IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12527

QUANTUM COMMUNICATION

Arshitha G[1], Shwetha V[2]

ECE Dept. SJCIT, Chikballapur[1]

Assistant Professor, SJCIT, Chikballapur[2]

Abstract: Quantum communication is built on a set of disruptive concepts and technologies. It is driven by fascinating physics and by promising applications. It requires a new mix of competencies, from telecom engineering to theoretical physics, from theoretical computer science to mechanical and electronic engineering. First applications have already found their way to niche markets and university labs are working on futuristic quantum networks, but most of the surprises are still ahead of us. Quantum communication, and more generally quantum information science and technologies are here to stay and will have a profound impact on the twentieth century. Hence, this technology plays a vital role in modern day communication.

I. INTRODUCTION

The Quantum Communication enjoys an enviable position in physics, in between fundamental quantum mechanics and applied quantum optics [1]. For most physicists, quantum communication is merely a playground to explore fascinating topics like entanglement, superposition of large objects, and, more generally, to look for places where quantum physics may fail, that is to explore the limits of quantum physics. This playground requires new technologies and concepts. Usually, new technologies are driven by applications and quantum communication is no exception: the emerging and future technologies are driven by the need for

1. Fast Quantum Random Number Generators (QRNG): from cryptography to internet lotteries and gaming.
2. Reliable fiber-based Quantum Key Distribution (QKD): for today's cryptography applications.
3. Quantum repeaters: for future continental scale fiber optic quantum communication.
4. Earth to satellite links: for free space quantum communication.

Quantum communication is a method of transmitting information through the use of quantum mechanical principles, such as entanglement and superposition. Unlike classical communication, which is limited by the laws of physics, quantum communication provides a means of secure communication that is immune to interception or eavesdropping. Quantum computers excel at complex problem solving. The unique properties of qubits let them solve certain classes of problems faster and more efficiently than traditional computers. Quantum technology is advantageous for materials science, pharmaceutical research, subatomic physics, and logistics. he growth of modern technological sectors have risen to such a spectacular level that the blessings of technology have spread to every corner of the world, even to remote comers. At present, technological development finds its basis in the theoretical foundation of classical physics in every field of scientific research, such as wireless communication, visible light communication, machine learning, and computing. The performance of the conventional communication systems is becoming almost saturated due to the usage of bits. The usage of quantum bits in communication technology has already surpassed the limits of existing technologies and revealed to us a new path in developing technological sectors. Implementation of quantum technology over existing system infrastructure not only provides better performance but also keeps the system secure and reliable. This technology is very promising for future communication systems. This review article describes the fundamentals of quantum communication, vision. design goals, information processing, and protocols. Besides, quantum communication architecture is also proposed here. This research included and explained the prospective applications of quantum technology over existing technological systems, along with the potential challenges of obtaining the goal.

II. LITERATURE SURVEY

[1] 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, Bangalore, India, 2004, pp. 175-179

The above said research paper provides a keen information on the principles of quantum cryptography concepts. It states that the quantum cryptography is a method of encryption that uses the naturally occurring properties of quantum mechanics to secure and transmit data in a way that cannot be hacked and its further processes.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.12527

[2] Artur Ekert, "Quantum cryptography based on Bell's theorem," Physical Review Letters, vol. 67, no. 6, pp. 661-663, 1991.
This research journal states the Bell's theorem usage in the concept of quantum cryptography communication. The theorem determines that quantum mechanics is incompatible with local hidden-variable theories given some basic assumptions about the nature of measurement and its intellectual studies are explained in the said paper.

[3] Xiao-Qiang Shao, Fei Gao, and Yong-Yi Mao, "A review of quantum key distribution protocols," Quantum Information Processing, vol. 15, no. 11, pp. 4357-4373, 2016.
The research paper provides the abstraction of quantum key distribution technology in the real-world applications. It defines that quantum key distribution is a key establishment protocol which creates symmetric key material by using quantum properties of light to transfer information from Client A to Client B in a manner which, through the incontrovertible results of quantum mechanics, will highlight any eavesdropping by an adversary and computes the solutions.

[4] K. Banaszek and I. A. Walmsley, "Photon counting in quantum optics," Progress in Optics, vol. 46, pp. 223-331, 2019.
The above research journal states the technology of photon detection and computational methods in the field of ray optics and many more. It depicts that photon counting is a technique in which individual photons are counted using a single-photon detector. The counting efficiency is determined by the quantum efficiency and the system's electronic losses and proves it.

III. BLOCKDIAGRAM AND DESCRIPTION

A basic idea of quantum communication is to take advantage of the oddities of quantum physics, like the uncertainty relation, the superposition principle and randomness. Note the conceptual revolution: instead of being afraid of quantum peculiarities and trying to avoid their detrimental effects for standard technologies, the new generation of quantum engineers aim at exploiting the new physics. In particular they fully admit quantum physics as it stands and want to find original uses for its most counter-intuitive features. It is somewhat surprising, and disappointing that it took six or seven decades before realizing that this new physics ought to produce new technology. One might argue that the laser, semiconductors, superconductivity, among others, are technologies based on quantum physics. However, the big difference with quantum communication and more generally with quantum information science and technology - is that it exploits quantum physics at the level of individual quanta. The simplest example is the quantum random number generator. Since the detection of a single photon after one of the two output ports of a beam splitter is an intrinsically random event, it offers a valuable source of randomness, see Figure 1. Moreover, according to today's physics, such a source of randomness is unique: no device based on classical physics will ever produce true randomness, only at best "pretty good" pseudo-random numbers, or noise, whose origin is hard to fully identify. Yet, engineering a photon source, beam-splitter and two CMOS-based single-photon detectors is not that complex: the existing commercial QRNG is about the size of a match-box. Unlike, classical communication, which is limited by the laws of physics, quantum communication provides a means of secure communication and hence behaves hypothetically aligned with the photon's theories.

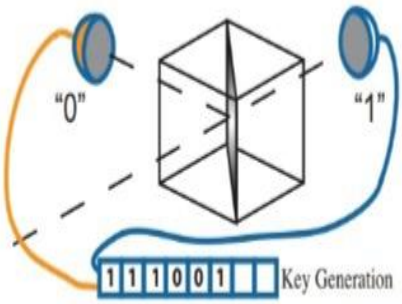

FIG. 1: Quantum random number generation - one single photon at a time is sent to a 50/50 beam splitter and can only exit in one of the output modes. This process is fundamentally random and the photon's detection is used to the generate truly random bit strings.
Another example, whose basic principle is rather straightforward, is QKD [3]. Every first-year quantum physics student knows that measurements tend to unavoidably disturb the quantum state of the system under investigation. This has

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.12527

puzzled generations of students and professors. Now, if this ”negative fact” is applied to an adversary, like a spy on a communication channel where the bits are carried by quantum systems, like photons, then it is the spy who can’t measure the bits without unavoidably leaving a trace of her intrusion under the form of some disturbance. Again, the reasoning is so simple that one wonders why no student came across that idea long ago (or did their professor tell them to shut-up and compute?). Thus, while QRNGs generate randomness, QKD provides a means of distributing private (secure) randomness.

Further presentation of what quantum communication is and how it relates to entanglement and other quantum oddities can be found, e.g., in [1]. In the following we concentrate on future technology challenges. Near-Future Technologies: The most advanced applications of quantum communication are clearly QRNG and QKD. The first was initially developed as a component of the second. It was originally thought that QRNG would also find applications in classical cryptography and in Monte-Carlo numerical simulations. QRNG did find some application in classical cryptography (e.g., the state of Geneva uses QRNG to produce the pin-codes used for internet voting), but by far the largest application came as a surprise: internet gambling for which it has now been certified by Metas [4] This is a good example that applications of new technologies are hard to predict (physicists are especially bad at predicting good commercial applications!). QRNG development is a timely topic, but any approach should concentrate on three key requirements:

1. Origin of randomness easily identifiable. One should be able to quantify how much randomness is truly quantum and how much is ”technological noise”, e.g., thermal noise, detector noise, etc.
2. Reliability, size and price. There is no fundamental reason for a QRNG not to be as small and cheap as a standard electronic chip.
3. Fast, in particular faster than classical, physical, RNG. The minimal rate of future QRNG should be in the range of hundreds of Mbps to Gbps. Present QKD systems are mostly based on the historical BB84 protocol [5] (with some improvements like SARG [6] and Decoy-state [7–10]). However, better protocols have been invented in the context of fiber networks [11, 12] . It should be understood that BB84 originally was described using polarization encoding, which is intuitively easy to understand, though in practice most real systems use some type of phase encoding that is more compatible with fiber optical systems. Despite these advances, the best QKD protocols have probably not yet been discovered. In any case, the protocol should use telecom photons (i.e. around 1550 nm), be compatible with standard optical fiber networks and combine them with the necessary quantum features to guarantee ”quantum security”. This requires synergy between telecom engineers and quantum theorists. Most technology developments on QKD concentrate on single-photon sources and on detectors [13]. However, somewhat surprisingly, single-photons are not required for QKD: it is much easier to use so-called pseudo single-photon sources, i.e., strongly attenuated pulsed lasers. These are cheap, very reliable and fast (GHz rates). Note however, that single-photon sources could find their application in quantum repeaters [14], see below. Improving single-photon detectors, on the contrary, is a real must. The best detectors in terms of efficiency are superconductor bolometers, though these are prohibitively slow and operate at a few millikelvin [15]. QKD applications need cheap, compact, electronically cooled detectors. Today this is achieved with semiconductor detectors (InGaAs APDs) though their performance and functionality need to greatly improve. The APDs need to have lower dark count rates and ”after pulsing” [16], which can introduce errors on the key. Furthermore, one of the most important characteristics of single-photon detectors, that is too often neglected, is the maximum count rate. Future QKD systems will need to generate several Mbps of secure keys.

Some physicists speculate that QKD systems using not-so-weak laser pulses and homodyne detection, continuous variable (CV) QKD [17], will outperform single-photon schemes. They argue that, contrary to single-photon schemes, homodyne detection always produces a result. This is correct, though the results are necessarily very noisy. We expect that it is more efficient to let Nature select the cases with low noise, i.e. the cases where a single-photon is detected, rather than to always have a noisy result, where the noise has then to be removed by sophisticated error correction algorithms. Furthermore, for long distances the not-so-weak laser pulses tend to become pseudo-single-photon and the difference between the two systems vanishes. But, admittedly, the future will show us the truth with possibly both systems finding their niches.

An increasingly important requirement for future QKD schemes is that they run on the same fiber as the classical channels (both the classical processing and encrypted data channels). This is a serious challenge as the intensity difference is huge: 8 to 9 orders of magnitude. Hence, Raman scattering and other nonlinear effects have to be taken into account: even microwatts can produce enough photons to impair the quantum communication; recent efforts suggest that multiplexing quantum and classical channels in a fiber is limited to around 50 km [18] with current technology. A serious push towards network compatibility can also be witnessed by the number of QKD test beds running or planned worldwide. In 2008 in Vienna the European consortium SECOQC demonstrated a mix of different QKD systems running in a complex network [19]. A triangular network has been running continuously in Geneva (data available in real time at www.swissquantum.com) since April 2009. In Durban, South-Africa, yet another net-work runs continuously carrying

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.12527

real data and in October 2010 a large network will commence operation in Tokyo, while others have been announced for Madrid and China. Another sign of the maturing of QKD is the appearance of quantum hackers. They do not attack the principle on which QKD relies, as this is provable secure, but take advantage of implementation weaknesses [20-22]. The latter can, and have to be, tested and strengthened, rendering QKD more and more reliable.

The rate of future QKD systems will be such that true Mbps one-time pad encryption should be possible over metropolitan networks. This is including all the real-time classical processing, communication and network overheads. It will thus be the result of an interdisciplinary team of engineers.

IV. APPLICATIONS

1) Enhanced Secure Computations: Quantum communication offers an extremely high level of security that cannot be violated by hackers, ensuring the confidentiality and integrity of sensitive information.
2) Cryptography: Quantum cryptography is used for encrypting and decrypting data, making it extremely difficult for cyber criminals to intercept or tamper with.
3) Teleportation: The ability to teleport quantum information between locations using entangled particles allows for faster and more secure communication compared to traditional means.
4) Quantum key distribution: Quantum key distribution can be used for generating shared secret keys, which can then be used for symmetric encryption to secure communication.
5) Quantum random number generators: Quantum random number generators can be used for generating truly random numbers, which are difficult to predict, making them useful for cryptography and data security.
6) Quantum sensing: Quantum sensors can be used for detecting and measuring the smallest changes in physical parameters, such as temperature or magnetic fields, allowing for more accurate and efficient communication.
7) Quantum computing: Quantum communication is an integral part of quantum computing, which is expected to revolutionize computing and communication technology with its ability to solve complex problems faster than classical computers.
8) Satellite-based communication: Quantum communication can be used for secure satellite-based communication, which has applications in areas like national defense, disaster management, and remote sensing.

V. CONCLUSION

Over the past few decades, the applications of classical theories and principles have led the technological advancement in communication systems almost to its edge. Fascinating and innovative features are added to communication systems to overcome ongoing challenges. The way users are increasing, it can be easily predicted that even the technological development in 6G communication network systems cannot fulfill the growing demands and network security in the future. For this reason, to think outside of the box, scientists have introduced quantum physics, which has created a new path in modern physics. Scientists are giving hard and soul efforts to establish quantum based technological systems. Nowadays, several experiments are done to develop a shared infrastructure between quantum and classical communication systems.

These technologies play a vital role in health care, space, banking, underwater communication, industry, and transportation. Besides, many other research and experiments are ongoing for the development of the quantum systems. In this review paper, we present definition and mechanism of quantum communication, the vision of quantum communication, difference between classical and quantum communication. This gives a clear overview of different types of implementation in quantum communication and its prospects. Quantum communication design goals and information processing have been demonstrated profoundly.

We proposed quantum communication architecture that clarifies the steps of quantum communication system from transmission to reception end, what will have to keep in mind before designing the system, and the information processing steps in quantum communication. Major QKD protocols functionality and their principles are explained elaborately. Numerous application scenarios are set out for different prospects of quantum technologies such as quantum internet, quantum computing, quantum based satellite communication, quantum underwater communication, and quantum IoT. Moreover, the challenges in quantum communication systems and future research directions are also illustrated. We believe that this review article will serve as a noble resource for comprehending the fundamentals, applications, protocols, and research directions of emerging quantum technology.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.12527

REFERENCES

[1] V. Christianto and F. Smarandache, "A Harmless Wireless Quantum Alternative to Cell Phones Based on Quantum Noise," EC Neurology, vol. 10, no. 11, pp. 942-946, 2019.
[2] S. Mumtaz, J. M. Jornet, J. Aulin, W. H. Gerstacker, X. Dong, and B. Ai, "Terahertz Communication for Vehicular Networks," IEEE Trans. Veh. Technol., vol. 66, no. 7, pp. 5617–5625, 2017.
[3] International Telecommunications Union, "IMT Traffic Estimates for the Years 2020 to 2030," Electron. Publ. Geneva, pp. 1–51, 2015.
[4] F. Tariq, M. R. A. Khandaker, K. K. Wong, M. A. Imran, M. Bennis, and M. Debbah, "A Speculative Study on 6G," IEEE Wirel. Commun., vol. 27, no. 4, pp. 118–125, 2020.
[5] N. Panwar, S. Sharma, and A. K. Singh, "A Survey on 5G: The Next Generation of Mobile Communication," Phys. Commun., vol. 18, pp. 64–84, 2016.
[6] A. Gupta and R. K. Jha, "A Survey of 5G Network: Architecture and Emerging Technologies," IEEE Access, vol. 3, pp. 1206–1232, 2015.
[7] N. Al-Falahy and O. Y. Alani, "Technologies for 5G Networks: Challenges and Opportunities," IT Prof., vol. 19, no. 1, pp. 12–20, 2017.
[8] C. Day, "Quantum Computing is Exciting and Important - Really!," Comput. Sci. Eng., vol. 9, no. 2, pp. 104, 2007.
[9] M. M. Wilde and M. H. Hsieh, The Quantum Dynamic Capacity Formula of a Quantum Channel, "Quantum Information Processing," vol. 11, no. 6, pp.1431-1463, 2012.
[10] H. V. Nguyen et al., "EXIT-Chart Aided Quantum Code Design Improves the Normalised Throughput of Realistic Quantum Devices," IEEE Access, vol. 4, pp. 10194–10209, 2016.
[11] G. Carcassi, L. Maccone, and C. A. Aidala, "Four Postulates of Quantum Mechanics are Three," Phys. Rev. Lett., vol. 126, no. 11, pp. 1–10, 2021.
[12] S. M. Barnett, "Quantum Information," Oxford Univ. Press, 2009.
[13] T. Varga and L. Bacsardi, "Efficient Simulation of Quantum Based Searching," in Proc. of 22nd Int. Conf. Software, Telecommun. Comput. Networks, SoftCOM 2014, pp. 403–407, 2011.
[14] G. Arun and V. Mishra, "A Review on Quantum Computing and Communication," in Proc. of 2014 2nd Int. Conf. "Emerging Technol. Trends Electron. Commun. Networking", ET2ECN 2014, pp. 1–5, 2014.
[15] T. Curcic et al., "Quantum Networks: From Quantum Cryptography to Quantum Architecture," Comput. Commun. Rev., vol. 34, no. 5, pp. 3–8, 2004.
[16] S. T. Cheng, C. Y. Wang, and M. H. Tao, "Quantum Communication for Wireless Wide-Area Networks," IEEE J. Sel. Areas Commun., vol. 23, no. 7, pp. 1424–1432, 2005.
[17] P. Zoller et al., "Quantum Information Processing and Communication: Strategic Report on Current Atatus, Visions and Goals for Research in Europe," Eur. Phys. J. D, vol. 36, no. 2, pp. 203–228, 2005.
[18] N. Gisin and R. Thew, "Quantum Communication," Nat. Photonics, vol. 1, no. 3, pp. 165–171, 2007.
[19] X. T. Yu, J. Xu, and Z. C. Zhang, "Distributed Wireless Quantum Communication Networks," Chinese Phys. B, vol. 22, no. 9, 2013.
[20] G. Brennen, E. Giacobino, and C. Simon, "Focus on Quantum Memory," New J. Phys., vol. 17, pp. 16–19, 2015.
[21] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A Vision for The Road Ahead," Science, vol. 362, no. 6412, 2018.
[22] S. J. Nawaz, S. K. Sharma, S. Wyne, M. N. Patwary, and M. Asaduzzaman, "Quantum Machine Learning for 6G Communication Networks: State-of-the-Art and Vision for the Future," IEEE Access, vol. 7, pp. 46317–46350, 2019.
[23] A. S. Cacciapuoti, M. Caleffi, F. Tafuri, F. S. Cataliotti, S. Gherardini, and G. Bianchi, "Quantum Internet: Networking Challenges in Distributed Quantum Computing," IEEE Netw., vol. 34, no. 1, pp. 137–143, 2020.
[24] T. Huang, W. Yang, J. Wu, J. Ma, X. Zhang, and D. Zhang, "A Survey on Green 6G Network: Architecture and Technologies," IEEE Access, vol. 7, pp. 175758–175768, 2019.
[25] S. K. Munish Bhatia, Sandeep K. Sood, "Quantum Based Predictive Fog Scheduler for IoT Applications," Comput. Ind., vol. 111, pp. 51–67, 2019.
[26] D. D. Li et al., "Proof-of-Principle Demonstration of Quantum Key Distribution with Seawater Channel: Towards Space-to-Underwater Quantum Communication," Opt. Commun., vol. 452, no. July, pp. 220–226, 2019.
[27] A. Manzalini, "Quantum communications in future networks and services," Quantum Reports, vol. 2, no. 1, pp. 221–232, 2020.
[28] A. Wallucks, I. Marinković, B. Hensen, R. Stockill, and S. Gröblacher, "A Quantum Memory at Telecom Wavelengths," Nat. Phys., vol. 16, no. 7, pp. 772–777, 2020.
[29] S. K. Singh, A. El Azzaoui, M. M. Salim, and J. H. Park, "Quantum Communication Technology for Future ICT - Review," J. Inf. Process. Syst., vol. 16, no. 6, pp. 1459–1478, 2020.
[30] M. Bhatia and S. K. Sood, "Quantum Computing-Inspired Network Optimization for IoT Applications," IEEE Internet Things J., vol. 7, no. 6, pp. 5590–5598, 2020.