Demonstrating BB84 Quantum Key Distribution in the Physical Layer of an Optical Fiber Based System

Márton Czermann[1,4], Péter Trócsányi[1], Zsolt Kis[2], Benedek Kovács[3] and László Bacsárdi[1] *Member, IEEE*

***Abstract*—Nowadays, widely spread encryption methods (e.g., RSA) and protocols enabling digital signatures (e.g., DSA, ECDSA) are an integral part of our life. Although recently developed quantum computers have low processing capacity, huge dimensions and lack of interoperability, we must underline their practical significance – applying Peter Shor's quantum algorithm (which makes it possible to factorize integers in polynomial time) public key cryptography is set to become breakable. As an answer, symmetric key cryptography proves to be secure against quantum based attacks and with it quantum key distribution (QKD) is going through vast development and growing to be a hot topic in data security. This is due to such methods securely generating symmetric keys by protocols relying on laws of quantum physics.**

In this paper we introduce a fiber based QKD system that is being built in Hungary in a collaboration between Budapest University of Technology and Economics (BME), Wigner Research Centre for Physics and Ericsson Hungary. We demonstrate the first successful quantum key distribution over physical layer in accordance with the truth table of BB84 protocol in the country. We apply light pulses at 1550 nm wavelength, reducing their power to less than one photon per pulse level. We create two phases of operation including an initialization phase in which software and hardware solutions are proposed for synchronizing the units of the two communicating parties. We introduce a data processing and a timing mechanism and elaborate on the results of the demonstration. We also inspect the possibilities of efficiency enhancement and give an outlook on further development directions.

***Index Terms*—BB84; quantum key distribution; symmetric key encryption; phase encoding; fiber optic system; adaptive filtering; synchronization**

I. Introduction

WE need encryption to send data securely. Today's encryption solutions can be divided into two major groups: symmetric and asymmetric key encryption. However, quantum computers pose serious threats on asymmetric key encryption due to Shor's algorithm, which is a polynomial-time quantum computer algorithm for integer factorization. But there are symmetry-key algorithms like One-Time-Pad (OTP) which provides mathematically proven security. The critical question is how the communicating parties can share the key used for symmetric encryption since they need to use the same key for both encryption and decryption [1], [2].

Quantum key distribution (QKD) [3], [4] offers an efficient and secure solution for this key exchange and its security is based on the laws of physics. Since unknown quantum bits cannot be copied due to the No Cloning Theorem (NCT) [5], an attacker does not have the opportunity to copy information which is being shared between Alice and Bob. This means that a passive attack is not possible against QKD protocols, the eavesdropper must actively intervene. However, QKD protocols work in such a way that the active presence of an eavesdropper disrupts communication, bringing noise into the quantum channel which can be detected by the communication parties. So the presence of an attacker would be revealed.

At Budapest University of Technology and Economics, we've already researched QKD both in theory [6] and practice [7] in the recent years as well as researched different quantum random number generator setups [8]. In this paper, we present the demonstration results of the first Hungarian QKD system which uses BB84 protocol for key exchange. The article is organized as follows. Section II gives a short overview of different QKD initiatives. Section III introduces our system, while Section IV details our procedures used for initializing signal levels and timing. The operation of the system is described in Section V, our demonstration results in Section VI.

II. QKD in the 21st century

Although the majority of quantum links and networks established during the past two decades have been fiber-based, there have been several examples of free-space approaches, too. Since the technology of optical telecommunications is widespread, applying attributes of light as quantum carrier is a favorable solution. Having the infrastructure already deployed facilitated the development of terrestrial fiber-based quantum links and networks implementing various QKD protocols – such as the 3.6 Tbps optical backbone network deployed by China United Telecom in which a quantum communication (QC) link was integrated with classical ones [9].

The prospect of scalability, however, is challenging for this kind of key distribution due to the attenuation of fibers, which limits the transmission range of photons to a few hundred

[1] Department of Networked Systems and Services, Budapest University of Technology and Economics, Magyar tudósok krt 2., Budapest 1117, Hungary. (e-mail: czermann@mcl.hu, p.trocsanyi@edu.bme.hu, bacsardi@hit.bme.hu)

[2] Wigner Research Centre for Physics, Budapest, Hungary (e-mail: kis.zsolt@wigner.hu)

[3] Ericsson Hungary, Budapest, Hungary (e-mail: benedek.kovacs@ericsson.com)

[4] corresponding author

This research was supported by the National Research Development and Innovation Office of Hungary within the Quantum Technology National Excellence Program (Project No. 2017-1.2.1-NKP-2017-00001) and by the Ministry of Innovation and Technology and the National Research, Development and Innovation Office within the Quantum Information National Laboratory of Hungary.

DOI: 10.36244/ICJ.2021.3.5

kilometers even applying the best quality optical fibers. Other terrestrial solutions are based on trusted nodes that must either be physically secured in order to be considered as a segment of a secure key distribution method or apply quantum repeaters. The latter option requires the complex technology of quantum memories in order to find a workaround for the NCT and extend the distances of QKD. In spite of scepticism around the practicability of this late technology, various architectures based on space-borne quantum memories have already been proposed [10]. Recent study on quantum technologies in space in general has also been carried out, summarizing the state of the art of this area [11]. Satellite-based quantum communication and technologies [12], [13], [14], [15] provide the means of bridging terrestrial fiber-based metropolitan networks and free-space links thus offering a scalable solution for physically secure communication and indicate directions towards a future global quantum internet [16], [17], [18].

Classifying the QKD systems by the protocols implemented by them, there are two fundamental protocol families that we can exemplify: prepare and measure and entanglement based. Both of them provide security for key distribution grounded in the laws of quantum mechanics. While former type of protocols operate with initial keys and exploit NCT, the latter ones are built on a quantum phenomenon: entanglement [5]. Although the vast majority of prepare and measure protocols is based on the widely-known BB84 protocol [3], several links have been established exploiting entanglement in the past two decades [19], [20], [21], [22], [23], [24]. Since we performed the demonstration on a prepare and measure system we would like to introduce some milestones from this family to make the navigation on the map of QC easier.

The first operating fiber quantum network was built in 2003 in the USA as a project of the Defense Advanced Research Projects Agency (DARPA) [25]. QKD was put into practice via coherent laser pulses propagating between 4 nodes to which a further free-space link with 2 extra nodes was connected later. In 2004 Austria launched a 4-year project called Secure Communication based on Quantum Cryptography (SECOQC), which facilitated the establishment of a quantum network with 6 nodes investigating the operation of 8 different protocols implemented between them [26]. SECOQC also proposed the idea of multi-layer QKD networks, such as SwissQuantum [27], which implements a structure similar to the one presented in Vienna. Three layers are applied for communication: a quantum layer, a key management layer and an application layer. During a 21 month operation between 2009 and 2011 low quantum bit error rate (QBER) was stable generating 300-900 thousand symmetric secret keys on a daily basis. In 2010 Tokyo also established their own project with the aim of observing the properties of a metropolitan quantum key distribution network with trusted nodes [28].

Finally, we can not enlarge upon QC without mentioning the achievements of China. In 2016 a satellite called Micius was launched, which connected 3 ground stations (Graz in Austria, Xinlong and Nanshan in China) as a trusted relay in an intercontinental QKD setup, generating symmetric keys at a distance of 7200 km between the two countries [29]. By 2018, a 2000 km long quantum key distribution link between Beijing and Shanghai was established connecting 32 nodes involving 4 metropolitan quantum networks. Finally, a paper in January of this year introduced an integrated space-to-ground quantum communication network over 4,600 kilometres based on the previously mentioned achievements [30].

Besides experimental quantum links and networks there are several concepts and objectives for QKD applications in real-life scenarios as well [31], [32], [33], [34], [35]. The accelerating tendency in the developement of QC (and technologies) has ushered in the era of the so called ’second quantum revolution.’ The expectations of this era include on behalf of the European Union to drive their own technological improvements in a global direction. Therefore the European Commission established an initiative called EuroQCI with the promise of the deployment of a Europe-wide QC network [36].

III. The BB84 system with phase coding

Our project is based on an architecture proposed in a 2002 publication [37]. The fiber-optic QKD link implements a flavor of the BB84 protocol that operates with very weak, phase modulated light pulses as quantum carrier between Alice and Bob. The light source and single photon avalanche detectors (SPADs) are both on Bob’s side and part of a large-scale interferometer in which the emitted pulses propagate from Bob to Alice and back. After they return the mean photon number is less than one per pulse. The phase shifts on the pulses are assigned to classical 0 / 1 values in initial keys randomly generated by Alice and Bob and after the interference classical 0 / 1 values are assigned to detection ticks of SPADs on the two output channels of the interference as symmetric raw key bits. The design of the system and development on it had been carried out in the spirit of plug & play operability: initialization and system operation should become automated and not need user monitoring.

The physical realization can be subdivided into a quantum transmitter and a receiver side, respectively A and B, for Alice’s and Bob’s units, in the schematic seen in Figure 1. The photon pulses that are emitted at 1550 nm wavelength and 5 MHz repetition rate travel back and forth between Bob and Alice. Bob sends altogether 480 pulses of 20 ns width called one frame. After they are emitted, the pulses go through an ATT and an inline polarizer (ILP) before they arrive to the CIR. Since the proper pulsed operation of our laser requires the generation of high intensity pulses, we inserted an attenuator right after the source in order to protect our SPADs from damage caused by crosstalk between CIR ports. Furthermore, the generation of short pulses requires a small level of bias current in the dark period of laser diode, which in turn results in some under threshold faint glowing of the laser diode, which yields quite high level of ambient photons. This emission increases the noise background of the photon counters. The attenuator suppresses efficiently this background. The ILP enhances the degree of polarization of the laser light. For the protection of our source the CIR proves to be a suitable solution as returning pulses are directed away from it (into SPAD1).

A 50 / 50 beam splitter (BS) creates the two separate arms of the interferometer: leaving the circulator the pulses get split

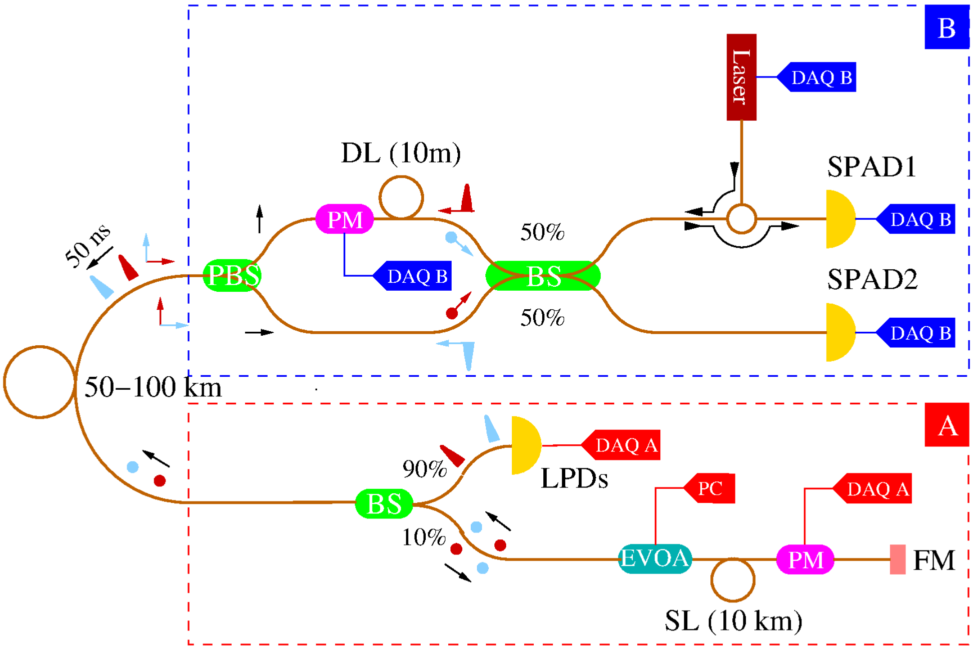


Fig. 1. Schematic of the QKD system as separate units of communicating parties.
Bob's unit (B): high power pulses are routed by a circulator (CIR) to the input port of a balanced beam splitter (BS) creating a reference (blue) and signal (red) pulse, marked with humps, and a polarization beam splitter (PBS) joins the signal paths of these. Alices's unit (A): first, the pulses are split by a 90 / 10 BS into a high power trigger signal for a linear photodetector (LPD) and low power carrier marked with dots, then the latter propagates through an attenuator (ATT), a storage line (SL) and a lithium niobate electro-optic phase modulator (PM) and back upon reflection on a Faraday Mirror (FM), and meanwhile the carrier is attenuated to the quantum level as it leaves Alice. As the carrier pulses return to Bob, their polarizations are switched, denoted by perpendicular arrows of the respective colors. The polarization switching lets swap paths propagating back and forth between Alice and Bob. According to their interference signal they produce ticks in SPAD1 or SPAD2 with given probabilities. Here data acquisition (DAQ) marks any point where a higher layer interface is needed.

into pairs here. Half of each pair gets a 50 ns time delay passing through a 10 m long delay line (DL) that is followed by Bob's phase modulator (PMb) which is off at this stage PMb. The two arms are coupled into a PBS that results in the delayed half sustaining a polarization orthogonal to the leading half. From this point on the 480 pairs follow each other to Alice's unit with this 50 ns time delay between the rising edges of the halves.

Traveling through a 50-100 km long optical fiber they arrive to Alice's side. During this experimental phase of the project we inserted only a 50 m long fiber for simplicity. Here, a 90 / 10 BS deflects the majority of the power into a linear photodetector (LPD) which has a central role in the timing mechanism for Alice's modulation as a monitor point for the position of incoming frames. The leading half of each pulse pair provides us the reference used later for the interference (when arriving back to Bob) and we modulate every trailing one . Alice performs encoding by phase shifting in either $(0-\pi)$ or $(\pi/2-3\pi/2)$ basis based on two bit random sequences as initial keys. The next component for the pulses is an electronic variable optical attenuator (EVOA), which we can control by software to reduce the pulse energy level to around one-photon after they get reflected from a Faraday Mirror (FM) and start their way back to Bob.

One last component on the transmitter side is a 10 km long storage line (SL) between the EVOA and Alice's phase modulator (PMa). This fiber segment is long enough to 'store' all of the 480 pulse pairs. If we think of a scenario without an Alice-side SL, the interaction of the forward and backward propagating pulse trains takes place between Alice and Bob in the multiple km long connection fiber. Regarding optical power, forward travelling pulses have high intensity (to be detectable with the sensitivity of the LPDs) while backward only one-photon level ones propagate. The Rayleigh scattering from the higher level pulses adds false detection to the backward travelling pulse train and higher noise level at the receiver. Inserting the SL prevents this scenario from occurring.

Returning to Bob's side the pairs are routed to opposite ports of the PBS than when they have left due to the FM swapping their polarization. This way the delayed halves take the shorter path, while the reference halves choose the path with the DL and PMb. Here, Bob modulates the phase randomly choosing from the basis $(0-\pi)$ based on his initial binary key. As all of the fibers are polarization maintaining on Bob's side and the optical path to Alice and back is identical for corresponding pulses, they arrive simultaneously to the balanced BS with identical polarization. If both parties choose the same basis, the pulse arrives to SPAD2 when the pulse pairs are in phase and to SPAD1 if one of them has a π phase shift. The interference is not deterministic in the case of different basis choices so then we will discard our classical bits assigned to the detector signal. Finally, Alice and Bob performs the basis reconciliation over Ethernet to get their symmetric sifted key.

We have always been taking plug & play principles into consideration as well as compact construction and economic but efficient operation. Still, until reaching the phase of a possible deployment the project serves scientific and research interests. Alice and Bob are connected to a power supply for the laser, mixed signal digital oscilloscope (MSO) for data acquisition (DAQ) and two 16-bit arbitrary waveform generator cards inside separate computers responsible for controlling the optical components. There is one more software-controllable voltage source for EVOAs.

IV. Initializing Signal Levels and Timing

We can describe two distinct phases of operation: initialization and key generation. In a deployed and working system the initialization phase sets attenuation levels and timing parameters to prepare for key generation so it's used less frequently. To enable quantum security the optical signal transmitted by Alice must be at the <1 photon / pulse level and for the optimal effect of phase modulation and noise rejection precise timing of the pulses is needed. Fluctuations in the physical properties of the fiber used as quantum channel need to be compensated for to control these conditions and the initialization tasks described here can be repeated as needed to achieve this. They include: setting attenuation levels, measuring the optical length of Alice's side, finally, based on several thousand frames setting up the series of arrival times of every incoming pulse. For this we developed our own algorithm aiming to achieve a fully automatic initialization phase, in accordance with the plug & play principles.

A. Setting optical power levels

We require different optical power levels for the two operation phases because we alternate between using different types of detectors. During initialization we need higher optical power level for our self-designed LPDs on Alice's side (while measuring optical path length, see in next step) than during key distribution.

The optical power received by Alice is increased by switching only Alice's attenuation. The increase is not as critical as the base power level for the key generation phase, it's just enough for both of Alice's LPDs to produce a signal high enough above the detectors' internal noise level to trigger the oscilloscope.

B. Measuring Alice's optical path length

We determine the instantaneous propagation time with 2 ns definition still using the oscilloscope. The bulk of Alice's signal path is the SL, in case of which our method for the length measurement exploits the role of the two LPDs. The first (LPDc) detects frames arriving to Alice (deflected by the 90 / 10 BS), while the other (LPDm) detects them travelling backwards (after reflection on the FM). Following the optical path of a single pulse entering Alice's device, we can determine the round trip time of the pulse when it travels back and forth between the BS and FM.

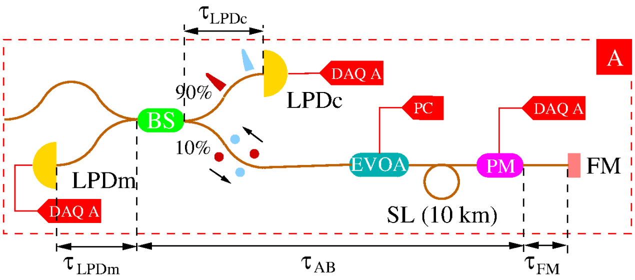


Fig. 2. More detailed view of Alice's components. Complementing the LPD on the signal input port of the BS another one was inserted on the tap output port. Notations: τ_{LPDc} denotes the time delay between the BS and LPDc, while τ_{LPDm} is the same for LPDm, τ_{AB} is the time delay between BS and PM, while τ_{FM} is the time delay between the PM and FM.

1) Details of the calculation: Using the notation of Figure 2, the delay time T_{total} between the two LPDs' signals (which detect identical parts of the incoming signal split at BS) is

$$\begin{aligned} T_{\text{total}} &= 2(\tau_{\text{AB}}+\tau_{\text{FM}})-\tau_{\text{LPDc}}+\tau_{\text{LPDm}} \\ &= 2(\tau_{\text{AB}}+\tau_{\text{FM}}), \end{aligned} \qquad (4.1)$$

where the two time delays τ_{LPDc} and τ_{LPDm} cancel, since the fiber lengths are the same between the BS and the two LPDs. We have mentioned in Section III that the trailing part of each pulse pair should be modulated. The minimal delay T_{min} between the detection of the leading part of an incoming pulse pair by LPDc and the modulation of the trailing part of the same pulse pair is given by

$$T_{\text{min}}=\tau_{\text{AB}}-\tau_{\text{LPDc}}+2\tau_{\text{FM}}+\tau_{\text{p}}, \qquad (4.2)$$

where τ_{p} is the pulse duration. Using this time delay, the modulation of the trailing part of each pulse pair starts right after the leading pulse has left the phase modulator. In our setup $\tau_{\text{LPDc}}=2\tau_{\text{FM}}$, $\tau_{\text{p}}=20$ ns. Hence T_{min} is given by

$$T_{\text{min}}=\tau_{\text{AB}}+20\,\text{ns}, \qquad (4.3)$$

where $\tau_{\text{AB}}=T_{\text{total}}/2-\tau_{\text{FM}}$, furthermore the refractive index and length of the fiber, $n_{\text{fiber}}=1.467$, L_{FM}=0.5 m, $c=3\cdot10^8$ m/s, so $\tau_{\text{FM}}=n_{\text{fiber}}L_{\text{FM}}/c\simeq2.45$ ns.

2) Producing the actual modulation delay for Alice: Using T_{min} here obtained from oscilloscope we don't account for the fact that Alice's card has a trigger-to-output delay of 238.5 sample clock cycles + 16 ns. But in the key generation phase directly the card is triggered to produce the phase modulation signal, so we still have to. With the 500 MSa/s base resolution setting applied in our tests and demonstration, this adds up to 493 ns, but in reality and together with the propagation times of the coaxial cables it has a value of 510 ns. (This value varies slightly, ostensibly due to the phase relation of the clocks in Alice's DAQ card and Bob's one, which provides the triggering optical signal.) Therefore, as part of this step we measure this total latency. We do so by setting an immediate output on triggering Alice's card and this time measuring the ΔT_{cor} time difference of the triggering optical signal and the card's output (yielding a $-\Delta T_{\text{cor}}$ correction to T_{min}).

3) Tolerance of the delay: The light pulse train contains 480 pulse pairs after leaving Bob's side. We wait for the first pulse of the pair to pass PMa after returning from the FM. There is a 50 ns delay between the two pulses of each pair (due to the DL) and every pulse is 20 ns wide, furthermore, systematic uncertainties that are the 2 ns definition of our measurement and the 2 ns sampling time of the DAQ cards summed up for worst case estimation leave a $T_{\mathrm{margin}} = 26$ ns or to fit into with the start of our modulation signal. The cards have 16×2 ns resolution for trigger delay so the geometry of the components must be chosen so that integer times 32 ns is well between $T_{\min} - \Delta T_{\mathrm{cor}}$ and $T_{\min} - \Delta T_{\mathrm{cor}} + T_{\mathrm{margin}}$. Otherwise, we can tune ΔT_{cor} with the choice of coaxial cable, T_{margin} with switching to 625 MSa/s on the waveform generator or in extreme case $T_{\min}$ by setting τ_{FM} with a custom made fiber FM.

C. Setting up detection time series for Bob

In this last step we set up a time grid of 480 points with a frequency that we calculate from the detection events of a few thousand frames. What we want to be certain about then, is the arrival time of the first pulse, so that we can know the exact arrival times of every qubit in a frame. In this way we can later identify each and every detection resulting from sent qubits and can proceed with the basis reconciliation process to sift our key.

We aggregated the detection signal from 4500 frames in this step of the initialization. Groups of detection time tags gather around a set of time values compared to a signal that is synchronous with the laser firing (both are produced by the DAQ card controlling Bob). Some other time tags can also be observed between these groups that can be assessed as noise. Our task is to determine whether detection ticks belong to signal or noise.

1) Measurements: For every time tag in the aggregated data we add the distances from its neighbours. We then filter the majority of the noise ticks from the signals by comparing this sum to a threshold of 50 ns – some of the latter category can also be considered noise (typically near the edges of groups) in this phase. After this separation we only work with the signal data.

We calculate the mean value of time tags in each group. We continue by setting up multiple grids of 480 points with slightly different period times in the range 201 ns $> T_{\mathrm{grid}} >$ 199 ns and we search for the grid with minimal sum of absolute differences from the calculated mean values fixing the first grid point to the first mean value. We determine period time of the photon arrivals with 2 ps precision: for one channel $T_{\mathrm{grid,CH1}} = 199.996$ ns while for the other $T_{\mathrm{grid,CH2}} = 199.994$ ns so we initialized our data processing scripts with a common $T_{\mathrm{grid}} = 199.995$ ns. (The deviation from the expected 200 ns justifies opting to make this measurement, especially because this time grid is what helps us select signal and filter noise in the key generation phase.) The other required value was the first expected time of arrival, i. e. the mean value from the time tags in the first group on each channel. These values were $t_{1,\mathrm{CH1}} = 98964.089$ ns and $t_{1,\mathrm{CH2}} = 98974.460$ ns for SPAD1 and SPAD2 respectively, counted from emission. This 10 ns delay on channel 2 is due to the circulator that inserts 2 m of fiber before SPAD2.

2) Utility of results: To see why $T_{\mathrm{grid,CHi}}$ values can be determined in 10 ppm agreement and used to obtain T_{grid} with optimal accuracy, let's discuss how the aggregated frames are produced. Although Alice can perform no modulation throughout initialization, Bob alone can keep introducing a $\pi/2$ phase shift so that balanced optical power exits the interferometer arms. By doing so, for the same ordinal number of detection groups in the aggregated data of the 2 channels, signal photons originate from the same light pulse. Consequently, detection group mean values pairwise correspond to the same expected pulse arrival times, and the same holds for variances and higher moments, in addition the same time grid should give the best fit to them. We essentially have 2 measurements on 4500 points for the best fitting time grid which are sampled in identical circumstances and thus can be averaged to get a more precise value.

The choice of the first detection group mean as origin of the time grids to fit to data can be shown to be best as follows. The detector dead time being much greater than pulse width causes tick probability to decay exponentially over the first few pulses, resulting in a pronounced peak in tick number per group at the beginning of frames. The gradual 'opening' of the detectors makes this actually a global maximum for a frame, i. e. the first one the most sampled (most accurate) pulse arrival time.

Considering that this argument is based on the waiting time for the first impulse of the frame after the last one of the previous frame being much greater than the dead time, it makes the measurement also useful for estimating photon number per pulse. We can neglect the dead time and say that detectors tick any time they measure at least 1 photon in these pulses, detecting any photon with $\eta = 0.1 \ll 1$ efficiency. For such η the detection probability p can be calculated as if an N photon coherent pulse were being detected with η attenuation and an ideal detector [38], i. e.

$$p = 1 - \exp(-\eta N). \tag{4.4}$$

We have summed up the counts of the two detectors and divided it by the number of pulses 4500 sent. Then inverting the formula (4.4) we obtained $N = 0.62$ for the mean photon number in the pulses.

V. KEY DISTRIBUTION

This phase of the operation implement s interference-based QKD with the truth table of BB84. As prerequisite for the proper operation of this phase we have to run the initialization to configure our control scripts and components. The only variables that are set in this phase are the modulation bits and the physical signals for the modulators based on them. One thing left to determine in advance for this is the driving voltage set for the modulators to achieve the necessary phase shifts.

Earlier we measured the equivalent control voltage V_c for π phase shift on Bob's phase modulator having Alice's modulation off: then we get constructive interference at the SPAD2 output of Bob's 50 / 50 BS and desctructive at the SPAD1 output with Bob's PM off. The situation is interchanged if we introduce a phase shift of π, i. e. in both cases we get detection on only one SPAD neglecting noise. Modulating with 1.55 V random impacts are expected biased so that $N_{\mathrm{det,CH1}}/N_{\mathrm{det,CH2}} = Q = 0.859$ ($N_{\mathrm{det,CHi}}$ being the photon count on SPAD i) due to the attenuation of the circulator.

Alice needs 2 different bases, which means 4 different phase shifts altogether: 0, π, $\pi/2$ and $3\pi/2$. However, the current geometrical dimensions (τ_{FM} on Figure 2 in particular) constrain Alice to modulate pulses traversing the modulator in both directions, i. e. start to modulate as soon as a pulse *reaches* PMa *towards* FM so that the whole pulse is modulated through, albeit twice. Then pulses are orthogonally polarized on the two passes. The PM having polarization dependent characteristics such V_c values are sought that the sums of phase shifts in 2 directions are π, $\pi/2$ and $3\pi/2$ for the pulses. We performed an exhaustive search over a range of voltage values. At every inspected value we emitted 100 frames and calculated the $N_{\mathrm{det,CH1}}/N_{\mathrm{det,CH2}}$ quotient, comparing it to Q , this way we were able to determine 1.22 V for $\pi/2$.

When searching higher voltages for $3\pi/2$ we experienced high fluctuations and quotient values were far away from Q. Based on calculations we assumed that sinusoidal characteristics can be a close approximation for the operation of the PM but only when we modulate between $-\pi$ and π phases. Since the PM is operational at negative voltage s and our signal generator can output positive and negative voltages, the issue was solved by mirroring the 1.22 V for $\pi/2$ on zero point and search for the proper V_c for $3\pi/2$ there. With this idea we successfully found -1.23 V good enough for $3\pi/2$ phase shift. Our approach for finding π phase shift was based on the sinusoidal characteristics and two V_c values of 1.22 V for $\pi/2$ and an earlier estimated 3.56 V for $3\pi/2$ that we could not place in practice due to the unfavorable results mentioned before. Our assumption was that the demanded V_c for π should have been at the mean of this two values, that is 2.39 V. We checked this voltage with our scripts and so we got the presumed satisfying results. The control voltages paired to the bases in the implemented BB84 protocol applied in our system for the demonstration can be seen summarized in Table I.

TABLE I
CONTROL VOLTAGES FOR BASES

	phase [rad]	voltage [V]
Bob	0	0
	π/2	1.55
Alice	0	0
	π	2.39
	π/2	1.22
	3π/2	-1.23

The modulation delay in compliance with IV-B3, the DAQ card sampling frequency, memory and buffer size and trigger mode is set on Alice's side as well as parameters necessary for the waveform we would like to generate (e.g. analog / digital output, channel options, generation mode) by a Python module created to support the key distribution process. Exploiting the capabilities of the card we implemented the key distribution on Alice's side and we created the data processing at Bob to distill the key.

VI. DEMONSTRATION RESULTS

The truth table of BB84 regarding our system enumerates the 8 cases of basis pairing with Alice's and Bob's choices in Table II. We performed deterministic demonstration, i.e. we inspected all 8 cases by generating constant series for every initial key combination. This way tracing back the sources of errors in the results is as simple as comparing them to the truth table of the BB84 protocol.

For each case we prepared series of 100 frames. In the 4 matching basis choice scenarios we expected the sifted key bits at Bob to be the same as in Alice's initial key. In the data processing of the detected pulses we call an impact noise if it is outside a 25 ns radius centered at any expected arrival time in the grid we established in the initialization phase. Similarly, we call signal those impacts that are within this time interval. In matching basis choice scenarios we count the signal bits different from Alice's initial key values and name them false bits, the rest correct ones. From these data we can calculate the success rate of our implementation as the ratio of correct to all signal bits.

When dealing with different basis choices, we compare the bias photon count ratio to $Q = 0.859$ because for each such combination one detection tick means one sample of a modulation voltage measurement described in Section V. The percentage difference from this bias is a figure of merit for the accuracy of the modulation. The results of the demonstration are introduced in Tables III and IV.

In case of similar basis choices the results are introduced in Table III. These scenarios are responsible for producing sifted key bits. This means that the success rate calculated from this data is the determining factor in the quality of our demonstration. The last row of Table III shows that our implementation corresponds to the theoretical BB84 truth table in between 78.22 % and 97.49 % and that the more places in our system we apply modulation the more error we introduce into the signal detection. Still, the above 90 % values present promising first results.

The penultimate row of the Table IV shows that in a worst case scenario we have 5.33 % difference from Q, which occurs when we apply modulation on both sides. The first three columns indicate the error rate that a single modulation produces (4.89 % – 9.66 % that represents 14-30 false bits out of 100 frames). Together with previously mentioned results this suggests that the modulation creates interference that deviates from the optimal. Further adjustments of the modulation voltages may take care of this deviation, enhance success rate and fix Q_{measured} values more precisely to Q.

The cumulative results that have been calculated only from the same basis choice scenarios are summarized in Table V. Our system operates at 88.11 % success rate over physical layer based on 400 frames and altogether almost 2000 photon impacts. This only refers to the raw key bit success rate

TABLE II
BB84 TRUTH TABLE

Basis and phase choice of Alice	0 (0)	0 (0)	0 (π)	0 (π)	1 ($\pi/2$)	1 ($\pi/2$)	1 ($3\pi/2$)	1 ($3\pi/2$)
Alice bits ('encoding')	0	0	1	1	0	0	1	1
Basis choice of Bob	0 (0)	1 ($\pi/2$)	0 (0)	1 ($\pi/2$)	0 (0)	1 ($\pi/2$)	0 (0)	1 ($\pi/2$)
Bob bits ('measurement')	0	–	1	–	–	0	–	1

In practice, Alice and Bob sample an independent and uniformly distributed random variable on each transmission (within a frame) to select a combination. In 4 combinations they choose matching bases and in 4 different ones; in the former case their identical bits yield the sifted key bits and in the latter, marked with dashes (–), Bob collects data to be statistically tested against the hypothesis of the presence of an eavesdropper (Eve).

TABLE III
RESULTS FOR SAME BASIS CHOICE SCENARIOS

Phases (bases) (Bob – Alice)	0 - 0	0 - π	$\pi/2$ - $\pi/2$	$\pi/2$ - $3\pi/2$
Noise	25	34	46	53
Signal	439	423	464	482
False Detection (Out of Signal)	11	34	65	105
Success Rate [%]	**97.49**	**91.96**	**85.99**	**78.22**

TABLE IV
RESULTS FOR DIFFERENT BASIS CHOICE SCENARIOS

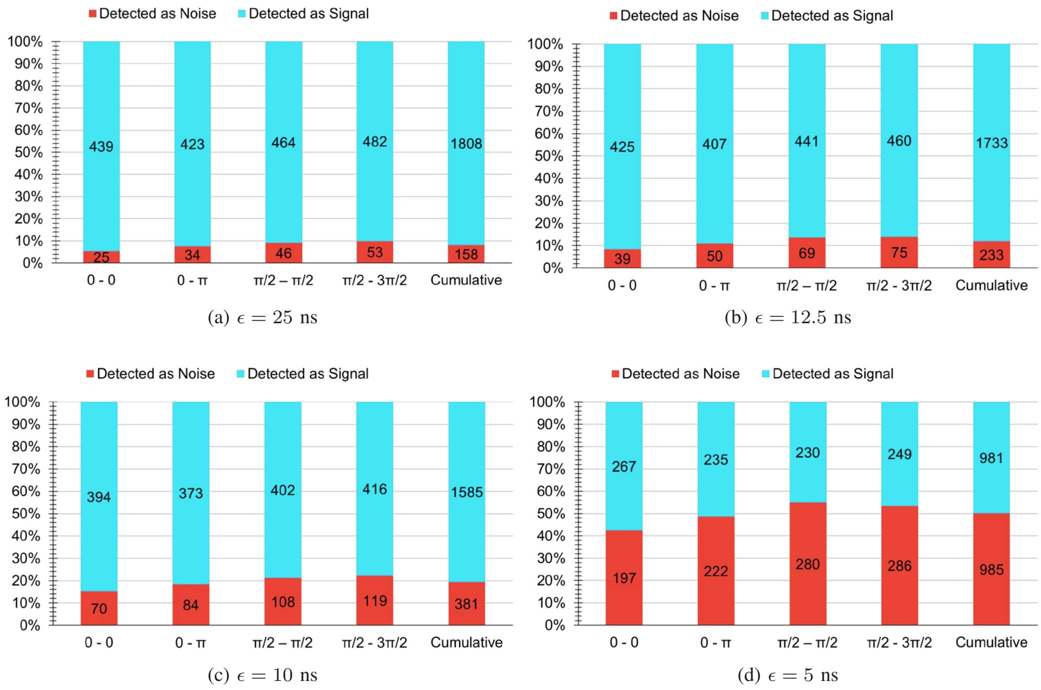
Phases (bases) (Bob – Alice)	0 - $\pi/2$	0 - $3\pi/2$	$\pi/2$ - 0	$\pi/2$ - π
Noise	46	44	53	49
Signal	671	659	679	653
Ticks on SPAD1 and on SPAD2 resp.	318 ; 353	288 ; 371	323 ; 356	283 ; 370
Q_{measured} ($N_{\text{det,CH1}}/N_{\text{det,CH2}}$)	0.901	0.776	0.907	0.765
Difference from target $Q = 0.859$ [%]	**4.89**	**9.66**	**5.59**	**10.9**
Difference [detector ticks]	14.8	30.8	17.1	34.8

and does not concern the classical key distillation methods utilized by upper layers – our research only covers the physical layer of the system. Since this error rate of 11-12 % is only scratching the edge of the possibility to indicate the presence of an eventual eavesdropper [39], we've started to search for solutions and development directions to reach a success rate reliably above 90 %.

Besides the control voltages for the bases, the timing of the Alice-side modulation can also be a critical error source as well as our detection process. We modulate in two passes so we have to start the modulation earlier by 5 ns, i. e. two times the propagation time τ_{FM} between PMa and FM: T_{margin} is narrowed down to 21 ns. This is necessary for avoiding non-uniform modulation of the pulses. We may get less noisy transmission if we could synchronize to the instance

TABLE V
CUMULATIVE RESULTS FOR SAME BASIS CHOICE SCENARIOS

Noise	158
Signal	1808
False Detection (Out of Signal)	215
Success Rate [%]	**88.1084**



(a) $\epsilon = 25$ ns

(b) $\epsilon = 12.5$ ns

(c) $\epsilon = 10$ ns

(d) $\epsilon = 5$ ns

Fig. 3. Change in classification of ticks as signal or noise with varying ϵ

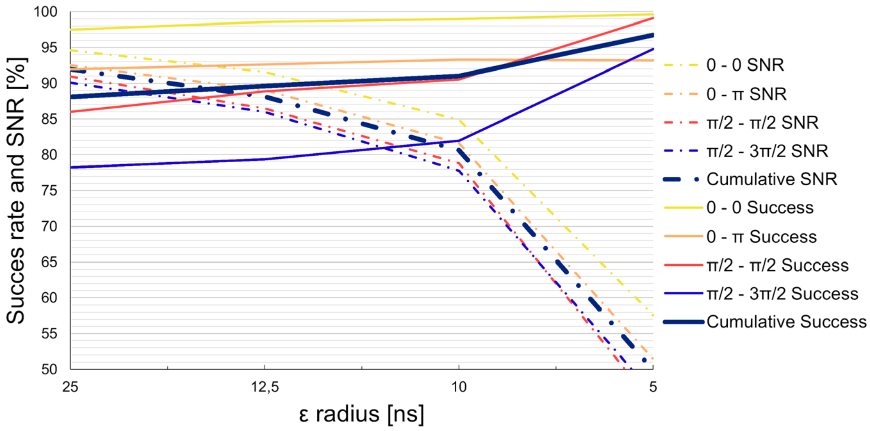


Fig. 4. Percentage SNRs and success rates as functions of ϵ in a finer sweep, noise seen to start dominating above cca. 10 ns

before the pulses arrive to the modulator back from the mirror but they've left PMa propagating towards it. This requires the extension of the fiber path between these components. The other critical part is the detection where we decided to consider the ticks within an $\epsilon = 25$ ns radius around every point in the grid. After getting the demonstration results we considered modifying this radius in the hope of achieving better success rates. Our motivation was to filter more noise from our transmitted pulses so we started to shrink this 50 ns time interval – first to 25 ns, then 20 ns and finally to 10 ns ($\epsilon = 12.5, 10, 5$ ns, respectively). This way we also exclude more signal bits, decreasing our SNR that can be seen on Figure 3. The question is how this software modification will affect our success rates. Recalculating the demonstration results with these new ϵ values we arrive at Figure 4. We can observe that the curves representing the success rates rise monotonously with the decrease of the radius. Setting $\epsilon = 5$ ns the curve representing the cumulative success rate can reach 96.73 % – meanwhile the SNR, unfortunately drops dramatically. This means that we can make our protocol 8 % more effective with bit identification, making it more secure but signal bit rates will fall resulting in slower key generation. We need to find the optimal ϵ, which depends on our optimizing strategy. We calculate trends in success rate and SNR on the 3 sections. Between 5 ns and 10 ns the slope of the SNR significantly drops so we can choose 10 ns to be a threshold point as one strategy that results in over 90 % success rate and only a 10 % reduction in SNR. However, a preferable solution is to improve the SNR of the system in advance so that our corresponding curves in this diagram could shift towards smaller ϵ, while the ones representing success rates to wards greater. This way we could improve the efficiency of our system to a great extent only slightly reducing bit generation rate.

VII. Outlook

We are currently at the start of a next stage with various kinds of research goals to be set.

- *Optimization of current components*
  Adjustments of PM voltages with reference to Table IV, in particular $\Delta Q = Q_{\text{measured}} - Q$ – these results are significantly higher than what we expected based on previous results from determining these voltages.
  We can also try using gated detection as in the original paper proposing this architecture. It's worth pointing out, though, that the time grid fitting method for detection is the mechanism that enables our implementation to work with detectors in (or potentially only capable of) free running mode.
- *Hardware improvement*
  Our EVOAs have the feature of modulation, which gives the idea to set higher attenuation values when Alice isn't transmitting or Bob's detectors aren't expecting frames. Yet with the bandwidth of currently used MEMS devices is insufficient for this.
- *Improvement towards field applicability*
  Small form factor pluggable (SFP) lasers have become more and more commonly available and widespread for use in telecommunication, which makes it desirable to test performance with such a source. Furthermore, the oscilloscope would have to be substituted with the similarly common time to digital conversion (TDC).
  A step towards field practicality would be fully automating DAQ cards to operate independently from PCs (like they do now).

VIII. Conclusion

In this paper we made a successful approach to realize quantum key distribution in an optical fiber system, for which a precise modulation timing was implemented at Alice. The system structure required synchronisation between Alice and Bob taking emitted pulse frames as reference. Our calculations revealed a tight criteria for the time window targeted with the modulation signal. For establishing this timing mechanism for key distribution, we introduced an initial phase within necessary adjustments of optical power levels and optical length measurements within 2 ns accuracy are carried out. In subsections IV-A and IV-B we describe our solutions for adjusting our system parameters to find the critical modulation time window.

We implemented BB84 protocol in our system setting up the bases for modulation on both sides as described in section V by performing exhaustive search to find the control voltages responsible for the appropriate phase shifts on the laser pulses. A detection grid was also set up at Bob during initialization phase introduced in subsection IV-C. The grid consisting of the expected photon arrival time series includes a basic initial noise filtering. Furthermore, the adjustment of a single parameter of noise filtering gives the opportunity of setting efficiency adjustments in raw key quality and generation by software.

Based on the first results our system operates at 88.11 % success rate for the aggregated data. Part of the deterministic tests we achieved 97.49 % as the best individual performance among base pairings. The demonstration showed the potential in our system to reach this level also in overall efficiency with parameter optimization, hardware improvements and more efficient software techniques. We intend to implement these upgrades by the principles of plug & play that we have followed during our previous efforts, as well.

Our work contributes to the research goal of providing quantum security in commercial communication networks that stands economically.

References

[1] S. Imre, "Quantum computing and communications - introduction and challenges," *Comput. Electr. Eng.*, vol. 40, no. 1, p. 134–141, Jan. 2014, DOI: 10.1016/j.compeleceng.2013.10.008.

[2] ——, "Quantum communications: explained for communication engi- neers," *IEEE Communications Magazine*, vol. 51, no. 8, pp. 28–35, August 2013, DOI: 10.1109/MCOM.2013.6576335.

[3] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, p. 7–11, Dec 2014, DOI: 10.1016/j.tcs.2014.05.025.

[4] L. B. Laszlo Gyongyosi and S. Imre, "A Survey on Quantum Key Distribution," *Infocommunications Journal*, vol. XI, no. 2, pp. 14 – 21, 6 2020, DOI: 10.36244/ICJ.2019.2.2.

[5] S. Imre and F. Balázs, *Quantum Computing Basics*. John Wiley & Sons, Ltd, 2004, ch. 2, pp. 7–42, DOI: 10.1002/9780470869048.ch2.

[6] D. Kobor and E. Udvary, "Optimisation of Optical Network for Continuous-Variable Quantum Key Distribution by Means of Simulation," *Infocommunications Journal*, vol. XII, no. 2, pp. 18 – 24, 6 2020, DOI: 10.36244/ICJ.2020.2.3.

[7] A. Mraz, Z. Kis, S. Imre, L. Gyongyosi, and L. Bacsardi, "Quantum circuit-based modeling of continuous-variable quantum key distribution system: Simulation results of a novel cvqkd circuit," *International Journal of Circuit Theory and Applications*, vol. 45, 04 2017, DOI: 10.1002/cta.2347.

[8] Ágoston Schranz and E. Udvary, "Mathematical analysis of a quantum random number generator based on the time difference between photon detections," *Optical Engineering*, vol. 59, no. 4, pp. 1 – 13, 2020, DOI: 10.1117/1.OE.59.4.044104.

[9] Y. Mao, B.-X. Wang, C. Zhao, G. Wang, R. Wang, H. Wang, F. Zhou, J. Nie, Q. Chen, Y. Zhao, Q. Zhang, J. Zhang, T.-Y. Chen, and J.-W. Pan, "Integrating quantum key distribution with classical communications in backbone fiber network," *Opt. Express*, vol. 26, no. 5, pp. 6010–6020, Mar 2018, DOI: 10.1364/OE.26.006010.

[10] M. Gündoğan, J. S. Sidhu, V. Henderson, L. Mazzarella, J. Wolters, D. K. L. Oi, and M. Krutzik, "Proposal for space-borne quantum memories for global quantum networking," *npj Quantum Information*, vol. 7, no. 1, p. 128, Aug 2021, DOI: 10.1038/s41534-021-00460-9.

[11] R. Kaltenbaek, A. Acin, L. Bacsardi, P. Bianco, P. Bouyer, E. Diamanti, C. Marquardt, Y. Omar, V. Pruneri, E. Rasel, B. Sang, S. Seidel, H. Ulbricht, R. Ursin, P. Villoresi, M. van den Bossche, W. von Klitzing, H. Zbinden, M. Paternostro, and A. Bassi, "Quantum technologies in space," *Experimental Astronomy*, Jun 2021, DOI: 10.1007/s10686-021-09731-x.

[12] M. Mastriani, S. Iyengar, and L. Kumar, "Satellite quantum communication protocol regardless of the weather," *Optical and Quantum Electronics*, vol. 53, 04 2021, DOI: 10.1007/s11082-021-02829-8.

[13] L. Bacsardi, “On the way to quantum-based satellite communication,” *Communications Magazine*, IEEE, vol. 51, pp. 50–55, 08 2013, doi: 10.1109/MCOM.2013.6576338.

[14] J. S. Sidhu, S. K. Joshi, M. Gündoğan, T. Brougham, D. Lowndes, L. Mazzarella, M. Krutzik, S. Mohapatra, D. Dequal, G. Vallone, P. Villoresi, A. Ling, T. Jennewein, M. Mohageg, J. G. Rarity, I. Fuentes, S. Pirandola, and D. K. L. Oi, “Advances in space quantum communications,” *IET Quantum Communication*, vol. n/a, no. n/a, Jul 2021, doi: 10.1049/qtc2.12015.

[15] K. Günthner, I. Khan, D. Elser, B. Stiller, Ömer Bayraktar, C. R. Müller, K. Saucke, D. Tröndle, F. Heine, S. Seel, P. Greulich, H. Zech, B. Gütlich, S. Philipp-May, C. Marquardt, and G. Leuchs, “Quantum-limited measurements of optical signals from a geostationary satellite,” *Optica*, vol. 4, no. 6, pp. 611–616, Jun 2017, doi: 10.1364/OPTICA.4.000611.

[16] C. Simon, “Towards a global quantum network,” *Nature Photonics*, vol. 11, no. 11, pp. 678–680, Nov 2017, doi: 10.1038/s41566-017-0032-0.

[17] P. Villoresi, T. Jennewein, F. Tamburini, M. Aspelmeyer, C. Bonato, R. Ursin, C. Pernechele, V. Luceri, G. Bianco, A. Zeilinger, and et al., “Experimental verification of the feasibility of a quantum channel between space and earth,” *New Journal of Physics*, vol. 10, no. 3, p. 033038, Mar 2008, doi: 10.1088/1367-2630/10/3/033038.

[18] L. Calderaro, C. Agnesi, D. Dequal, F. Vedovato, M. Schiavon, A. Santamato, V. Luceri, G. Bianco, G. Vallone, and P. Villoresi, “Towards quantum communication from global navigation satellite system,” *Quantum Science and Technology*, vol. 4, no. 1, p. 015012, dec 2018, doi: 10.1088/2058-9565/aaefd4.

[19] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, “Entanglement-based quantum com- munication over 144km,” *Nature Physics*, vol. 3, no. 7, pp. 481–486, Jul 2007, doi: 10.1038/nphys629.

[20] K. Resch, M. Lindenthal, B. Blauensteiner, H. Böhm, A. Fedrizzi, C. Kurtsiefer, A. Poppe, T. Schmitt-Manderbach, M. Taraba, R. Ursin, P. Walther, H. Weier, H. Weinfurter, and A. Zeilinger, “Distributing en- tanglement and single photons through an intra-city, free-space quantum channel,” *Opt. Express*, vol. 13, no. 1, pp. 202–209, Jan 2005, doi: 10.1364/OPEX.13.000202.

[21] F. Steinlechner, S. Ecker, M. Fink, B. Liu, J. Bavaresco, M. Huber, T. Scheidl, and R. Ursin, “Distribution of high-dimensional entanglement via an intra-city free-space link,” *Nature Communications*, vol. 8, no. 1, p. 15971, Jul 2017, doi: 10.1038/ncomms15971.

[22] R. Valivarthi, M. G. Puigibert, Q. Zhou, G. H. Aguilar, V. B. Verma, F. Marsili, M. D. Shaw, S. W. Nam, D. Oblak, and W. Tittel, “Quantum teleportation across a metropolitan fibre network,” *Nature Photonics*, vol. 10, no. 10, pp. 676–680, Oct 2016, doi: 10.1038/nphoton.2016.180.

[23] Q.-C. Sun, Y.-L. Mao, S.-J. Chen, W. Zhang, Y.-F. Jiang, Y.-B. Zhang, W.-J. Zhang, S. Miki, T. Yamashita, H. Terai, X. Jiang, T.-Y. Chen, L.-X. You, X.-F. Chen, Z. Wang, J.-Y. Fan, Q. Zhang, and J.-W. Pan, “Quantum teleportation with independent sources and prior entanglement distribution over a network,” *Nature Photonics*, vol. 10, no. 10, pp. 671–675, Oct 2016, doi: 10.1038/nphoton.2016.179.

[24] M. Mastriani, S. S. Iyengar, and K. J. Latesh Kumar, “Bidirectional teleportation for underwater quantum communications,” *Quantum Information Processing*, vol. 20, no. 1, p. 22, Jan 2021, doi: 10.1007/s11128-020-02970-5.

[25] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, “Current status of the DARPA quantum network,” in *Quantum Information and Computation* III, E. J. Donkor, A. R. Pirich, and H. E. Brandt, Eds., vol. 5815, International Society for Optics and Photonics. SPIE, 2005, pp. 138 – 149, doi: 10.1117/12.606489.

[26] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, “The SECOQC quantum key distribution network in vienna,” *New Journal of Physics*, vol. 11, no. 7, p. 075001, jul 2009, doi: 10.1088/1367-2630/11/7/075001.

[27] D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, and et al., “Long-term performance of the swissquantum quantum key distribution network in a field environment,” *New Journal of Physics*, vol. 13, no. 12, p. 123001, Dec 2011, doi: 10.1088/1367-2630/13/12/123001.

[28] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, “Field test of quantum key distribution in the tokyo qkd network,” *Opt. Express*, vol. 19, no. 11, pp. 10 387–10 409, May 2011, doi: 10.1364/OE.19.010387.

[29] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, and et al., “Satellite-relayed intercontinental quantum network,” *Physical Review Letters*, vol. 120, no. 3, Jan 2018, doi: 10.1103/physrevlett.120.030501.

[30] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, S.-L. Han, Q. Yu, K. Liang, F. Zhou, X. Yuan, M.-S. Zhao, T.-Y. Wang, X. Jiang, L. Zhang, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, C.-Y. Lu, R. Shu, J.-Y. Wang, L. Li, N.-L. Liu, F. Xu, X.-B. Wang, C.-Z. Peng, and J.-W. Pan, “An integrated space-to-ground quantum communication network over 4,600 kilometres,” *Nature*, vol. 589, no. 7841, pp. 214–219, Jan 2021, doi: 10.1038/s41586-020-03093-8.

[31] S. E. Ltd, “Cryptography secures swiss elections,” (accessed: 03.08.2021). [Online]. Available: https://optics.org/article/31646

[32] R. Naik and P. Reddy, “Towards secure quantum key distribution protocol for wireless lans: a hybrid approach,” *Quantum Information Processing*, vol. 14, 12 2015, doi: 10.1007/s11128-015-1129-3.

[33] “Sk telecom continues to protect its 5g network with quantum cryptography technologies,” Mar 2019, (accessed: 03.08.2021). [Online]. Available: https://www.idquantique.com/sk-telecom-continues-to-protect-its-5g-network-with-quantum-cryptography-technologies/

[34] R. Asif and W. J. Buchanan, “Recent progress in the quantum-to-the-home networks,” in *Telecommunication Networks*, M. A. Matin, Ed. Rijeka: IntechOpen, 2019, ch. 2, doi: 10.5772/intechopen.80396.

[35] “Banking,” Aug 2020, (accessed: 03.08.2021). [Online]. Available: https://www.idquantique.com/random-number-generation/applications/banking/

[36] A. M. Lewis and M. Travagnin, “A secure quantum communications infrastructure for europe,” Joint Research Centre, Report JRC116937, 2019.

[37] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, “Quan- tum key distribution over 67 km with a plug&play system,” *New Journal of Physics*, vol. 4, pp. 41–41, jul 2002, doi: 10.1088/1367-2630/4/1/341.

[38] G. Zambra, A. Andreoni, M. Bondani, M. Gramegna, M. Genovese, G. Brida, A. Rossi, and M. G. A. Paris, “Experimental reconstruction of photon statistics without photon counting,” *Phys. Rev. Lett.*, vol. 95, p. 063602, Aug 2005, doi: 10.1103/PhysRevLett.95.063602.

[39] P. W. Shorand J.Preskill,“Simple proof of security of the bb84 quantum key distribution protocol,” *Phys. Rev. Lett.*, vol. 85, pp. 441–444, Jul 2000, doi: 10.1103/PhysRevLett.85.441.

Márton Czermann received his BSc degree in 2020 in Electrical Engineering from the Budapest University of Technology and Economics. He started his MSc studies at the Department of Networked Systems and Services at the same faculty. He joined a fiber-based DV-QKD project in 2018 which realizes the BB84 algorithm and a free space entanglement-based DV-QKD project in 2019. Since 2020, he is also a participant of Quantum Future Academy, Berlin.

Péter Trócsányi MSc student with the major of Research Physicist. In 2019 started investigating polarization phenomena and joined Ericsson Hungary RD as an intern. He received his BSc in Electrical Engineering from the Budapest University of Technology and Economics in 2020 prototyping optical quantum random number generators for his thesis. That year he started his Physics studies which involved shifting his focus from fiber to free space optics. He joined Wigner Research Center for Physics as an intern in 2021. He has been member of Simonyi (since 2016) and Wigner (since 2020) Colleges for Advanced Study.

Zsolt Kis gained the PhD degree in physics in 2000 at the University of Szeged. His main research field is quantum optics. Recently he has been leading a research group on developing single photon sources in the visible and telecommunication wavelength domain. He has participated in the development of the first Hungarian CV QKD system. Now he leads the development of a new CV QKD system and a DV QKD system which realizes the BB84 algorithm.

Benedek Kovács edge computing expert. The main responsibilities are engineering the evolution of telecommunication networks in the area of 5G and edge computing and managing innovation projects and university collaborations. Joined Ericsson in 2005 as a software developer and tester, and later worked as a system engineer, served as the characteristics, performance management and reliability specialist in the development of the 4G VoLTE solution, since then he focuses on edge computing. Kovács holds an MSc in information engineering and a PhD in mathematics from the Budapest University of Technology and Economics.

László Bacsárdi (M'07) received his MSc degree in 2006 in Computer Engineering from the Budapest University of Technology and Economics (BME) and his PhD in 2012. He is corresponding member of the International Academy of Astronautics (IAA). Between 2009 and 2020, he worked at the University of Sopron, Hungary in various positions including Head of Institute of Informatics and Economics. Since 2020, he is associate professor at the Department of Networked Systems and Services, BME and head of Mobile Communications and Quantum Technologies Laboratory. His current research interests are quantum computing, quantum communications and ICT solutions developed for Industry 4.0. He is the past chair of the Telecommunications Chapter of the Hungarian Scientific Association for Infocommunications (HTE), Vice President of the Hungarian Astronautical Society (MANT). Furthermore, he is member of AIAA, IEEE and HTE as well as alumni member of the UN established Space Generation Advisory Council (SGAC). In 2017, he won the IAF Young Space Leadership Award from the International Astronautical Federation.