ sending 10 Mpps. This is a significant improvement over the previous experiment where the pulse rate was 1 million per second. The plane was between 1100 and 1300 m and the distance between the transmitter and receiver apparatus was 20 km. Scintillation, beam wandering and broadening was negligible for this experiment.

The total attenuation introduced during the process is constituted by several components. This comprises a free−space loss of 15 dB, atmospheric attenuation between 6−39 dB (9 in average), tracking loss on both the transmitter and receiver side 3 and 1 dB respectively. Furthermore, the attenuation caused by imperfections in optical parts adds another 3 dB and the coupling loss of the diode in the focal plane of Bob adds 2 dB. With this the total attenuation of the 20 km channel length is 33 dB in average but can vary between 30 and 63 dB depending on the weather conditions.

Tracking is accomplished by a GPS based closed−loop tracking system with active course tracking. The downlink transmissions wavelength is 850 nm with 10 MHz pulses where $\mu = 0.5$. The polarizations is done by a four−path laser diode. Bob is using a four−diode single photon detector for the incoming photons. The experiment was conducted after sunset and under new moon conditions. The achieved shifted key rate was 145 bit/s with the actual secure key−rate being 4.8 bit/s with a 4.5% QBER which is sufficient to encrypt transmissions over 1 Git/s.

V. RECENT ACHIEVEMENTS

Experiments to test the feasibility of satellite communication are important to overcome challenges introduced by the channel attenuation, tracking inaccuracy or imperfections in the physical parts. In satellite communication there are different "schools" , shown in Figure 3, that use different methods, each has certain advantages over the others. The first approach is the downlink communication introduced in the previous experiment. In this scenario the transmitter (Alice) is located on the satellite and the receiver (Bob) is on the ground station. The other is the uplink method where Alice is in the

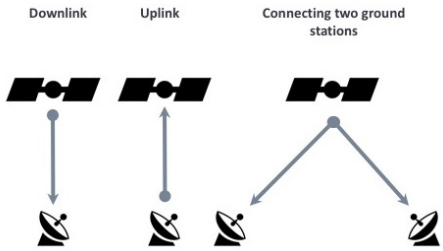

Fig. 3: Schematic overview of satellite based QKD transmission directions. In the downlink scenario the sender is located on the satellite and the ground station is the receiver. This is reversed at the uplink connection. The third scenario is different, here the satellite sends an entangled photon pair at two distant ground stations, where these stations can perform a Bell−type measurement on their half.

ground. As the atmospheric density is lower as we ascend, the downlink communication suffers less from diffraction and beam wandering as these effects are only introduced in the lower atmospheric layers. However, the receiver telescope is facing up and it is more exposed to noise that can come from, for example from a full moon. Both the downlink and uplink connection can serve as trusted node to establish keys between two ground stations or it can simply do a QKD between a ground station and the satellite. First the satellite establishes a secret key with an earth station and later can perform QKD with another earth station where this time it sends the established key as the secret message. The third approach is to directly connect two ground stations with the help of entanglement where the satellite generates an entangled pair and sends it over to the ground stations. In this scenario theoretically the satellite can act as an untrusted node since the parties will be able to detect any malicious activity by performing a Bell test.

A successful demonstration of a ground station based transmitter where the satellite was imitated by a moving truck was done in 2015 [12]. The distance between Alice and Bob was 650 m with the truck moving at 33 km/h to match the angular speed of a satellite traveling at a 600 km altitude with up to $0.75°/s$. On both sides a beacon and a tracking algorithm is applied to synchronize the alignment of the apparatus. The used protocol is a decoy state [13] BB84 where intensity and polarization of the photons are modulated. Weak coherent pulses at 532 nm are sent through a sum−frequency generation method combining a pulsed 810nm and a CW 1550 nm laser with the advantage that the 1550 nm laser removes the phase correlation between the pulses. The 532 nm pulses are sent to the transmitter via an optical fiber. The fiber transmission can introduce rotations in the polarization due to temperature fluctuations and the motion of the fiber. To mitigate this effect, the authors used a polarization characterization and compensation system based on a modified optical chopper which as it rotates lets through 50% of pulses unchanged, 30% is blocked and 20% is polarized in the horizontal, vertical, diagonal, antidiagonal, left circular or right circular polarization. 10% of the passed signals are sent to a single photon detector through a beam splitter which allow the tomograpical characterization of the polarization state to implement a real time polarization drift correction of the states. This drift can be caused by the fiber or other birefringent elements. Before the signal leaves the transmitter any phase or rotation is compensated using a set of motorized wave plates. With a total 30,6 dB attenuation during a 4 second transmission and a signal average photon number of 0.495, a decoy average photon number of 0.120, with a signal QBER of 6.55% and a decoy QBER of 5.49%. From a 5844 bit long shifted key a 160 bit long secure key was obtained through LDPC error correction and privacy amplification.

The biggest milestone in free space quantum key distribution comes from an actual satellite QKD demonstration made in 2016 with satellite Micius. [14] Fiber and terrestrial free space links exponentially reduce the transmission efficiency as they introduce a lot of attenuation. However, in empty space the photon loss is negligible. Therefore, successful demonstrations of QKD were conducted with satellite altitudes between 500 and 1200 km. The protocol as in the previous experiment was a decoy state BB84 at an 850 nm transmitter wavelength. A method for increasing the transmission efficiency would be to increase the signal power, however this is not possible for security reasons described before. The other approach is to mitigate the channel attenuation at all stages possible. The advantage of the downlink method that was used is that beam wandering becomes significant only at the end of the transmission channel due to atmospheric turbulence, but at that point the beam size is larger due to diffraction than the wandering and it won't significantly effect the transmission rate. For a 1200 km transmission the attenuation introduced by diffraction is around 22 dB. To establish the link between the parties a high−precision acquiring, pointing and tracking system is used with beacon leasers. The cascaded multi−stage APT system that was designed by the authors, reduces the pointing error below 3 dB. To reduce background noise temporal and spectral filtering is added to the system, plus the beacon leaser is used for ATP synchronization and to get timing information that is used to tag the received signal photons within a 2-ns time window. During the transmission motorized dynamical polarization compensation must be used to compensate the rotation angle offset induced by the relative motion of the satellite and the ground station. The BB84 decoy state protocol uses 3 intensity levels with 50% of the time signal, 25−25% of the time the two decoy states are transmitted with $\mu_s = 0.8,\ \mu_1 = 0.1,\ \mu_2 = 0$. The single photon detection efficiency of the ground station detectors is 50%. The overall optical efficiency considering the receiving telescope and the fibre coupling on the ground station is ˜16%. The classical communication is conducted through radio transmission between the satellite and the ground station. Every night the satellite passes the ground station an approximately 5−minute time period is open for the key exchange. In a short 273 s QKD transmission the ground station can detect 3,551,136 detection events from which 1,671,072 bits of sifted key is acquired. With the satellite at higher altitudes the shifted key rate decreases from 12 kbit/s at 645 km, to around 1 kbit/s at 1200 km and has a peak rate of 40.2 kbits/s at 530 km. The QBER varies between 1.1−3% depending on the altitude. For comparison if we would like to cover the same distance

with a single fibre and conduct the same experiment even with perfect single photon sources and 100% efficient single photon detectors to obtaining 1 bit of shifted key over 1200 km would take 6 million years.

When the information is encoded in photon polarization the alignment of the transmitter and receiver apparatus becomes necessary. For this reason, they must have a shared reference frame (SRF). In polarization encoding this would ideally mean that if the transmitter sends a horizontally polarized photon the receiving apparatus should be able to detect it in case of a rectilinear detection, with probability 1, since the probability of correct detection is $cos^2\phi$ where ϕ is the angle difference between the devices reference frame, which should be zero. Constantly monitoring the rotation introduced by the apparatus is important, however during the transmission further rotation can be added by the channel and decoherence can worsen the rate of correct detection even if the parties used the same bases. A solution for this problem was proposed and demonstrated in reference [15]. The idea behind this experiment is to send rotational invariant photonic states by combining photon polarization and orbital angular momentum. OAM is a different degree of freedom in angular momentum compared to spin angular momentum which is associated with polarization. In this case the electromagnetic field is described by a twisted wavefront which has a helical shape and it's composed of ℓ intertwined helices with an optical vortex in the center, where photons carry $\ell\hbar$ OAM. Using this mode increases the channel cross−section size and it is only suitable for free space experiments, as single mode fibers are not compatible with this mode over long distances. OAM is conserved in vacuum, however it is affected by atmospheric turbulence. Rotational invariance is achieved with compensating misalignments in polarization with misalignments in spatial modes. A 210m QKD transmission was performed using BB84 decoy state protocol sending the qubits in the decoherence−free subspace of the four−dimensional OAM−polarization product Hilbert space. At the transmitter side there are 4 polarized attenuated lasers that can send photons in horizontal, vertical, right circular or left circular polarization states. Next the photons are transformed into rotational invariant states by a q−plate (space−variant birefringent plate with topological charge q). At the receiver side a second q−plate transforms back the incoming photon into the original polarized state which is then observed by polarizers and single photon detectors. This setup is insensitive to the relative reference frames of the users. The experiment was performed in different setups by rotating the transmitter telescope with $0°$, $15°$, $45°$, $60°$. Only compensation of polarization alterations coming from fiber distortions at Alice's side was performed, without making changes at the receiver side. Without using the rotational invariant states the QBER would depend on the relative angle Θ between Alice's and Bob's reference frames and would make QKD infeasible above a rotation angle of $15°$. However with this approach the key exchange was successfully performed even in the other scenarios.

Satellite based quantum communication would require a cheap and easy to deploy satellite network that could connect terrestrial locations that are not otherwise connectable using fiber based links. Using nano−satellites that could perform orbit−to−ground transmission of QKD both with single and entangled photons, is the proposal of the CubeSat Quantum Communications Mission (CQuCoM) [16]. The approach is to lunch miniaturized satellites massing only a few kilograms called nanosats, that are much easier to lunch, cheaper to develop and operate, and therefore highly reduces the cost of such missions. The CubeSat platform is highly accessible as all parts can be ordered online that are necessary to build a fully functional satellite. CubeSats are rapidly lunched for scientific, commercial and governmental purposes with 120 launched in 2015 and 118 in 2014. Ideally the CubeSats are capable of WCP BB84 QKD (decoy state) and entanglement based QKD where one−half of each pair is used in the downlink transmission and the other half is retained. The major challenge is the high pointing accuracy required to minimize data loss. The CQuCoM CubeSat platform is based on PICosatellite for Atmospheric and Space Science Observations (PICASSO) system which is a 3U (three unit) system but can be modified into 6U.

Using traditional radio frequencies or laser communication the mass of the spacecraft scales with the maximum data rate achievable from space. Small satellites are very limited in bandwidth using radio frequencies. Low orbit cubesats can reach only tens of Mbps. The National Institute of Information and Communications Technology (NICT) in Japan has launched the SOTA (Small Optical Transponder) mission [17], to experimentally prove the feasibility of high−bitrate laser-communication from a micro−satellite platform. SOCRATES (Space Optical Communications Research Advanced Technology Satellite) is a 48 kg microsatellite with Sun−synchronous near−circular orbit at an altitude of ∼600 km. Although the primary purpose was to perform high−speed transmission of data using lasercom a QKD experiment was conducted as well using non−orthogonal, linearly polarized laser sources at $\lambda = 1549$ nm wavelength.

One big challenge in free space QKD is that during daytime transmission the background noise is significantly higher and it can increase the dark count rate which results in a higher QBER and that lowers the key−rate. In an experiment at the Spanish National Research Council [18], researchers performed a 24 hour experiment and monitored how the background noise effects the QBER and thus the secret key−rate. The results show that there is a significant difference between the daylight and nighttime transmission. Between 21:30 and 6:30 there is almost zero background noise and the QBER is only around 2% with a high secret key rate. As soon as the sun rises, the background noise rises, and as a consequence the QBER, making the secret key rate much lower.

From these experiments it is clear that the free space link attenuation may vary between day and night transmission, but the channel itself cannot be improved. The photon detection efficiency due to the imperfections in single photon detectors, like dead time or dark counts, also puts a limit on the number of photons that can be successfully transmitted in one second. Encoding more than one bit of information in each qubit can be a promising method with the aim of increasing the key−rate of the QKD transmission. High dimensional QKD

Year/Ref.	Method	Keyrate	Distance
1991/[2]	ground based	1.2 bit/s	32cm
1996[3]	ground based	1kHz	75m
1998/[4]	ground based	50Hz	950m
2002/[5]	ground based	118,064/236≈ 500 bit/s	9.81 km
2006/[6]	ground based	2.3 bit/s	144km
2012/[7]	aircraft-to-ground downlink	4.8 bit/s	20 km
2015/[8]	ground based (uplink)	40 bit/s	650m
2016[10]	Satellite downlink	1 kbit/s and 40.2 kbits/s (shifted)	1200 km and 530 km

Fig. 4: QKD transmission method, performance and distance overview

using hyperentangled photons that use polarization and at the same time energy−time entanglement −(here the photon arrival times contain the extra information)− as an extra degree of freedom, were successfully performed with a 1.2−km long free−space link across Vienna [19]. This approach not only increases the channel captivity, but it is further beneficial for improving noise and eavesdropping resistance. Information can be encoded in different photonic degrees of freedom, such as transverse orbital angular momentum, discrete photon arrival time bins or continuous variable energy–time mode. Hyperentanglement can be achieved by spontaneous parametric down−conversion in nonlinear crystals and can be described as the tensor product of the two lower dimensional Hilbert spaces, thus acquiring a four−dimensional hyperentangled state. Photon A was measured locally while B was transmitted to the receiver over a 1.2 km free space link, overlapped with a 532-nm beacon laser for pointing, acquisition and tracking. On both sides the parties used a polarization analyzer and an optional transfer setup, that coupled the energy−time degree of freedom to the polarization degree of freedom. The coincidence rate at Alice's side was ~ 400 kcps while Bob detected ~ 350 kcps and an average ~ 20 kcps two−photon detections per second. The average link transmission efficiency was around 18% calculating all losses from source to receiver. To verify the presence of entanglement and evince the presence of an eavesdropper hyperentanglement−assisted Bell−state measurements can be used.

VI. CONCLUSION

Quantum communication and free space QKD is still in an early R&D stage and it will take a lot of time and investment as well as miniaturization and cheaper components, until it can become a true alternative to classical public key algorithms on a large scale. As it is the only method to establish keys with theoretical unconditional security it will be the go to option for a lot of sectors where security is at−most important, such as governmental institutions, banking, military or for strictly confidential company secrets. There are a lot of different approaches and protocols within free space quantum key distribution and at this stage it would be hard to predict which will be the go to direction. As free space quantum key distribution is making it's baby steps there were significant improvements over the last 20 years both in terms of performance and achieved distance. Figure 4. summarizes some of the results that were achieved in this time period.

ACKNOWLEDGMENT

The research was supported by the Hungarian Scientific Research Fund − OTKA PD−112529. The research is connected to COST Action CA15220 Quantum Technologies in Space.

REFERENCES

[1] S. Imre and F. Balázs. Quantum Computing and Communications – An Engineering Approach. Wiley, 2004
[2] L. Hanzo; H. Haas, S. Imre, D. O'Brien, M. Rupp and L. Gyongyosi, "Wireless Myths, Realities, and Futures: From 3G/4G to Optical and Quantum Wireless", Proceedings of the IEEE, Volume: 100 , Issue: Special Centennial Issue, pp. 1853-1888.
[3] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing. Bangalore, India: IEEE, 1984
[4] C. H. Bennett, G. Brassard and J-M Robert, "Privacy amplification by public discussion", SIAM Journal on Computing Vol. 17, no. 2 April 1988, pp. 210-229
[5] Michael A. Nielsen and Isaac L. Chuang. Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge University Press, New York, NY, USA, 10th edition, 2011.
[6] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and John Smolin, Experimental Quantum Cryptography, Journal of Cryptology, 1992, volume 5, pages 3-28.
[7] B. C. Jacobs and J. D. Franson, Quantum cryptography in free space, Opt. Lett. 21, 1854-1856 (1996), https://doi.org/10.1364/OL.21.001854.
[8] W. T. Buttler, et al. Practical Free-Space Quantum Key Distribution over 1 km, Phys. Rev. Lett. Vol. 81, issue 15, pages = 3283--3286, 1988
[9] J. Richard at al. Practical free-space quantum key distribution over 10 km in daylight and at night, Physics Division, Los Alamos National Laboratory, Los Alamos, NM 87545, USA
[10] R. Ursin at al. Free-Space distribution of entanglement and single photons over 144 km, 2006
[11] Florian Moll, Sebastian Nauerth at al. Communication system technology for demonstration of BB84 quantum key distribution in optical aircraft downlinks. DOI: 10.1117/12.929739, 2012.
[12] J-P. Bourgoin, at al. Free-space quantum key distribution to a moving receiver, Opt. Express 23, 33437-33447 2015
[13] Hoi-Kwong Lo, Xiongfeng Ma, Kai Chen, Decoy State Quantum Key Distribution. Phys. Rev. Lett. 94, 230504 2005
[14] Sheng-Kai Liao at al. Satellite-to-ground quantum key distribution, Nature 10.1038/nature23655, 2017
[15] V. Giuseppe, at al. Free-Space Quantum Key Distribution by Rotation-Invariant Twisted Photons, Phys. Rev. Lett. vol. 113, issue: 6, doi = 10.1103/PhysRevLett.113.060503
[16] Daniel KL Oi at al. CubeSat quantum communications mission. EPJ Quantum Technology 2017, volume 1.
[17] A. Carrasco-Casado at al. LEO-to-ground optical communications using SOTA (Small Optical TrAnsponder) – Payload verification results and experiments on space quantum communications http://dx.doi.org/10.1016/j.actaastro.2017.07.030
[18] A. Carrasco-Casado; V. Fernández; N. Denisenko, Chapter from the book "Optical Wireless Communications", pp. 589-607 doi: 10.1007/978-3-319-30201-0_27 Springer, 2016
[19] F. Steinlechner, at al. Distribution of high-dimensional entanglement via an intra-city free-space link, DOI: 10.1038/ncomms15971

László Bacsárdi obtained M.Sc. degree in computer engineering at Budapest University of Technology and Economics (BME) in 2006. He holds an associate professor position at the University of Sopron, where he is the Head of the Institute of Informatics and Economics. He wrote his PhD thesis on the possible connection between space communications and quantum communications at the BME Department of Telecommunications in 2012. His current research interests are in mobile ad hoc communication, quantum computing and quantum communications. He is the Secretary General of the Hungarian Astronautical Society (MANT), which is the oldest Hungarian non-profit space association founded in 1956. He is member of the board of a Hungarian scientific newspaper ('World of Nature') and he is the publisher of a non-profit Hungarian space news portal ('Space World'). Furthermore he is member of IEEE, AIAA and the HTE as well as alumni member of the UN established Space Generation Advisory Council (SGAC).

Tamás Bisztray obtained B.Sc. degree in mathematics and an M.Sc. degree in computer science at Eötvös Loránd Univesity (ELTE). He is a PhD student at Budapest University of Technology and Economics in the topic of Quantum communication algorithms. He is working at Ericsson as an intern on Quantum Communication methods. His current research interests are in quantum communication algorithms and how these can be improved to better serve and enable a quantum encryption network.