Asian Journal of Physics
Vol. 31, Nos 3-6 (2022) 577-591
Available on: www.asianjournalofphysics.com

ap

A brief review of free-space quantum key distribution experiments towards satellite QKD

S Mujumdar, V Bhat, and R Chatterjee

Tata Institute of Fundamental Research, Mumbai -400 005, India

Dedicated to Professor Bishnu P Pal for his enormous contributions to the advancement of research and education in science and technology through his unique vision and outstanding dedication

In the modern era where connectivity is the heart of our civilization, secure communication acquires more importance than ever. Throughout human history people have been using various techniques of cryptography, whose security is essentially based on 'computational complexity'. But with the recent advent of powerful computers and concepts like quantum computing, it's just a matter of time before "classical" techniques are compromised. Quantum cryptography provides security based on laws of physics and hence are future proof. Over the last three decades, quantum cryptography has developed considerably both theoretically and experimentally. In this article, we briefly review selected experimental efforts in the progression of free-space quantum key distribution over the years and how it has reached the current technological pinnacle of satellite-based quantum communication. Finally, we end the article by listing the three demonstrations hitherto of free-space QKD in India.

Keywords: Quantum Cryptography, Quantum Key Distribution.

1 Introduction

The need to securely communicate information via encryption is as old as information itself. One of the most famous or, rather infamous, examples is the German Enigma machine used extensively during World War II. But as ingenious as it might have been, it was eventually broken by the genius of Alan Turing using the world's first computer Colossus. This underlines the vulnerability of classical cryptography. In the year 1982, W Wooters and W Zurek published a stunning idea that an arbitrary quantum state with no prior information cannot be cloned [1]. This is the no-cloning theorem, the bedrock of Quantum Cryptography that provides future-proof security. The earliest known work on quantum cryptography was the concept of conjugate coding introduced by Weisner in the late 60s (unpublished until 1983) [2]. This concept proposed using quantum mechanics to store secret information [2] but its implementation remained in the realm of science fiction. The authors of [3] say "for instance, quantum bank notes [2] require the ability to store a single polarized photon or spin-1/2 particle for days without significant absorption or loss of polarization". But the true realization of quantum cryptography didn't come into force until the mid-1980s due to the popularity of public-key encryption. In the late 1970s, public-key cryptography was introduced as a fully realizable implementation on the then-current infrastructure [4]. Public key encryption (also called asymmetric key distribution) is like a safe and key system, where the receiver creates a safe and hands it to a sender who locks their information in it. The receiver has the key that he can use to unlock it. Any brute force attempt to crack the safe takes an infeasible amount of time. Mathematically, we use one-way functions whose inversion is extremely time-consuming without certain available information which, in this case, plays the role of the key. One example of such a scheme is the algorithm developed by Ron Rivest, Adi Shamir and Leonard Adleman, called the RSA algorithm [5]. But, a breakthrough came when Bennett and Brassard

Corresponding author
e mail: mujumdar@tifr.res.in (S Mujumdar)

focused on using quantum states to transmit information rather than store it. Thus, they could perform private key encryption using quantum bits. Private key encryption is a method in which the sender and the receiver share the same secret key (symmetric key distribution), and use it to encrypt and decipher. The most famous example is the One-time-pad developed by Gilbert Vernam in 1919. In this method, the sender adds to her binary message m the key k which is at-least as long as the message, to obtain crypto-text $((m + k)\text{mod}^2 = c)$. The receiver, after receiving, subtracts the key to obtain back original message $(c - k = m)$. It can be shown mathematically that if the key is sufficiently long, completely random and secret, then even with infinite computing power, one cannot break the crypto-text. Such a cryptography scheme is called Information-theoretic secure and is provably the most secure scheme available.

Bennett and Brassard expanded Weisner's earlier work into a complete quantum key distribution protocol which they published in 1984 [6], thus leading to the name BB84. The first demonstration of free-space quantum key distribution was by Bennett *et al* in 1989 [3]. They used a green LED driven by a weak current, collimated by a pinhole-lens setup, followed by an interference filter and a sheet polarizer. The result of this was a weak coherent pulse with a mean of 0.1 photons per pulse (ppp), about half of which is emitted in the first 500ns. They used two Pockels cells (PC) to randomly choose between the four states. This constituted the Alice, i.e, the sender module. The light then propagated for about 32cm followed by their Bob, the receiver module. Bob had another PC and a calcite Wollaston prism following which the split light went into either of the two photomultiplier tubes (9% quantum efficiency) to measure in either of the two bases. A single timing-and-detection-unit synchronized Alice and Bob via a computer. They used the same computer to control Alice as well as Bob, but with two programs with no cross-talk. A typical run of 10 minutes had 715,000 pulses of mean 0.12ppp sent by Alice, 2000 of which was received in the correct basis by Bob with 79 errors (3.95%). After error correction, this came down to 1379 identical bits between Alice and Bob.

2 Preliminary Experiments

Using detectors sensitive to single photons necessitates a dark environment for the experiments. Therefore, for seven years following Bennett *et al*'s seminal work, many of the experimental demonstrations of QKD protocols were fibre based. Coupling the fibre directly to the detector reduces the noise photons reaching the detector as they are not coupled into the fiber. However, while this is advantageous, fibres are notorious attenuators bringing any realistic single-photon implementation distance, at that time of experimentation, up to 30 km [7]. Nonetheless, in November 1996, Jacobs and Franson reported the implementation of BB84 for distances up to 150m of free space, in daylight [8]. This was a major achievement. They showed that it was possible to get a good enough signal to noise ratio with appropriate techniques. Earlier, the group had already implemented a fibre based BB84 in 1995 [9], and with a few modifications, they adapted the design for free space. Alice's He-Ne laser source was pulsed (0.1μs) using a PC modulator, followed by two PCs for polarisation switching similar to [3]. To expand the beam, it was fibre-coupled into a telescope. Bob had two etalons followed by a telescope to collect the light and a fibre then carried the photons to a Pockels cell-Wollaston prism setup [3]. To correct for the drift in polarisation due to the fibres [10], they employed a feedback loop from Bob's end to Alice's. This way the voltages applied to Alice's PC were dynamically adjusted every minute by sending some dummy photons. The two control computers (one for Alice and the other for Bob) were synchronized using an Ethernet cable which also carried the classical data (basis choice) and the bit information for error calculation between Alice and Bob. They reduced the background using three main techniques. First, the usage of a narrow on-window reduced the background by a factor of 100. Second, the usage of filters and etalons reduced the background by a factor of 10^5. Finally, the small-angle acceptance of the fibre further reduced the background by a large factor of 10^{10}. To quote the authors on this, "These factors were so effective in reducing the background signal that the filtered background rate when focused on a white wall fully illuminated by a direct sunlight was less than 50Hz". The result of all this was a secret key rate of 1kHz at a QBER of 2% before error correction.

3 Free space QKD from static bases

Up until then, the QKD demonstrations either were run in the same computer or used a direct Ethernet connection between Alice and Bob for time synchronization. This limits the key exchange rate. So, two years later, in 1998, Buttler *et al* exchanged quantum keys via the B92 protocol [11,12] over 205m. While the distance per se is not a major improvement from the previous work (of 150m), this served as an important milestone due to their unique time synchronization scheme. Their basic setup (see Fig 1) is quite similar to the one discussed in [5], with two changes. First, Alice needed only a single PC as B92 needs only two non-orthogonal states. Second, the timing scheme was to use a fibre beam splitter between the laser source and PC. One path went directly into the PC. This was a bright pulse containing ~ 10^5ppp. The other went through a longer path (introducing a 50 ns delay) and an attenuator before going into the PC. This was their weak coherent pulse with ~1.4ppp. The bright pulse acted as a trigger on Bob's end which was then used for gating a small time-window 50ns after it. This, in one shot, served as a timing pulse as well as gating which drastically reduced the noise. They also designed a Bob using a beam splitter so that it passively chooses the basis to measure in. This eradicated the need for a dedicated controller for the active switching such as a triggered PC.

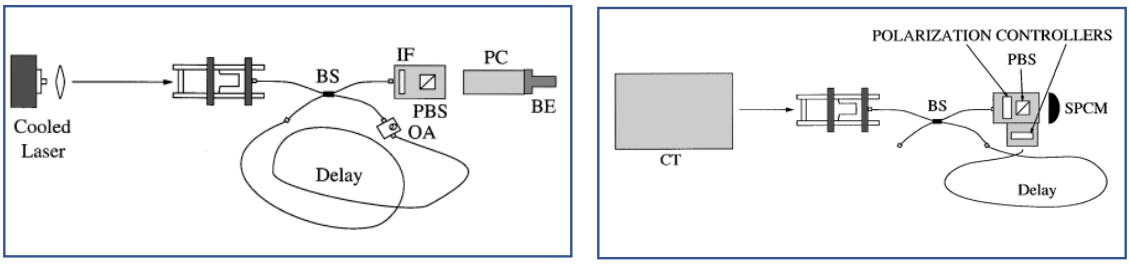

Fig 1. Left panel: QKD transmitter (Alice) and Right panel: QKD receiver (Bob) from Buttler *et al.* Reproduced with permission from [13].

Later, the same group of. Buttler *et al* [13] at the los Alamos National Laboratory, New Mexico in the year 1998, implemented B92 over a distance of about 950m. Their Alice consisted of a temperature-controlled pulsed diode with an interference filter to obtain wavelength of 772nm ± 2.5 nm and a pulse width of ≈ 1ns. The pulse was attenuated to obtain a mean photon number per pulse of $\lessapprox 0.1$. A combination of PBS and Pockel's cell allowed for two mutually unbiased states, namely horizontal ($|h\rangle$) and right circular ($|r\rangle$), to be labelled and sent as bit 0 and 1, respectively. On Bob's side, a 50/50 beam splitter acting as a quantum random switch directed the photons to either of two arms that responded only to a particular bit with 50% probability making the total detection probability of Bob as 25%. The authors report in their paper that with the detectors of efficiencies of 65% and 16%, respectively, they were able to achieve a bit rate of ~ 50 Hz with a QBER of ~ 0.7 % for a distance of 240m and ~ 1.5 % for 500m and 950m. The paper is a classic work representing the power of QKD as a plausible future secure communication methodology. Apart from ideas of how an attack by Eve can be detected, the authors also talk about the first practical application of weak coherent pulses to be used in satellite (specifically, low Earth orbit satellites (LEO)) systems for doing extreme long distance quantum communication.

The final key rate of 50Hz was much lower than the fibre counterpart. This is exactly the issue that Rarity *et al* addressed in their work two years later in 2001 [14]. Their goal was two-fold. The first obvious one was to increase the key rate as high as possible. The second was to design a setup that would specifically translate well into a satellite-based approach. This implied that their setup had to be light, robust and of high quality. To that end, they invented a timing-synchronizing mechanism that does not require extra optics. Importantly, up until then, all the demonstrations used weak coherent pulses and not true single photon sources. The authors of [4] state "*All experiments to date have been performed using weak light pulses to*

approximate single photon sources". Due to high power dissipation of PCs, they would be ill-suited for satellites. They needed something else for polarisation switching. At Alice end, they used four acousto-optic modulators (AOMs), out of which only one would be active at any given time based on an actively generated random number lookup table. Each AOM is followed by a half-waveplate which sets the polarisation into desired states. This configuration allowed them to operate at a rate of 10 MHz with 0.1 ppp. The four beam paths were then recombined to create a single Alice beam. The light was then sent to a telescope which transmitted the light to Bob. At Bob's end, they used a beamsplitter and a delay line technique to passively switch between the polarisation bases. For timing and synchronizing Alice's and Bob's computers, they reserved some bits purely for timing. In each (approximate) second, in the first 210ms, they sent a set of predetermined bits to uniquely indicate the start time. The next 600ms, they send the random key while the last 200ms is kept silent, to allow the computers to verify a successful transmission. The best key rate achieved was 954 bits/s over a distance of 1.9km at night.

A year later, the same group collaborated with LMU Munich [15] and demonstrated BB84 between two summits in Germany over a distance of 23.4 km. They reported a QBER of 5%. Around the same time, a group in USA demonstrated BB84 over 10 km in daylight [16]. The authors of [14] also published a definitive guide on how to go about implementing a satellite based QKD system in [17]. Here, they explored three possibilities, viz, (i) encoder (E) on ground with detector (D) on satellite, (ii) E on satellite with D on ground and finally (iii) E and D on ground with retroreflector and polarizer on satellite. They calculated the bit rates from all the three combinations with design limitations in mind (weight carried by the satellite, possible orbits and viewing times etc.) and concluded by favoring option (ii), i.e, the use of a down-looking transmitter.

It was in 2003 that the first ever free space communication was achieved that used true single photon sources [18]. Aspelmeyer and team from Austria used spontaneous parametric down conversion (SPDC) to create entangled photons, one of which was sent to Alice and another sent to Bob, separated by 650 m. They achieved a coincidence rate of 15 per second. They used a single counting and timing device precluding the need for synchronization. Since this demonstration [18] was limited to 600 m, it did not have an immediate bearing on satellite communication because the challenge in the latter is 1 km of atmospheric turbulence.

The idea of using entangled source as a viable methodology for free space and satellite-based QKD gained credibility after the group of Peng *et al* (see Fig 2) [19], in the year 2005, reported a successful experiment where they were able to send entangled photon pairs over a noisy free-space channel over a distance of 13 km (larger than the effective atmospheric thickness on earth). The methodology in this work, especially the time synchronization using laser pulses on both the receiver sides, turned out to be a major developmental step inspiring later works. The sender was located on top of a Mountain in Hefei, China and employed a β-Barium Borate (BBO) crystal pumped by an by an Argon ion laser working at 351 nm (peak power of 300mW). Type-II spontaneous parametric down conversion provided polarization-entangled photon pairs (at 702 nm) such that local measurements yielded 10,000 entangled photon pairs per second. These were transmitted using two refracting type telescopes (focal length 2 m) with a beam size of 12 cm to reduce diffraction effects. The two receiving stations Alice and Bob were located at a distance of 7.7 km and 5.3 km, respectively from the source with no direct line of sight between them. Alice and Bob used smaller refracting type telescopes leading into subsequent optics designed to measure photons in a particular basis, and finally into single photon detectors through multi-mode fibres. Since Alice and Bob were not located at equal distances from the sender and air disturbance caused random time differences, the authors came up with an ingenious solution for time synchronization. They divided a 532nm pulsed laser at the source into two parts and sent them to both the receivers travelling the same optical path as entangled photons. During post processing, the time difference between the synchronization pulses from two receivers and the time difference between two entangled photons would be measured thus indicating the corresponding pair photons on each side.

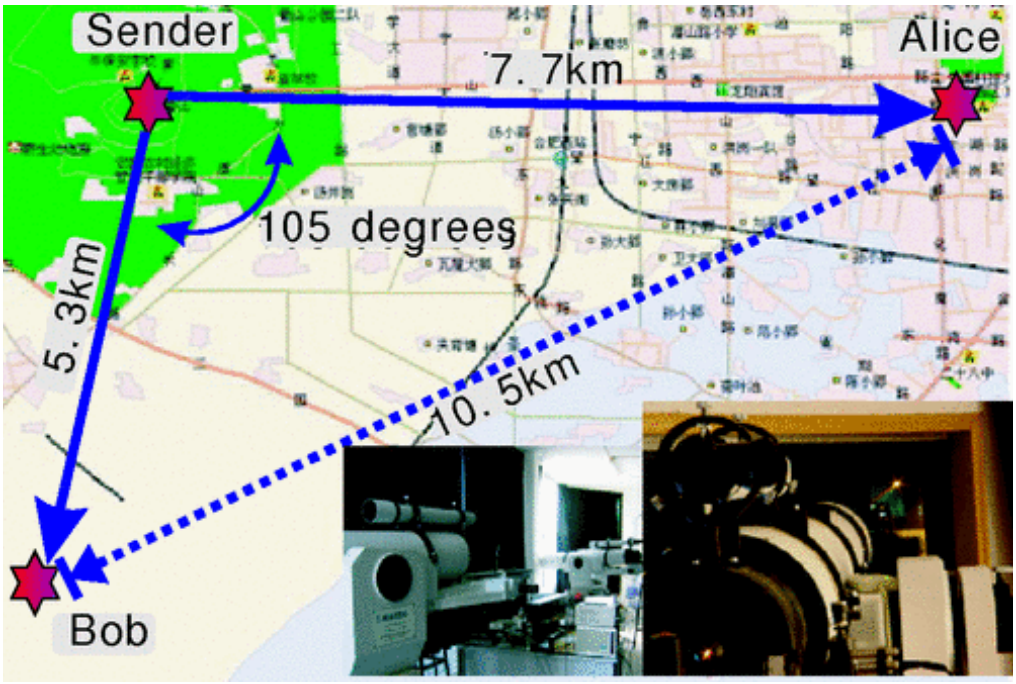

Fig 2. Schematic diagram of locations in the experiment of Peng *et al*. The entangled-photon source is situated at the foot of a high television tower, on the top of Dashu Mountain. Alice is located on the west campus of USTC, and Bob is located at Feixi, a county of Hefei city. Communication was achieved even in the noisy city environment. Reproduced with permission from [19].

With an average dark count and background count of 150 Hz and 400 Hz, respectively, the single photon count rate on Alice and Bob sides were 40 kHz and 18 kHz, respectively. Out of these, 300 Hz of coincident photon count rate was obtained with average visibility for each basis ≈ 91%. With the coincident photons for which the basis did not match, they were used to do Bell's inequality test that yielded $S = 2.45 \pm 0.09$ which is very close to $S = 2\sqrt{2}$ for a completely entangled source. This established the security of the source. After a collection time of 4 minutes, a total of 15,308 coincidences were obtained using which a sifted key of 7956 bits was obtained with QBER = 5.83%. After error correction and privacy amplification, they were able to distil a secure key of length 2435 bits thus obtaining a bit rate of ≈ 10 bits/s. This experiment was a major leap forward towards use of entangled source for long distance experiments.

One of the most successful demonstrations of long distance entangled photon pair distribution, its measurement and its utility in E91 protocol [20] was done by Ursin *et al* [21] in the year 2006 on the Canary Islands of La Palma and Tenerife. In their experiment, they used a 355 nm picosecond- pulsed laser of very high repetition rate of 249 MHz and average power of 150 mW. The laser pumped a β- Barium-Borate(BBO) crystal to undergo a type−II spontaneous parametric down conversion to create polarisation-entangled photon pairs at the wavelength 710nm ± 3nm close to a singlet state of the form, $|\Psi^{(-)}\rangle = 1/\sqrt{2}\,(|H\rangle|V\rangle_B - |V\rangle_A|H\rangle_B)$, where H and V are horizontal and vertical photon states while A and B represent the two distinct spatial modes directed to Alice and Bob, respectively. Locally, the authors were able to register ~ 1 Million Hz counts with coincidence rate of 145,000 Hz and subsequent measurements of visibility in H/V and −45°/45° bases yielded peak to peak variation of 98% and 96%, respectively. While one of the photons was measured locally (Alice), the other was coupled to a single mode fiber and directed to telescope of 150 mm diameter and 400 mm focal length to transmit over a free space link of 144 km to Bob located inside

the On-Ground-Station (OGS) on Tenerife island having a 1m aperture Coudé telescope. For a high-fidelity quantum transmission, maximum link efficiency was necessary and for that a closed loop tracking system using a 532 nm beacon laser was used transmitting from Bob's side to Alice. The opposite direction was used to avoid cross talk between the tracking channel and the quantum channel. This beam was imaged on a CCD which gave a rough idea of the beam attenuation over the distance and actively compensated for beam wander. On Bob's side, the beam diameter was effectively between 3.6 – 20 m and further optics to focus the resultant beam onto avalanche photo-diodes. A total link efficiency of −30 dB was achieved with −8 dB to −12 dB owing to atmospheric loss and −10 dB to −16 dB owing to the beam spreading larger than the receiving aperture. The total quantum efficiency (including all the optics) was computed to about 25%. With all these in hand, the authors were able to record 120 Hz counts and per detector with 50 Hz counts owing to background noise. A time-tagging device with a least count of 156 ps was used to time-tag photons on both sides, which were synchronized with the help of a 10 MHz local oscillator clock and GPS synchronization (time drift of 10−11s over 100 s). On performing the test for violation of CHSH inequality with 7, 058 coincidences registered over an accumulation time of 221 s, they were able to establish an S value = 2.508 ± 0.037, very close to the actual value of S = $2\sqrt{2}$ for a perfectly entangled source thus establishing security of the channel. For the basis for which the angles matched, they were able to register a total of 789 coincidences over 75 s from which they concluded a QBER = 4.8% ± 1%. With subsequent error reconciliation and privacy amplification, they distilled a secure key of 178 bits. Their experiment was a major step ahead for not only long-distance entanglement experiments, but also for long distance single photon experiments.

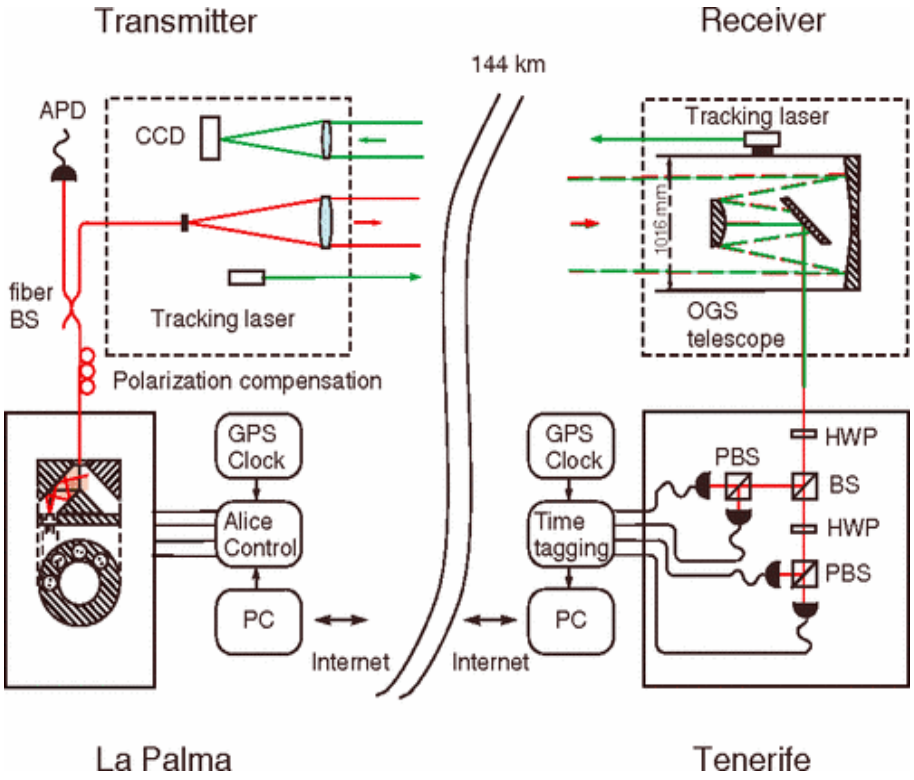

Fig 3. Schematics of the experimental setup on the Canary Islands. BS, beam splitter; PBS, polarizing beam splitter; HWP, half-wave plate; APD, avalanche photo diode. Reproduced with permission from [23].

4 Free space QKD from mobile platforms

QKD from static platforms has been practiced from a research-and-development vantage point. The end goal must be to achieve as much long-distance transmission with as high fidelity as possible between two connecting centers. Although use of fibres is plausible in a connected area such as within a city or two cities, enabling inter- and intra-continental connectivity and connectivity to remote places, the best options are HAPs, or high-altitude platforms such as aerial vehicles or satellites. Satellites have been now accepted as the most efficient means for connecting multiple points on the globe. The satellite is envisaged to transmit quantum keys to various ground stations which can then be used by all of the ground stations for communications. The development of satellite based QKD communication has moved steadily, taking small leaps like testing the fidelity of long-distance propagation in the order of magnitude of low-earth-satellite (LEO) distances, to moving platforms like airplanes and hot air balloons, and finally satellite to ground station connections per se.

The feasibility of long-distance propagation and use of decoy state protocols [22] to counter the vulnerability of weak coherent pulsed sources was first quantitatively analyzed by Schmidtt-Manderbach *et al* in the year 2007 with their experiment on the Canary Islands [23] (see Fig 3). The two ground stations located at La Palma and Tenerife are separated by about 144 km, which can emulate the distance than between LEO satellites and ground stations. The use of decoy state protocol ensures that the communication is immune to photon number splitting attack and the attenuation in the optical path need not be scaled to the link efficiency between two ends. This emphasized higher sifted bit rate without compromising security. They used a two-way tracking system to continuously maintain an optical link power of ≈ -30dB. The report underlines the difficulty of maintaining a consistent optical link because the beam, originating from Alice with a diameter of 1.5 m, is expanded to about 4 – 20 m due to atmospheric effects and diffraction. They used GPS modules for time synchronization and a 10 Mbit/s Ethernet connection to transmit all the classical information needed.

Under good atmospheric conditions, the authors were able to achieve an optical link efficiency of −28 dB, in which the atmospheric losses and beam spreading were attributed losses of −10 dB and −14 dB, respectively. With all the optics and detectors accounted for on Bob's side, they were able to sustained a detection efficiency of ~ 25% and dark count + stray light counts of ~ 1 kHz. With these numbers in hand, they decided on sending 87%, 9% and 4% of signal, decoy and vacuum pulses respectively. Over a 17 minutes' data acquisition, they were able to tag 799, 000 detections, from which the sifted key included 218 kbits yielding a QBER = 6.48%. After revealing only 63 kbits of key for error correction they were able to obtain a secure key of length 12.5 kbit and hence a key rate of 12.8 b/s. This signifies a major step forward because they were able to produce a higher key rate in free space than previously recorded. This laid the pathway for feasibility of satellite-based communication.

Another important work is reported by Sebastian *et al* [24] in the year 2013, where the same kind of experiment (without decoy state protocol) is performed on a moving platform. An airplane moving at a speed of 290 km/h transmitted to a ground station at an effective distance of $\approx$ 20 km. The setup in this experiment was very compact and the active tracking beacon systems onboard the aircraft and the ground station maintained an optical link consistently with a link value of −38 dB. The beacon and QKD signal were transmitted co-linearly but at different wavelengths. Specifically, a 1550 nm laser was employed for tracking. For the signals, 4 identical 850 nm laser diodes of pulse width $\approx$ 1ns and repetition rate of 10 MHz were used. The four beams were recombined with appropriate beam splitters, followed by an attenuator and a photodiode for measuring outgoing photon statistics. This photon statistics setup could be switched in and out of line by a servo. As a proof of principle, the laser polarisations were not randomly selected but sent in

a deterministic fashion as HVDAHVDAHVDA. Due to the small outlet aperture of the aircraft, the smallish beam size at the origin became almost about 3.4 m at a distance of 20 km. The ground station used a large aperture telescope for capturing and directing the light to a Bob setup that was directly mounted to the moving telescope. A dichroic mirror separated the 1550 nm tracking beam from the QKD signal thus enabling the system to work simultaneously. Alice, on the other hand, carried a near field camera along with a Quadrant photo-diode feeding back to coarse and fine adjustment modules. A major challenge faced by the authors was related to tagging the correct polarization encoding on Bob's side. This was because of the relative change of reference frame for the measurement of polarization arising from the moving aircraft. To compensate for this, all birefringence of the optics was measured a-priori, and the compensation was modeled as a function of the angular position of the aircraft that was broadcast to the ground station using a UHF radio link. With all these arrangements in place and a stable QKD signal, a 10 minutes' data acquisition was implemented for Alice operating at a mean of 0.5 photons per pulse and Bob's detectors with dark and ambient light counts of about 1 kHz. The authors were able to tag photons at a rate of 800 Hz yielding a mean sifted key rate of about 145 bits/s and a total QBER of 4.8%. They show in their paper [24] that, if the decoy state arrangements are taken into consideration, then one can obtain a secure key rate of 7.9 bits/s.

The experiments on the airplane gave a lot of insight into the feasibility and requisite technology to successfully maintain an optical link for a quantum channel. Other groups working in this field performed a lot of experiments on mobile platforms before proceeding for satellite based QKD. The two following papers are very notable for research laying the groundwork for both feasibility and technological know-how. The group of Wang *et al* in the year 2013 reported a series of experiments [25] performed in various spots around the Chinese lake Qinhai. These studies were meant to simulate the conditions that Low-Earth-Orbit satellites need to counter in order to establish and maintain a stable quantum channel. Their first experiment was done by mounting a custom-designed transmitter and receiver on a pair of turntables to simulate the changing angular velocities, while the second experiment mounted the transmitter on a hot air balloon to simulate random varying effects and changes of altitude. The final experiment was a very long-distance measurement to test for high loss channel. For both the experiments, they used a decoy state BB84 protocol for standard testing. The transmitter terminal consisted of 4 pulsed laser diodes (wavelength 850nm ± 0.3 nm, pulse width 1 ns) that were spatially filtered with a single mode fiber and led into optics that can generate 4 states of BB84. The diodes were chosen randomly using a high-speed random number sequence generated from random physical noise, and an attenuator set the requisite amount of power for operation. Finally, the beams were mixed with a 532 nm pulsed laser used for timing synchronization (with accuracy of 1ns) as well as for pointing and tracking procedure and was led to a Cassegrain telescope (200mm aperture and 10× magnification) to be transmitted. The receiver consisted of a Cassegrain telescope (300mm aperture with 12× magnification) leading to a dichroic mirror that separated the 532nm for timing and tracking while the signal was led to necessary optics and fed into avalanche photo-diodes using multi-mode fibres. The receiver itself sends a beacon at 671nm to the transmitter to form a closed loop active tracking system. the first experiment had the transmitter in a building near Qinghai Lake and receiver on ~ 40km away at Heimahe both mounted on a turntable imparting complex non-linear change in angular velocity with maximum angular velocity = 21mrads^{-1}. The photo-diodes registered a dark count rate of 800Hz with count rates ~ 5000Hz. With a fine-tuning accuracy of about 5μrad, the channel incurred a total loss of ≈ 40dB, for this experiment they were able to achieve a bit rate of ≈ 150 bits/s with average QBER of 2.8%. The next experiment was done by mounting the transmitter on a tethered hot air balloon on the Qinghai lakeside while the receiver was kept at an island on the lake. With a straight-line distance of ~ 20km and average angular velocity of transmitter = 10.5mrad/s, the transmitter maintaining a pointing accuracy of 5μrad and in a time of 3 − 5s of key acquisition a bit rate of 150 bits/s with QBER = 2.35% was obtained. For the final experiment, two points were chosen that were ~96km apart providing a total channel loss of ~ 50dB. To accommodate such tough changes the

receiver telescope was changed to Cassegrain of aperture 600mm and 5.6× magnification and the detectors were changed to high quantum efficiency detectors (> 45%) with dark counts ~ 100Hz and stray background counts ~ 20Hz. Under these conditions the receiver registered a total of 500Hz counts leading up to a bit rate of 48bits/s and a QBER of 4.04%. All these three experiments were of a paramount knowledge that led to the Chinese to later develop better satellite experiments and increase the know-how of the community in general.

Another important experiment reported by the group of J.-W. Pan [26] in the year 2013, was the actual transmission of weak coherent pulses to space and receiving them with a high signal-to-noise ratio. This experiment was particularly important since it truly illustrated how one can create a consistent receiving system to measure single photon level sources. To do the experiment, the authors used the Challenging Mini-satellite Payload (CHAMP) created in Germany and launched by Russia in the year 2000. The system has a set of multiple 2 cm diameter retroreflectors on each side of the satellite. The Chinese ground station (Shanghai observatory) used a low power (0.4nJ, 702 nm), high repetition rate of 76 MHz and short pulsed (3 ps) laser for quantum data. The alignment and timing beacons consisted a laser ranging system (LRS) that employed a laser beam (532nm) transmitted from a telescope of diameter 20 cm, and the retro-reflected beam was received onto a telescope of diameter 60 cm respectively, positioned at a distance of 30 cm beside the transmitter. The total free space channel was ~800 km long. Under such conditions, they were able to receive pulses at an average rate of 0.85 photons per pulse. The experiment was performed deliberately at night time and when the satellite was in the Earth shadow, for which the average dark counts in the detector was about 100 Hz. After time synchronization, the group achieved a count rate of 570 Hz with an SNR of 16:1.

While the Chinese groups took small but major steps towards their ultimate goal for satellite communication, the Japanese not only started off with things in the sky, but made very estimated research on the factors that can effectively affect fidelity of polarization and time tagging. They also have made an aim to make the process much more cost effective, thus advancing in a step further to global realization.

The Micius mission was launched in the year 2016 by the Chinese space agency to perform dedicated studies on (a) QKD using weak coherent pulses, as well as (b) entanglement experiments and protocols. The satellite is a low earth satellite (LEO) moving in a sun-synchronous orbit at an altitude of about 500 km and has two dedicated payloads. The first one is used to perform decoy state BB84 protocol with an OGS at Xinglong near Beijing, while the other payload has the capability to send entangled photon pairs with high coincidence rate. Towards the first payload, Liao *et al* [27] designed a module to implement Alice of a decoy-state protocol transmitting at a wavelength of 850 nm. The module has eight pulsed laser diodes (peak wavelength = 848.6 nm with pulse width = 0.2 ns and repetition rate of 100 MHz) with temperature controls to maintain stable intensity with variation < 5% and a synchronization system with jitter < 10ps. Polarizing and nonpolarizing optics combine the 8 laser lines along with a 532 nm beacon laser (pulse width = 0.9ns, repetition rate = 10kHz). These beams were incoupled into a 300 mm aperture Cassegrain telescope (with a very narrow beam divergence of ≈ 10 μrad) to be sent down to the receiving station at Xinglong. The receiving station used a 1m aperture Ritchey-Chretien telescope (focal length = 10m) to receive from the satellite. Apart from the Bob module, the telescope has a sensitive camera for the beacon laser (CMOS with 2.3°×2.3° field of view and 40Hz frame rate). It transmits its own beacon at 671 nm (divergence = 0.9 mrad) which is received by the satellite using an onboard camera (CMOS, with field of view = 0.64 mrad×0.64 mrad and frame rate of 2 kHz) to create a precise closed loop feedback-based pointing and tracking system. The beacon lasers were also used for time synchronization with a reported synchronization jitter < 0.5 ns. The initial coarse alignment was done by forecasting the orbital position of the satellite (uncertainty < 200m) obtaining a pointing accuracy of 0.5°, while the closed-loop feedback system increased the precision to ≈ 1.2 μrad. At a maximum distance of about 1200 km, the beam expansion is ≈ 12 m accounting for almost 22 dB of loss due to diffraction. The atmospheric absorption and turbulence was attributed 3 – 8 dB loss and the pointing error accounted for 3dB loss. For executing the BB84 decoy protocol, the authors chose the signal,

decoy and vacuum mean photon numbers as 0.1,0.8 and 0, respectively with probabilities 50%, 25% and 25%. On the ground station, the Bob module used detectors of efficiency 50% (dark counts < 25Hz, time jitter ≈ 350ps). Along with the optics, the overall optical efficiency was around 16%. The incoming photons were time tagged in windows of 2 ns and a radio frequency channel (bandwidth uplink: 1M bit/s, downlink: 4M bit/s) was used for classical communication. For a pass time of ≈ 5 minutes (exactly 273s), a total of 1,671,072 sifted bits were registered. For a distance of closest approach (≈ 650 km) the bit rate was 12 kbit/s, while for the farthest distance of 1200 km, it was about 1 kbit/s. During this time, the quantum bit error rate varied between 1 − 3% with average = 1.1%. Over 23 days of experimentation, the authors could achieve the best sifted bit rate of 40 kbits/s at a minimum altitude of 530 km. These results motivate a push to establish a multi-satellite link making quantum communication commercially viable.

Onboard the same satellite is the second payload to study QKD using entangled photon pairs. Yin *et al* in 2019 [28], used the payload as a source of entangled photons. The two beams carrying the pairs of entangled photons were received at two ground stations located at Delingha and Nanshan, separated by ≈ 1120 km. Specifically, the optical source is a periodically poled Potassium titanyl phosphate ($KTiOPO_4$) crystal placed inside a Sagnac interferometer and pumped in both clockwise and anti-clockwise directions by a continuous-wave laser of central wavelength = 405nm and line-width of 160 MHz. This generates wavelength-degenerate down-converted photon pairs at 810 nm which are polarization entangled having a state close to = $1/\sqrt{2}\left(|H\rangle_A |V\rangle_B - |V\rangle_A |H\rangle_B\right)$, Here, A and B are the two spatial directions sent to Alice and Bob, while V and H represent vertical and horizontal polarization states. The photons are guided by two single mode fibres to two independent transmitters (beam divergence ≈ 10μrad). With a pump power of 30 mW, the payload can generate upto 5.9×10^6 entangled photon pairs per second. In this configuration, both the Alice and Bob are receivers. Each used a 1.2 m aperture telescope that led the light into optics that randomly choose one among three bases of measurement. The photons were collected using 105 μm core multi-mode fibres and fed into single photon detectors having efficiency better than 53% (dark count rate = 100Hz). A motorized half wave plate compensated for polarization shifts due to relative motion of satellite with respect to the ground station. The incoming photons were both spatially and temporally filtered for higher fidelity of measurement. Similar to the decoy-state experiment, the ground stations and the satellite used a 532nm beacon laser-based tracking system as well as time synchronization (repetition rate = 10 kHz) allowing pointing accuracy of 2 μrad and 0.4 μrad for Delingha and Nanshan, respectively. A GPS pulse was also used to synchronize between the satellite and the two ground stations. The entangled photon pairs were time gated in a small window of 2.5 ns with accuracy of 0.77 ns. For an overall experimentation time of 285 s, the channel loss in each of the receivers was estimated to be between 56 – 71 dB. The survival of the entanglement was endorsed by a CHSH type Bell's inequality test using 1,021 trials made over effective time of 226 s, during which they were able to establish the value of S = 2.56 ± 0.07, very close to the theoretical value of $2\sqrt{2}$. To implement QKD, the authors chose the BBM92 protocol for which they were able to attain a sifted key rate of 1.1 Hz and the best-case average quantum bit error rate of ≈ 4.5%. The authors describe a multitude of precautions and steps taken to counter any type of suitable attack that can be mounted on the system to breach security. In conclusion, they were able to distill a 372-bit secret key among the two stations suggesting a successful entanglement based QKD protocol being performed with a bit rate of 0.12 bits/s.

The Indian Scenario

In the Indian scenario of these efforts, there are three reports hitherto as enlisted below.

The group of Prof Urbasi Sinha, incharge of the Quantum Information and Computing Laboratory at the Raman Research Institute, Bangalore, implemented a BBM92 protocol using polarization-entangled photon pairs. Alice (1) and Bob (2) both measure the stream of incoming photons: say, horizontally polarized

i.e. H and vertically polarized i.e. V (or say, V and H). The photons entering the Alice's and Bob's setups are segregated randomly, for measurement along the two rectilinear or diagonal projection bases, with a 50:50 probabilities by a beam-splitter. The schematic of the experimental setup is presented in Fig 4. The free-space (atmospheric) channel length from sender (source/Alice's setup) to the receiver (Bob's setup) is ≈50 meters. Each of these basis projections can again lead to either of the two outcomes (i.e., detection of the photon along the transmitted arm: horizontally (H) or diagonally (D/+) polarized photon, or along the reflected arm: vertically (V) or anti-diagonally (A) polarized photon of the polarizing beam-splitter). Hence, one obtains an overall eight coincidence detections between the Alice's and Bob's detector clicks. Out of them four (i.e., A1-B2, A2-B1, A3-B4, and A4-B3) form the desirable set (signal: HV/VH, DA/AD) and the other four (i.e., A1-B1, A2-B2, A3-B3, and A4-B4) form the undesirable set (noise: HH/VV, DD/AA). We assess the number of coincidences in these sets by analyzing the signal-to-noise ratios (SNRs), through the consideration of suitable window spans around the peak maxima. The signal and the noise coincidence values thus obtained within these window regions are then used to compute the raw key rate, the quantum-bit-error-rate (QBER) and the key symmetry of our protocol implementation. The first measurements carried out in February 2021 achieved a reasonably good key rate along with an information-theoretically secure QBER. This is a part of India's first project on satellite based quantum communications "Quantum Experiments with Satellite Technology" which is a collaboration between the Quantum Information and Computing lab at RRI and the Indian Space Research Organization.

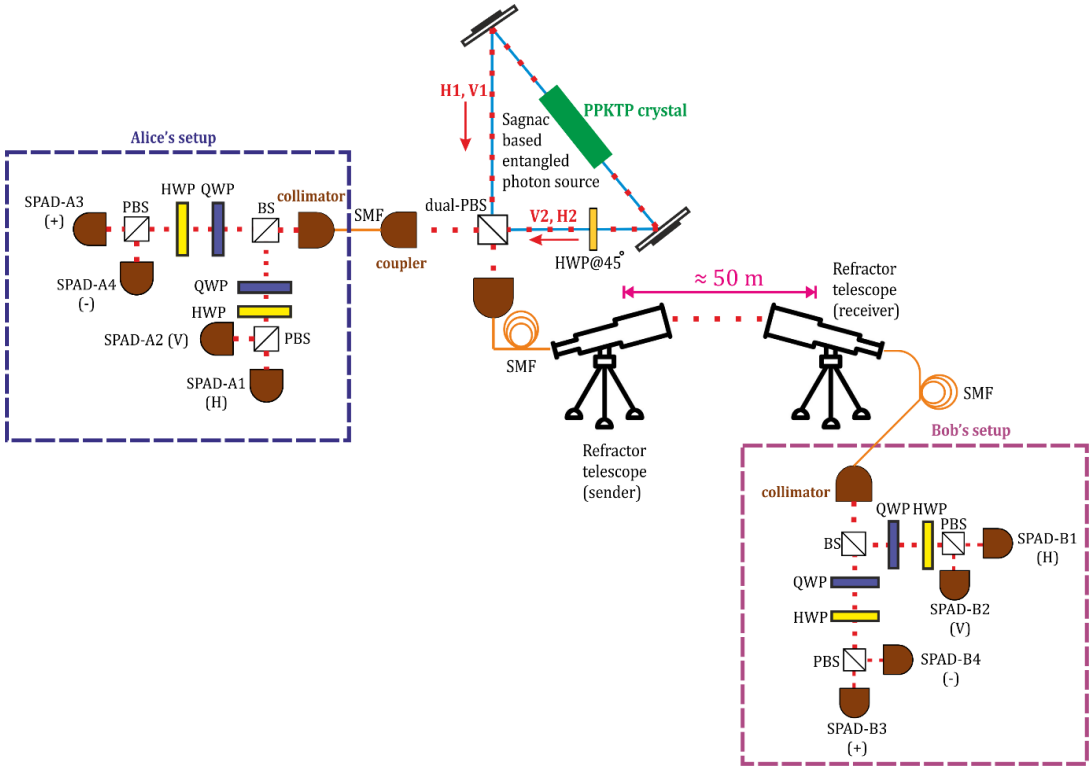

Fig 4. Abridged schematic of the experimental setup at RRI. The abbreviations PPKTP, SMF, HWP, QWP, PBS, BS, SPAD, and dual-PBS stand for periodically-poled potassium-titanyl-phosphate, single-mode fibre, half-wave plate, quarter-wave plate, polarizing beam splitter, beam splitter with 50/50 splitting ratio, single photon avalanche detector, and dual-wavelength polarizing beam splitter, respectively. Picture courtesy of QuIC lab, RRI.

An actual drone-shot of the venue for the experiment can be found below:

Another demonstration of free-space QKD was reported by the group pf Prof R P Singh, Physical Research Laboratory, Ahmedabad. Doing QKD in the dusty atmosphere of Ahmedabad has its own limitations such as key rate. The group has built an inhouse QKD transmitter system capable of generating four random pulses with rate of 5 MHz. The laser pulse width is ~1ns with good spatial mode overlap (see Fig 5). They fed the random signal into the laser diode through FPGA based on LFSR technique. At Bob end, there was collection optics with polarization analysis optics whose output was connected to photon counting detectors. The quantum transmission happened over a free space non-LOS channel of 200 meters which is widely used in terrestrial communication and also in space communication (see Fig 6). The sift key rate of the demonstrated system was 200 kbps and after error correction and privacy amplification this went down to 150 Kbps with an average QBER of 4%. The group further performed BBM92 protocol (entanglement based BB84 protocol) in the same channel with the inhouse developed source of entangled photons at 810 nm. The sift key rate for BBM92 was observed to be 5Kbps with 4% QBER.

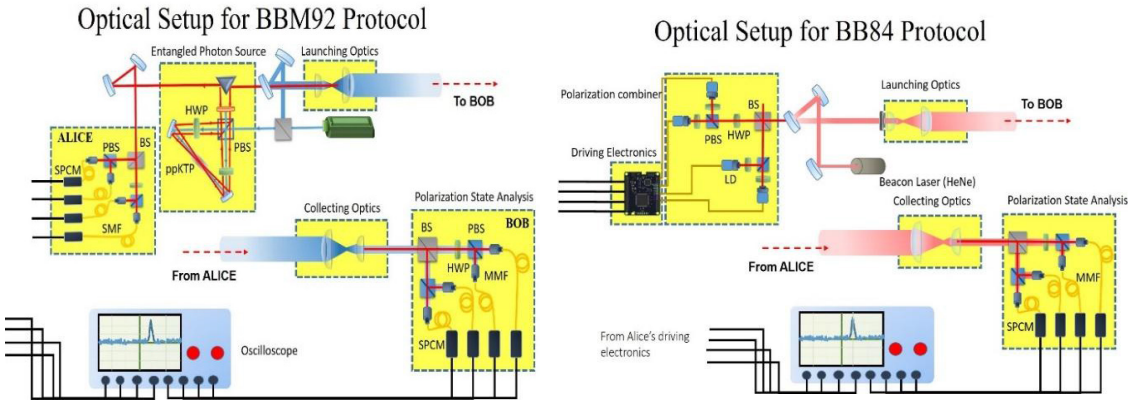

Fig 5. Optical Setup of the BBM92 and BB84 protocol in PRL, Ahmedabad. BS: Beam Splitter, PBS: Polarizing Beam Splitter, SPCM: Single Photon Counting Module, HWP: Half Wave Plate, LD: Laser Diode, ppKTP: Periodically polled Potassium Titanyl Phosphate, SMF: Single Mode Fiber, MMF: Multi Mode Fiber. Figure courtesy of PRL, Ahmedabad.

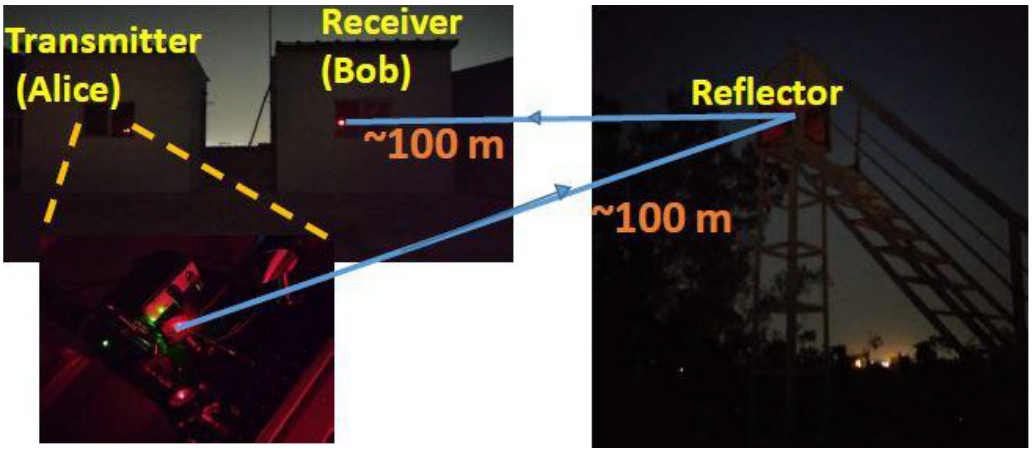

Fig 6. Field implementation of QKD using terrace of two buildings in Thaltej campus of PRL.

The third demonstration in India was reported by the Space Applications Centre (SAC) of ISRO, Ahmedabad [29,30]. In this work, the group reported the design and development of a fully automated inter-building QKD framework for generation and distribution of cryptographic keys based on the BB84 protocol (see Fig 7). A weak coherent pulse was used as the source. The quantum communication link was established between two buildings separated by 300 meter of atmospheric channel at the SAC, Ahmedabad. A novel synchronization technique enabled with indigenous NavIC (IRNSS) constellation was developed and implemented. The group achieved the generation of secure key rate as high as 300 Kbps with QBER< 3% for mean photon number per pulse (μ) of ~0.15. Further, the group reported a novel quantum secured end-to-end encrypted video calling app (QuViC) integrated with their communication demonstration.

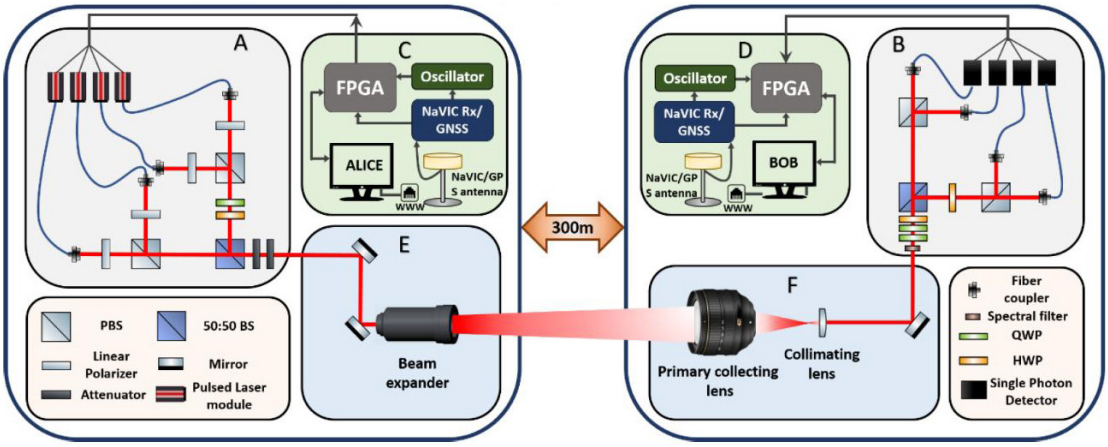

Fig 7. Inter-building QKD framework of SAC, Ahmedabad, with link over 300m (A) Quantum transmitter module (B) Quantum receiver module (C, D) FPGA modules connected to PLMs (Tx) and SPDs (Rx) respectively, NavIC/GNSS receiver system for synchronization (E, F) assemblies for incoming and outgoing beam shaping. Picture courtesy of SAC, Ahmedabad.

Pulsed laser modules (PLM) along with BB84 encoding optics module were used to transmit polarization-encoded photons in one of the four polarization states. Neutral density filters maintained the mean photon number (MPN) close to 0.15. The beam is then directed towards the front end optics module consisting of folding mirrors and a gimbal-mounted beam expander. The PLMs are randomly triggered using

FPGA system. The quantum receiver consists of front end optics module followed by BB84 decoding optics module and four single photon detectors. A visible beacon source, with 638nm wavelength, is used for coarse alignment between Alice and Bob terminals, with fine alignment achieved by gimbal rotary mounts. The NavIC enabled synchronization mechanism is used for time synchronizing both, Alice and Bob terminals, located 300m apart**.**

These experiments mark the ability of Indian scientific community of developing modern quantum applications in house and at the par with international standards which can be used for commercial purposes. We can expect many more sophisticated reports on similar experiments in the times to come.

References

1. Wootters W, Zurek W, A single quantum cannot be cloned, *Nature*, 299(1982)802–803.
2. Wiesner S, Conjugate coding, SIGACT News 15, 1 (Winter-Spring 1983), 78–88, DOI: https://doi org/10.1145/1008908.1008920.
3. Bennett C H, Bessette F, Brassard G, Salvail L, Smolin J, Experimental quantum cryptography, *J Cryptology*, 5(1992)3–28.
4. Diffie W, Hellman M, New directions in cryptography, IEEE Trans Inf Theory, 22(1976) 644–654,
5. Rivest R L, Shamir A, Adleman L, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM 21, 2 (Feb. 1978), 120–126,1978, doi. https://doi.org/10.1145/359340.359342.
6. Bennett C H, Brassard G, Quantum cryptography: Public key distribution and coin tossing, In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175, page 8. New York, 1984. http://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf
7. Marand C, Townsend P D, Quantum key distribution over distances as long as 30 km, *Opt Lett*, 20(1995)1695–1697.
8. Jacobs B C, Franson J D, Quantum cryptography in free space, *Opt Lett*, 21(1996)1854–1856.
9. Jacobs B C, Franson J D, Operational system for quantum cryptography, *Electron Lett*, 31(1995)232–234.
10. Czegledi C, Karlsson M, Agrell E, Johannisson P, Polarization Drift Channel Model for Coherent Fibre-Optic Systems, *Sci Rep*, 6, 21217 (2016); doi.org/10.1038/srep21217.
11. Butller W T, Hughes R J, Kwiat P G, Luther G G, Morgan G L, Nordholt J E, Peterson C G, Simmons C M, Free-space quantum-key distribution, *Phys Rev A*, 57(1998)2379; doi.org/10.1103/PhysRevA.57.2379.
12. Bennett C H, Quantum cryptography using any two nonorthogonal states, *Phys Rev Lett*, 68(1992)3121;doi. org/10.1103/PhysRevLett.68.3121.
13. Buttler WT, Hughes R J, Kwiat P G, Lamoreaux S K, Luther G G, Morgan G L, Nordholt J E, Peterson C G, Simmons C M, Practical free-space quantum key distribution over 1 km, *Phys Rev Lett*, 81(1998)3283; doi. org/10.1103/PhysRevLett.81.3283.
14. Rarity J G, Tapster P R, Gorman P M, Secure free-space key exchange to 1.9km and beyond, *J Mod Opt*, 48(2001)1887–1901.
15. Kurtsiefer C, Zarda P, Halder, Weinfurter H, Gorman P M, Tapster P R, Rarity J G, A step towards global key distribution, *Nature*, 419(2002)450; doi.org/10.1038/419450a.
16. Hughes J H, Jane E Nordholt1, Derek Derkacs1 and Charles G Peterson., Practical free-space quantum key distribution over 10 km in daylight and at night, *New J Phys*, 4(2002)43; doi.org/10.1088/1367-2630/4/1/343.
17. Rarity G, P R Tapster, Gorman P M, Knight P, Ground to satellite secure key exchange using quantum cryptography, *New J Phys*, 4(2002)82; doi.org/10.1088/1367-2630/4/1/382.
18. Aspelmeyer M, Böhm H R, Gyatso T, Jennewein T, Kaltenbaek R, Lindentha M, Molina-Terriza G, Poppe A, Resch K, Taraba M, Ursin R, Walther P, Zeilinger A, Long-distance free-space distribution of quantum entanglement, *Science.* 301(2003)621–623.
19. Peng C Z, Yang T, Bao X-H, Zhang J, Jin X-M, Feng F-Y, Yang B, Yang J, Yin J, Zhang Q, Li N, Tian B-L, Pan J-W, Experimental free-space distribution of entangled photon pairs over 13 km: Towards satellite-based global quantum communication, *Phys Rev Lett*, 94(2005)150501; doi.org/10.1103/PhysRevLett.94.150501.

20. Ekert A, Quantum cryptography based on Bell's theorem, *Phys Rev Lett*, 67(1991)661, doi.org/10.1103/PhysRevLett.67.661.
21. Ursin R, Tiefenbacher F, Schmitt-Manderbach T, Weier H, Scheidl T, Lindenthal M, Blauensteiner B, Jennewein T, Perdigues J, Trojek P, Ömer B, Fürst M, Meyenburg M, Rarity J, Sodnik Z, Barbieri C, Weinfurter H, Zeilinger A, Entanglement-based quantum communication over 144 km, *Nature Phys*, 3(2007)481–486.
22. Lo H K, Ma X, Chen K, Decoy state quantum key distribution, *Phys Rev Lett*, 94(2005)230504; doi.org/10.1103/PhysRevLett.94.230504.
23. Schmitt- Manderbach T, Weier H, Fürst M, Ursin R, Tiefenbacher F, Scheidl T, Perdigues J, Sodnik Z, Kurtsiefer C, Rarity J G, Zeilinger A, Weinfurter H, Experimental demonstration of free-space decoy-state quantum key distribution over 144km, Phys Rev Lett, 98(2007) 010504; doi. doi.org/10.1103/PhysRevLett.98.010504.
24. Nauerth S, Moll F, Rau M, Fuchs C, Horwath J, Horwath J, Frick S, Weinfurter H, Air-to-ground quantum communication, *Nat Photon*, 7(2013)382–386.
25. Wang J Y, Yang B, Liao S K, Zhang L, Shen Q, Hu X F, Wu J-C, Yang S-J, Jiang H, Tang Y-L, Zhong B, Liang H, Liu W-Y, Hu Y-H, Huang Y-M, Qi B, Ren J-G, Pan G-S, Yin J, Jia J-J, Chen Y-A, Chen K, Peng C-Z, Pan J-W, Direct and full-scale experimental verifications towards ground–satellite quantum key distribution, *Nat Photon*, 7(2013)387–393.
26. Yin J, Cao Y, Liu S B, Pan G S, Wang J H, Yang T, Zhang Z-P, Yang F-M, Chen Y A, Peng C-Z, Pan J-W , Experimental quasi-single-photon transmission from satellite to earth, *Opt Express*, 21(2013)20032–20040.
27. Liao S K, Cai W Q, Liu W Y, Zhang L, Li Y, Ren J G, Yin J, Shen Q, Cao Y, Li Z-P, Li F-Z, Chen X-W, Li-Hua Sun L-H, Jia J-J, Wu J-C, Jiang X-J, Wang J-F, Huang Y-M, Wang Q, Zhou Y-L, Deng L, Xi T, Ma L, Hu T, Zhang Q, Chen Y-A, Liu N-L, Wang X-B, Zhu Z-C, Lu C-Y, Shu R, Peng C-Z, Wang J-Y, Pan J-W, Satellite-to-ground quantum key distribution, *Nature*, 549(2017)43–47.
28. Yin J, Li Y H, Liao S K, Yang M, Cao Y, Zhang L, Ren J G, Cai W-Q, Liu W-Y, Li S-L, Shu R, Huang Y-M, Deng L, Li L, Zhang Q, Liu N-L, Chen Y-A, Lu C-Y, Wang X-B, Xu F, Wang J-Y, Peng C-Z, Ekert A K & Pan J-W, Entanglement-based secure quantum cryptography over 1,120 kilometers. *Nature*, 582(2020)501–505.
29. Biswas A, Banerji A, Chandravanshi P, Kumar R, Singh R, Experimental Side Channel Analysis of BB84 QKD Source, *IEEE J Quantum Electron*, 57(2021)1-7.
30. Jain A, Desai N M, Das T P, Meetai N R, Umamaheshwaran R, Development of key technologies for ISRO's Satellite Based Quantum Communication Program, in Proc. 72nd International Astronautical Congress (IAC), Dubai, UAE, 25-29 October 2021.

[*Received*: 01.05.2022; *revised recd*: 27.06.2022; *accepted*: 29.06.2022]

Prof Sushil Mujumdar is the Principal Investigator of the Nano-optics and Mesoscopic Optics Laboratory in TIFR, Mumbai. His expertise covers experimental and computational aspects of random lasing, light localization, near-field microscopy and quantum optics. He has been awarded merits such as the Ramanujan Fellowship, the National Academy of Sciences Scopus Young Scientist Award, the Swarnajayanti Fellowship, and the P K Iyengar Award for Excellence in Experimental Physics.

Vikas is a graduate student at the Nano-Optics and Mesoscopic Optics Laboratory in TIFR Mumbai. He is currently working on long distance quantum cryptography using photons and their entanglement. This involves working with various instruments that need constant debugging so he likes to call himself a quantum mechanic.

Rounak Chatterjee is a Research Scholar in the Tata Institute of Fundamental Research (TIFR), Mumbai, India. He is currently working in the field of long distance free space Quantum Communication. His primary research interests are in the field of single photon and entanglement photon sources compatible with applications in quantum cryptography and other quantum technologies in general.