Quantum communication experiments with entangled photon pairs

M. Peranić*, M. Lončarić*, A. Radman*, M. Stipčević*

* Photonics and Quantum Optics Research Unit, Center of Excellence for Advanced Materials and Sensing Devices, Ruđer Bošković Institute, Bijenička cesta 54, 10 000 Zagreb

Today, perhaps more than ever before, the security of information and communication is increasingly important. The cryptographic protocols used in classical cryptography are based on mathematical algorithms and can be breached. On the other hand, the laws of quantum physics enable quantum key distribution (QKD) and it is possible to achieve absolute security of communication based on the fundamental laws of nature. Anyone who would eavesdrop QKD-based communication must perform a measurement, which implies an impact on the system that can be detected by the sender and receiver. In this paper, we present a brief overview of QKD implementations and our experimental setup for generation of quantum key. Using this setup, we measured violation of the Bell's inequality of 114 standard deviations from the classical boundary, which confirms the non-local behavior of the entangled photon pairs. One can also use this source to create hybrid connections in combination with both optical fibers and free space.

Keywords* - *photonics, quantum optics, quantum communication, quantum networks, entanglement, cryptography

I. Introduction

Quantum key distribution (QKD) is a proven secure communication method that enables two (or more) parties to produce a random secret key. Opposite to the classical communication, QKD also won't be jeopardized by the development of quantum computers. The most commonly used QKD protocols are the so-called BB84 [1] and E91 [2] protocols, which use the fact that quantum states cannot be copied due to the no-cloning theorem in quantum physics, and that measurement essentially affects the quantum state of an object (so-called wave function collapse). On the other hand, quantum communication still has some limitations. One of them is the restriction to a small number of end users due to the problem of scaling quantum communication from two to a larger number of users. Other problems are large losses and decoherence that will occur when transmitting a signal over long distances, i.e. the restriction to short distances. If we try to increase the number of users and connect them to a quantum network, we also encounter several problematic aspects such as trusted nodes (Fig. 1) that are a potential security threat or active switches that limit both functionality and connectivity [3, 4]. In addition, imperfections of the entangled photon sources and corresponding detectors represent weak points that can expose QKD to attacks.

II. QKD implementations

A. Ground implementations

The world's longest chain of quantum communication-based links is in China and connects the cities of Beijing, Jinan, Hefei and Shanghai. The total length of the connection is over 2000 km, and networks of different topologies with 10 hubs have been built within each city. In order for the signal to be transmitted over such long distances, it was necessary to install 32 trusted nodes in the network. While in laboratory conditions the longest link without a trusted node of more than 400 km between two end users has been achieved [5], the record outside the laboratory is 192 km and was achieved via an optical fiber laid at the bottom of the sea connecting Malta and Sicily [6]. The optical fiber that was used did not transmit the classic signal at the same time (so-called dark fiber), and the specified distance was achieved by transmitting a signal from the same place where it was later detected (loopback). On the other hand, the largest network without a trusted node was established in Bristol, UK, in 2019 [7].

This network in Bristol supports up to eight fully connected users using only one source of entangled photon pairs that are shared without active switching between users using frequency multiplexing without the use of trusted nodes.

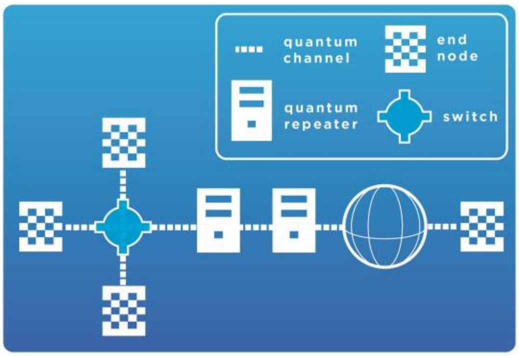

Figure 1. Quantum hardware elements examples [3]

While the QKD signal in the standard telecom fibers has an attenuation of about 0.2 dB/km, atmospheric attenuation in the air is significantly lower and therefore part of the research on the use of QKD is focused on Earth-satellite communication.

B. Space implementations

In late 2016, Chinese scientists launched the Micius satellite (weight 640 kg, power 560 W, 300 mm and 180 mm telescopes on-board) with the aim of exploring the possibilities of QKD-based communication using satellites [7]. The experiment lasted 23 days during different weather conditions, which also affected the results of the research. During 2017, a video conference was established via the Micius satellite between two locations on Earth 7600 km apart, in Austria and China [8] (Fig. 2). The generated key was used to encrypt two 5-kByte pictures and to AES-encrypt a video conference, refreshing the 128-bit seed key every second. The researches have also demonstrated downlink entanglement distribution generating 5.9 million entangled photon pairs per second at 810 nm and quantum teleportation in an uplink configuration [9].

While the Chinese research was more focused on demonstrating the feasibility of QKD entanglement-based protocols, Japanese researchers have conducted a small-scale experiment with the low-Earth orbit (LEO) satellite SORATES, which was carrying the SOTA (Small Optical TrAnsponder) laser communication terminal. It produced two non-orthogonally polarized signals in the ~800 nm band modulated at 10 MHz, which enabled QKD with estimated key rates of the order of several kbps [10].

Given better long-distance efficiencies, a satellite-Earth connection could be used to connect remote local terrestrial networks that would be built on the foundations of existing infrastructure at telecommunication wavelengths. In addition to generating an encryption key, QKD can be used for other applications such as clock synchronization [11], secure access to remote clouds [12] or the authentication of participants [13].

III. Current work

A. Entanglement

Entanglement is a quantum phenomenon that occurs when the particles are generated or interact in such a way

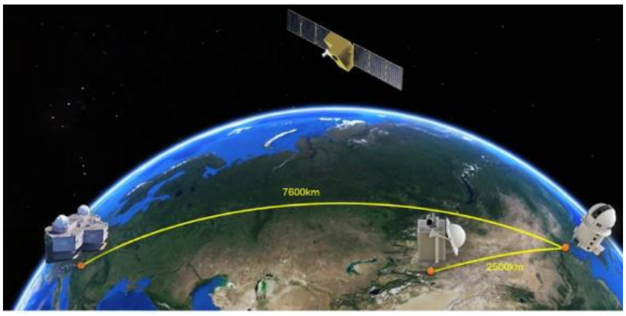

Figure 2. Space quantum communication [8]

that it is impossible to describe the quantum state of one of them independently of the state of the other. This phenomenon occurs no matter how distant entangled particles are from each other. Entanglement is the topic of the famous paper [14] by Einstein, Podolski and Rosen (so-called EPR paper or paradox) from 1935, in which they considered such behavior impossible in the terms of quantum theory as a complete and closed theory. Instead, they proposed a theory of hidden variables, which would expand quantum theory with some yet undetermined variables. However, almost 30 years later, Bell proposed a gedankenexperiment (thought experiment) that could rule out such hidden variable theory [15]. A similar inequality, that could be tested experimentally, was derived by Clauser, Horne, Shimony, and Holt (known as CHSH inequality). The results of their experiments truly showed a violation of this inequality. This result is in agreement with quantum theory and therefore theories of hidden variables have been increasingly abandoned.

B. Source of the polarization entangled photons

The main part of an experimental setup for QKD is the source of entangled photon pairs (Fig. 3). Photon pairs that are generated in the process of spontaneous parametric down conversion (SPDC) can travel two paths. Because these paths are indistinguishable, photons get entangled. In our setup, for the SPDC we are using 10 mm long periodically poled potassium titanyl phosphate (ppKTP) crystal of type-II with a poling period of 9.825 µm. In the SPDC process of type II, pump photons at 405 nm from a continuous wave laser are converted into two daughter photons known as signal and idler photons of mutually perpendicular polarization at 810 nm. This process satisfies the laws of energy and momentum conservation. The crystal has been placed inside of a Sagnac interferometer, which enables the pumping of the crystal from both sides. The entanglement comes from a superposition of created photon pairs on a polarization beam splitter providing maximally polarization-entangled Bell state. For the detection, we are using single photon detectors that are connected to the time taggers and further to the computer for analysis.

C. Results

Measuring the visibility:

$$V = (N_{max} - N_{min}) / (N_{max} + N_{min}), \quad (1)$$

where N_{max} and N_{min} correspond to a maximum and minimum number of coincidences for different sets of angles on polarizers at two users, shows that our source is producing maximally entangled photon pairs with visibility above 99% (Fig. 4). Measuring the CHSH inequality gives us a result of 114 standard deviations above the classical limit, which proves that "spooky action at a distance", as Einstein named entanglement, really is an integral part of quantum theory. These results are also a guarantee that our setup can be used for secure quantum communications.

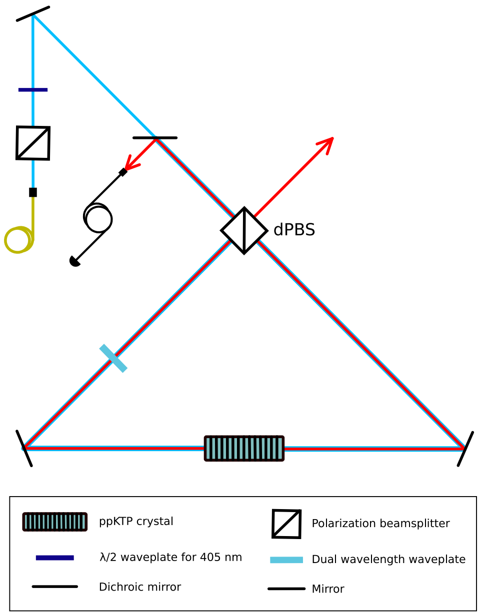

Figure 3. Experimental setup

D. *Other results*

In addition to the experiments with our source of polarization-entangled photons at 810 nm, our group has been working on the research of quantum networks at telecom wavelengths. In the recent experiment [6] conducted in collaboration with the University of Bristol and the IQOQI Vienna, we have realized the largest network with eight users using just one source of entangled photons. Different users have been connected with each other with different wavelengths using frequency multiplexing. This approach is scalable to large networks with hundreds of users. Furthermore, we have been part of a collaboration that established the first demonstration of quantum communication between Italy, Slovenia and Croatia during the G20 meeting in August 2021 in Trieste, Italy [17]. In addition to that, the 100.5 kilometer long quantum link between Trieste (in Italy) and Rijeka (in Croatia) was extended from Rijeka to the Croatian capital Zagreb via quantum enhanced communication, which is the first public demonstration of that kind. This significant achievement is a significant step toward pan-European quantum network.

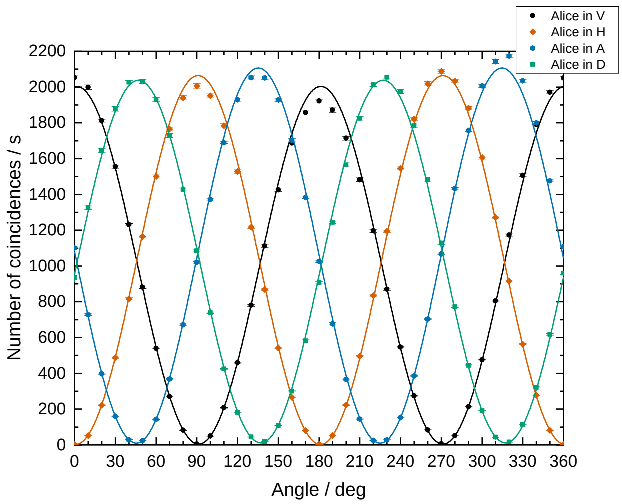

Figure 4. Results of visibility measurement

IV. Conclusion

Quantum communication offers possibilities for secure data transfer relying on already existing telecom communication infrastructure. The efforts for implementation are moving from laboratory conditions to real-life scenarios, exploring both terrestrial and space segment. Presented setup built in the Laboratory for Photonics and Quantum Optics of Ruđer Bošković Institute in Zagreb is a cornerstone for further experiments in the field of quantum communication and information. Its design and characteristics are proving its usability for exploring problems like hybrid ground-space communication schemes and advanced quantum communication networks.

Acknowledgment

Croatian Science Foundation, HRZZ grant No. IPS-2020-1-2616. and Croatian Ministry of Science and Education, MSE grant No. KK.01.1.1.01.0001.

References

[1] C. H. Bennett, G. Brassard, International Conference on Computer System and Signal Processing, IEEE, pp. 175–179, 1984

[2] A. K. Ekert, "Quantum Cryptography Based on Bell's Theorem," Phys.Rev.Lett., 67, pp. 661-663, 1991

[3] S. Werner, D. Elkouss, R. Hanson, "Quantum internet: A vision for the road ahead", Science 362, eaam9288, 2018

[4] P. Toliver et al., "Experimental investigation of quantum key distribution through transparent optical switch elements," IEEE Photonics Technology Letters, 15, 11, pp. 1669–1671, 2003

[5] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, "Secure Quantum Key Distribution over 421 km of Optical Fiber", PhysRevLett, 121, 190502, 2018

[6] S. Wengerowsky et al., "Passively stable distribution of polarisation entanglement over 192 km of deployed optical fibre," npj Quantum Inf 6, 5, 2020

[7] S.K. Joshi et al., "A trusted node-free eight-user metropolitan quantum communication network," Science advances, 6, 36, 2020

[8] J. Yin et al., "Satellite-based entanglement distribution over 1200 kilometers", Science, 356, pp. 1140–1144, 2017

[9] Sheng-Kai Liao et al., "Satellite-Relayed Intercontinental Quantum Network", Phys. Rev. Lett., 120, 030501, 2018

[10] J.G. Ren, P. Xu, H.L. Yong, L. Zhang, S.K. Liao, J. Yin, "Ground-to-satellite quantum teleportation", Nature 549, pp. 70-73, 2017

[11] A. Carrasco-Casado, H. Takenaka, M. Fujiwara, M. Kitamura, M. Sasaki, M. Toyoshima, "QKD from a microsatellite: the SOTA experience", Proceedings Volume 10660, Quantum Information Science, Sensing, and Computation X; 106600B, 2018

[12] P. Komar et al., "A quantum network of clocks", Nat. Phys., 10, pp. 582-587, 2014

[13] H. Buhrman, R. Cleve, S. Massar and R. de Wolf., "Nonlocality and communication complexity", Rev. Mod. Phys., 82, 665, 2010

[14] L. M. Ioannou, M. Mosca, "Public-key cryptography based on bounded quantum reference frames", Theo. Comp. Sci., 12, 560, pp. 33-45, 2014

[15] A. Einstein, B. Podolsky, N. Rosen, "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?", Phys. Rev. 47, 777, 1935

[16] J.S. Bell, "On the Einstein Podolsky Rosen paradox", Physics Physique Fizika 1, 195, 1964

[17] D. Ribezzo et al., "Deploying an inter-European quantum network", arXiv:2203.11359, https://doi.org/10.48550/arXiv.2203.11359, 2022