A roadmap for building quantum key distribution devices

Teodora Murariu
Departament CETATEA
National Institute for Research and Development of Isotopic and Molecular Technologies INCDTIM
Cluj-Napoca, Romania
teodora.murariu@itim-cj.ro

Andra Păstrăv
Departament of Communications
Technical University of Cluj-Napoca
Cluj-Napoca, Romania
andra.pastrav@com.utcluj.ro

Carmen Tripon
Departament CETATEA
National Institute for Research and Development of Isotopic and Molecular Technologies INCDTIM
Cluj-Napoca, Romania
carmen.tripon@itim-cj.ro

Cristian Morari
Departament CETATEA
National Institute for Research and Development of Isotopic and Molecular Technologies INCDTIM
Cluj-Napoca, Romania
cristim@itim-cj.ro

Emanuel Puşchiţă
Departament CETATEA
National Institute for Research and Development of Isotopic and Molecular Technologies INCDTIM,
Departament of Communications
Technical University of Cluj-Napoca
Cluj-Napoca, Romania
emanuel.puschita@com.utcluj.ro

Liviu P. Zârbo
Departament CETATEA
National Institute for Research and Development of Isotopic and Molecular Technologies INCDTIM
Cluj-Napoca, Romania
liviu.zarbo@itim-cj.ro

2022 21st RoEduNet Conference: Networking in Education and Research (RoEduNet) | 978-1-6654-5528-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/RoEduNet57163.2022.9921102

***Abstract*— Adopting the emerging quantum communication technologies seems to be a logical answer to the security challenges implied by the ever expanding of our communication networks and computing and storage facilities. Quantum communications are based on quantum key distribution, which uses quantum mechanical processes to generate cryptographic keys and to securely distribute them to the users in the networks. There already are quantum key distribution devices on the market, but it is ill advised to fully rely on such devices, in the national security use cases. Thus, each country in EU is actively trying or has already succeeded in developing their own prototypes. We present our roadmap for building such a quantum key distribution prototype and the current status of the R&D activities undertaken by our collaboration ITIM-UTCN.**

Keywords—quantum key distribution, quantum communications, quantum networks

I. Introduction

Quantum cryptography [1] is poised to revolutionize internet and communications by offering unconditionally secure means to transfer data. Since the seminal paper of Bennet and Brassard [2,3], it has been known that transmitted data, encoded in the degrees of freedom of quantum particles, can be immune to interception as long as the transmission follows a quantum communications protocol [2,4] and proper error correction is performed.

The increased digitalization of our society has raised the economic output of our society, and the standard at living, but, at the same time, has led to new threats to society such as the cybercrime and cyberterrorism. These threats cost the economies worldwide hundreds of billions [5] and various security solutions are sought to mitigate them. Employing quantum cryptography in quantum communications networks is one of the most attractive solutions due to its unconditional security.

In quantum cryptography, a cryptographic key is generated using a physical process which yields true random numbers. Quantum random number generators [6] are relatively inexpensive to make and there already are some very good such products on the market. They are employed both in quantum and classical cryptography. Once the random key is obtained, it has to be shared between the users in the quantum network. The sender (Alice) encodes the bits of this random key in the degrees of freedom of a quantum particle (most commonly a photon), and send it to the receiver (Bob). There are various quantum key distribution protocols developed to securely transmit the cryptographic key in the network and to prevent an eavesdropper (Eve) to intercept the information encoded in the photons. The attacker is prevented by the rules of quantum mechanics to copy eventual intercepted quantum information (qubits) to their own device. Additionally, a quantum measurement performed on a photon carrying information is bound to change its quantum state, which means the attack is likely to be detected by the network users.

While the principles of quantum key distribution (QKD) are well understood, engineering QKD devices capable of transmitting information over large distance is quite a challenge. The main issues are QKD vulnerability to noise which limits the transmission distance and the quantum key rates, and the difficulty of building quantum repeaters which would remove the distance limitations. Nonetheless, QKD research continues to be top priority for both governmental and private research labs due to the interest from both civil (banks, internet and telecom companies) and governmental actors (military, diplomats, etc.).

Over the last few decades, many quantum networks have been built [7] in order to set the stage for a future quantum internet [8]. Among those quantum networks, we mention the DARPA network [9], the SECOCQ network [10], Tokyo network [11], etc. More recently, China has unveiled its integrated space-to-ground quantum communication network [12] that spans over 4600 km and has a space link via China's quantum communications satellite Micius.

These developments were made possible by a sustained investment of many governments in R&D programs spurred by the increasing need for cybersecurity solutions. Quantum communications has become a topic of national interest and most countries are actively trying to develop their own products and networks in order to reduce the dependence on foreign solutions.

978-1-6654-5528-2/22/$31.00 ©2022 European Union

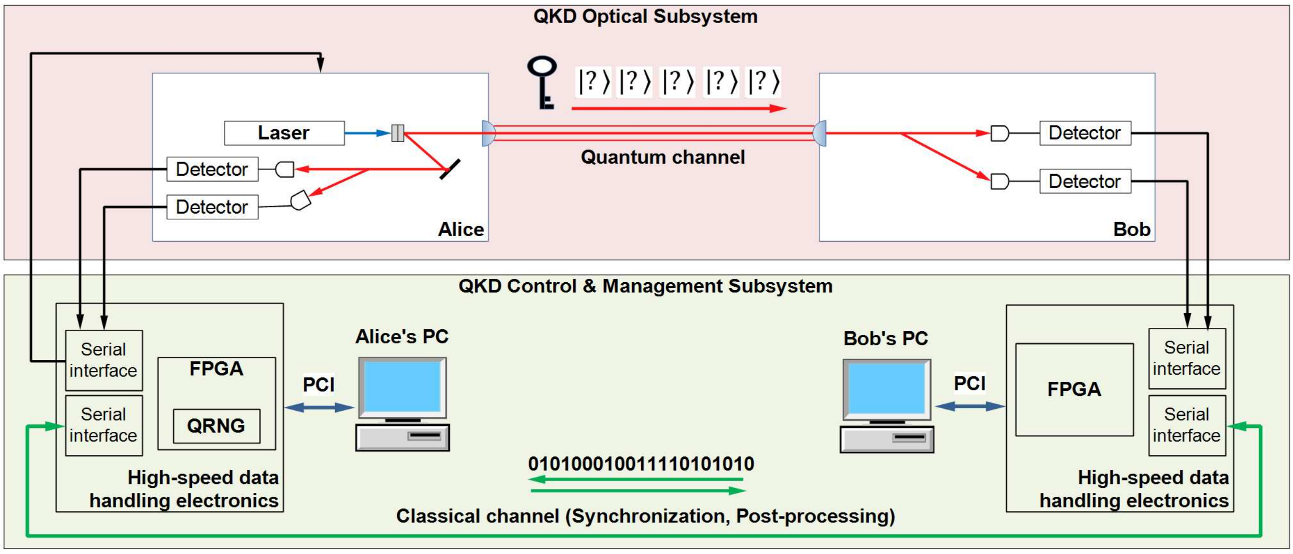

Figure 1 General architecture of our QKD solution.

In this context, our research collaboration is working on developing its own QKD device. Such device is meant to use only commercially available off-the-shelf components. In the following sections, we will discuss our planned steps for building such a device and present some of our results related to calibrating the photon source.

A typical QKD device has a quantum layer, where the quantum key data is generated, a classical layer, for management and control, and a software layer. The quantum layer consists in optical circuitry, photon sources and detectors, and devices for quantum random number generation. The classical layer consists of acquisition electronics, and synchronization electronics for raw key generation and extraction. The software layer processes the key information, and uses the key to encrypt the data exchanged by the two parties. In the next section, we will discuss in more detail the plans for building our device.

II. QKD Device Overview

The quantum communication link between Alice and Bob consists of two communication channels: (1) a quantum channel used to transport quantum bits from the physical quantum source (Alice) to the physical quantum receiver (Bob), and (2) a classical channel (for control & management of the QKD protocol). Thus, the QKD system consists of an optical subsystem for transmitting the quantum information and a control and management subsystem for channel synchronization and key extraction, as shown in Fig. 1. The QKD control & management subsystem controls the optical components (e.g., laser, polarizer, detectors) and establishes a classical channel between Alice and Bob to implement the QKD protocols and post-processing procedures.

The control & management system handles the channel synchronization. The synchronization between Alice and Bob is necessary to execute the QKD protocols and extract a key from the transmission. This key is not final, so additional postprocessing steps are necessary to correct errors and eliminate the possibility of eavesdropping.

A. The optical subsystem

The optical layer shown in Fig. 2 consists of two optical setups, for both Alice and Bob. The key component is the

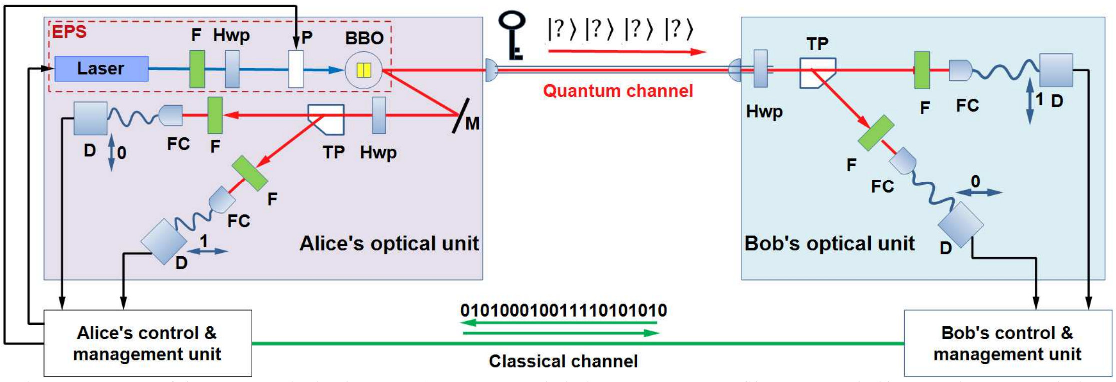

Figure 2 Main components of the QKD optical subsystem (EPS = entangled photon source, F = filter, Hwp = half-wave plate, P = polarizer, BBO = non-linear crystal, M = mirror, TP = Thompson prism, FC = fiber collimator, D = detector).

entangled photon source (EPS): a 405 nm continuous wave (CW) laser that undergoes spontaneous parametric down conversion (SPDC) in a non-linear crystal to produce entangled photon pairs at 810 nm. The photon pairs at nearly the same energy will follow two non-collinear paths and reach identical detection setups (band-pass filters and fiber-coupled detectors). The photon pairs are used to detect „coincidences” (pulses from Alice and Bob that arrived within tens of nanoseconds). Most of the necessary equipment for the QKD optical subsystem is already available at INCDTIM: dark room, optical table, optical and optomechanical components, detectors, electronics (FPGA), and computers. For the QKD implementation we will add two detectors (SPCM-AQRH-12-FC, Excelitas), two Thompson prisms (or alternatively two beam splitters), and two half-wave plates for polarization control.

In our planned implementation, entangled photon pairs are generated by Alice using a beta barium borate nonlinear crystal (BBO) via SPDC process. To encode information in these photons, we can polarize them (e.g., vertical-horizontal, representing logical 0 and 1). But photon polarization can be vulnerable to noise. Alternatively, we can use time bin encoding. In this case, a photon being sent from Alice, within a certain interval of time is considered a “1”, and the event in which the photon is not sent in that time interval is considered a “0”.

Each transmission of the cryptographic key consists in a data stream encoded in single photons. The detectors of Alice and Bob register counts every time a photon reaches them. One needs to be able to i) send well-defined single photon packages, ii) differentiate them from the noise, or “dark counts”, iii) know if Bob’s detected photon is the same sent by Alice, or not. To be able to do this, Alice and Bob must be able to share the same clock, which is used to synchronize the transmission. All the necessary operations for channel synchronization can be handled by an Arduino, or an FPGA controller – see Section C for more details. The next section discusses how to perform the photon counting necessary for the QKD transmission.

B. Photon Counting

A key element of the QKD technology is the ability to produce and detect laser pulses with controlled number of photons. Moreover, this number should be close to unity in order to encode and transmit specific quantum states.

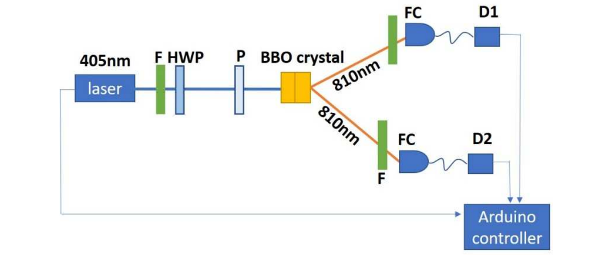

Figure 3 Experimental setup for controlled production and counting of photons by down-conversion. F-filter, HWP-half waveplate, P-polarizer, FC-fiber collimator, D-detector

Two approaches can be taken to reach this goal. The first one is to filter the number of photons by using mechanical devices (e.g., pinholes) or physical properties, such as polarization. A second one is to use sources with intrinsic low efficiency in photon production. The example here is the down-conversion process. In our case, the use of a BBO crystal and a radiation of 405 nm leads to photons with wavelength of 810 nm that are produced at a rate of about 10^{-10} [13]. In other words, by using an incident laser beam of 10 mW, we get a power of the converted flux of photons close to pW domain.

Such a source is a good candidate for QKD applications since a pulse with length of order of microseconds will reach the condition mentioned above (i.e.to include a number of photons close to one photon/pulse). Moreover, the photons generated in down-conversion experiments represent a source of entangled photons, opening the possibility for further applications.

The two detectors D1 and D2 collect the photons at 810 nm produced in the down-conversion process. The model used is Excelitas SPCM AQRH-12 FC, with a dark count around 150 counts/sec and a latency period of 30 ps.

The module for control of time-length of the pulse as well as the counting module for the photons are realized in our laboratory, using an Arduino Mega and a digital counting circuit. The photons are emitted in pulses with controlled length in the same period of time with their counting, then the process is repeated. We used series of 10000 sequences of pulse counting experiment and performed statistical analysis

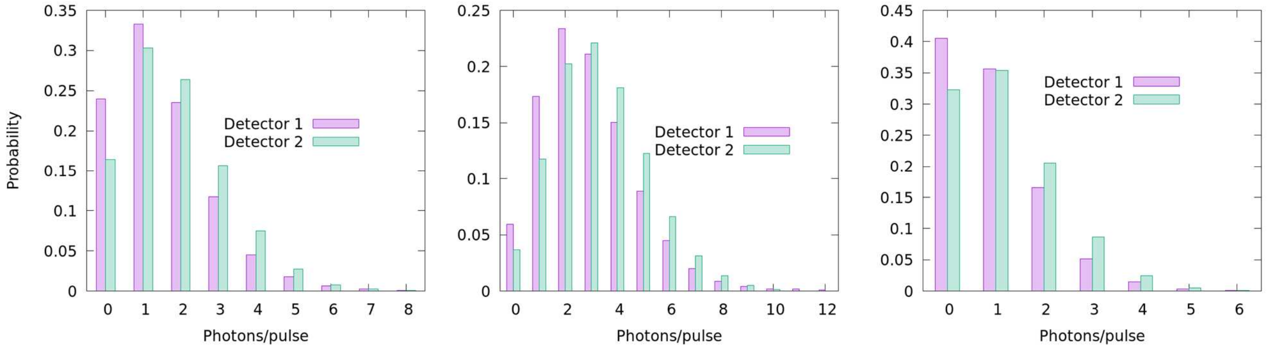

Figure 4 Statistical distribution of photon probability collected by each of the detectors D1 and D2 for different lengths of the laser pulse: from left to right T=25, 50 and 100 microseconds, respectively. We note that the average number of photons/pulse can be controlled by increasing/decreasing the pulse period. Note that for a pulse of about 25-50 microseconds the average number of photons is close to 1.

of the results. Precisely, we count the number of pulses with 0, 1, 2, … photons and divide it by 10000 to get the distribution probability for each number of photons/pulse.

Average	P(N=0)	P(N=1)	P(N=2)
0.8	0.449	0.359	0.143
1.5	0.223	0.334	0.251
2.5	0.082	0.205	0.256

Table 1 Table 2 Calculated distribution probability for a binomial scheme with a total of 10000 events and the average values indicated in first column (i.e., close to the average values for detector D1+D2 in Figure 4) for N=0,1 and 2.

The statistical information is related to the probability distribution of the emitted photons. Constant probability will lead to a Poissonian distribution of photons, while sub-Poissonian and super-Poissonian distributions are indications of bunching/antibunching of photons (i.e., time or space correlation of probability distribution for photons).

The results for different time-length of the pulses are summarized in Figure 2. The corresponding probability to get 0, 1, or 2 photons per pulse for binomials distribution (i.e., Poissonian distribution in the limit of small averages of the distribution) are summarized in Table 1. It can be seen that the numbers are very close to those obtained in our experimental counting, indicating that the sources are Poissonian. Moreover, the average number of photons per pulse can be controlled by tunning the period of the pulse.

C. *The control & management subsystem of the QKD system*

To provide high computational speed and implementation flexibility, the envisaged control & management subsystem for photon counting was implemented on a National Instruments (NI) dedicated platform.

The NI PXIe-1082 chassis` slots are loaded with an NI PXIe-8880 embedded controller, that runs LabVIEW/LabVIEW FPGA software and implements the QKD post-processing procedures, and two NI PXIe-7976 FlexRIOs for FPGA processing. Two NI USRP 2954R Software Defined Radios (SDRs) are also connected to the chassis and commanded by the PXIe-8880 controller. T

The USRPs are used for encrypted data transmission via an IEEE 802.11 wireless link. The NI CDA-2990 Octoclock provides 10MHz and 1PPs time and frequency reference signals for the USRPs synchronization. For proper and timely implementation of the necessary procedures, the development of this subsystem makes use of an emulated quantum channel.

The NI infrastructure has been successfully employed in the development of several SDR-based solution such as direction finding [14], beamforming [15] or intra-satellite communication [16,17]. Figure 5 illustrates the architecture of the QKD control & management subsystem customized for the implementation of the BB84 protocol [2].

D. *Extracting the quantum key from the transmitted signal*

To extract a cryptographic key from the optical transmission, one needs to perform a series of steps, as shown in Fig. 6. These steps allow Alice and Bob to have identical keys, without losing information to a third party.

BB84 protocol encodes every bit of the secret key into the polarization state of a single photon. The typical QKD implementation, assumes Alice sends the key to Bob, while an adversary, Eve, tries to intercept the data. The information

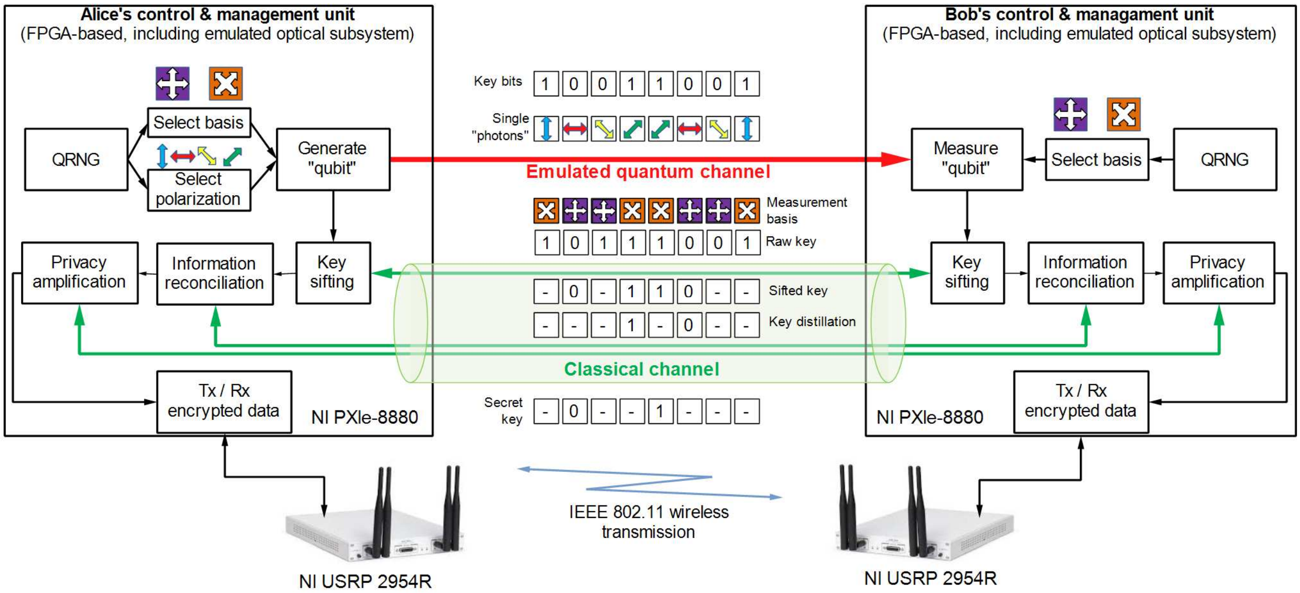

Figure 5 Main components of the QKD control & management subsystem.

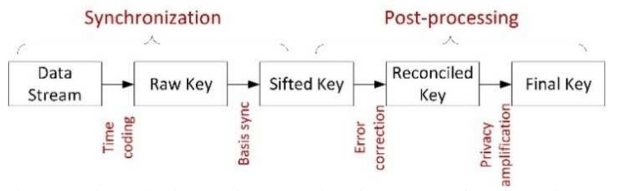

Figure 6 The typical steps for extracting the quantum key from the optical signal.

sent by Alice is encoded in the variables (i.e., polarization) of a stream of photons that are sent over the quantum optical channel. Alice generates two random bits for each photon she sends to Bob: the first bit determines the basis to be used: horizontal-vertical (H, V) or diagonal (+45º, -45º) and the second bit determines the polarization of the photon to be transmitted (e.g., (0, 1) = (H, V), or (0, 1) = (+45º, -45º)). For each incoming photon Bob generates a random bit to determine the measurement basis and records whether or not a photon arrived and its polarization. Bob is able to detect the photons sent by Alice, as long as the clock of his detectors is synchronized with the clock of Alice's laser. Once Alice finishes the transmission of her data stream, Bob will have a sequence of bits, named raw key.

The next step is the key sifting, in which Alice sends Bob, over a classical channel, the information regarding the basis used for each generated qubit. For the sifted key, Bob will retain only the bits with coinciding basis, while discarding the others. The sifted key may still contain errors (as a result of Eve's interference, noise and loss), which must be corrected during an information reconciliation (or key distillation) phase. First, Alice and Bob must obtain a reconciled key, which is identical for both. This can be done for example, following the cascade protocol [18]. As an example, Bob can divide the sifted key into subsets, and calculate their parity, which can be sent to Alice for verification over the post processing channel. Every subset with the wrong parity can be further divided until and the procedure repeated, until the faulty bits are found and discarded. The result is a reconciled key, which is identical for Alice and Bob. The reconciled key contains information known only to Alice and Bob, plus the information intercepted by Eve. It is assumed that Eve's information contains everything that has been transmitted over the classical channels (detector orientation, parity of key subsets, etc.), plus some of the information that Eve obtained intercepting photons sent by Alice. There are proven [19] privacy amplification procedures used to extract the final cryptographic key from the reconciled key, containing a negligible amount of information known to Eve. Alice and Bob may eliminate a certain number of bits from the reconciled key, bit 1, 5, 8, etc., until Eve's information regarding the key is negligible [19].

III. Conclusions

In conclusion, we have presented our planned steps for building our own quantum key distribution device. The device optical and electronic control & management subsystems were presented. We also presented some results related to the testing of the optical subsystem, to ensure that the optical transmission is reliable and reproductible. The plan is to finalize the optical subsystem, and then implement a full control & management system. Once the optical table setups are sufficiently tested, we plan on miniaturizing the optical setup, rebuilding our electronic interfaces as discussed in Sec. IIC, and build a first version of our QKD device(s), as described in the previous section. Finally, the key extraction algorithms will be implemented to allow the device to yield a ready-to-use quantum key.

Acknowledgements

T.M., C.M., and L.P.Z. acknowledge the Romanian National Authority for Scientific Research and Innovation, UEFISCDI for funding through the project Quantum Computation with Schrödinger cat states, contract ERANET-QUANTERA QuCos 120/16.09.2019.

References

[1] S. Pirandola, U.L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J.L. Pereira, M. Razavi, J.S. Shaari, M. Tomamichel, V.C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in Quantum Cryptography," *Adv. Opt. Photon.*, vol. 12, Dec. 2020, pp. 1012–1236.

[2] C.H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, India: 1984, p. 175.

[3] C.H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Theoretical Computer Science*, vol. 560, Dec. 2014, pp. 7–11.

[4] A.K. Ekert, "Quantum Cryptography Based on Bell's Theorem," *Phys. Rev. Lett.*, vol. 67, Aug. 1991, pp. 661–663.

[5] "New McAfee Report Estimates Global Cybercrime Losses to Exceed $1 Trillion | McAfee, LLC."

[6] M. Herrero-Collantes and J.C. Garcia-Escartin, "Quantum Random Number Generators," *Rev. Mod. Phys.*, vol. 89, Feb. 2017, p. 015004.

[7] S.-H. Wei, B. Jing, X.-Y. Zhang, J.-Y. Liao, C.-Z. Yuan, B.-Y. Fan, C. Lyu, D.-L. Zhou, Y. Wang, G.-W. Deng, H.-Z. Song, D. Oblak, G.-C. Guo, and Q. Zhou, "Towards Real-World Quantum Networks: A Review," *Laser & Photonics Reviews*, vol. 16, 2022, p. 2100219.

[8] S. Wehner, D. Elkouss, and R. Hanson, "Quantum Internet: A Vision for the Road Ahead," *Science*, vol. 362, Oct. 2018, p. eaam9288.

[9] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current Status of the DARPA Quantum Network," *Proc.SPIE*, 2005, pp. 138–149.

[10] 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 J. Phys.*, vol. 11, Jul. 2009, p. 075001.

[11] 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, May. 2011, pp. 10387–10409.

[12] 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, Jan. 2021, pp. 214–219.

[13] P.G. Kwiat, E. Waks, A.G. White, I. Appelbaum, and P.H. Eberhard, "Ultrabright Source of Polarization-Entangled Photons," *Phys. Rev. A*, vol. 60, Aug. 1999, pp. R773–R776.

[14] B. Rares, C. Codau, A. Pastrav, T. Palade, H. Hedesiu, B. Balauta, and E. Puschita, "Experimental Evaluation of AoA Algorithms Using NI USRP Software Defined Radios," *2018 17th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, 2018, pp. 1–6.

[15] C. Codau, B. Rares, T. Palade, A. Pastrav, P. Dolea, R. Simedroni, and E. Puschita, "Experimental Evaluation of a Beamforming-capable System Using NI USRP Software Defined Radios," *2019 18th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, 2019, pp. 1–6.

[16] R.-C. Buta, B.S. Kirei, C. Codau, A. Pastrav, C. Farcas, R. Simedroni, P. Dolea, T. Palade, and E. Puschita, "Design and Validation of a SpW Converter for Intra-Spacecraft Communications," *2021 44th International Conference on Telecommunications and Signal Processing (TSP)*, 2021, pp. 381–385.

[17] C. Cod au, A. Voina, A. Pastrav, T. Palade, E. Puschita, H. Hedesiu, and C. Chirap, "Experimental Evaluation of the IEEE 802.11ac Standard Using NI USRP 2954R," *2017 16th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, 2017, pp. 1–6.

[18] G. Brassard and L. Salvail, "Secret-Key Reconciliation by Public Discussion," Springer-Verlag, 1994, pp. 410–423.

[19] C.H. Bennett, G. Brassard, C. Crepeau, and U.M. Maurer, "Generalized Privacy Amplification," *IEEE Transactions on Information Theory*, vol. 41, Nov. 1995, pp. 1915–1923.