IET Quantum Communication

Editorial

IET Journals
The Institution of Engineering and Technology

Inaugural Editorial

eISSN 2632-8925
E-First on 15th July 2020
doi: 10.1049/iet-qtc.2020.0010
www.ietdl.org

Shahid Mumtaz[1] ✉, *Mohsen Guizani*[1] ✉
[1]*Instituto de Telecomunicações, Qatar University, Portugal*
✉ *E-mail: smumtaz@av.it.pt*
✉ *E-mail: mguizani@ieee.org*

Introduction and Importance

The fundamental research of Bennett and Brassard has emerged as a key work when considering the development of the principles of quantum cryptography and communication. The exploration of quantum cryptography is considered one of the supreme visions related to theories of quantum physics to guarantee unconditional security. The unconditional security property is verified by considering the no cloning theory -since the transferred quantum state can't be copied or duplicated. The quantum state can, however, be transmitted. The furthermost applied quantum communication laws are quantum teleportation and dense coding.

The idea of quantum teleportation relies on the quantum state being transferrable among remote users, using both classical communication for maintaining the distribution of measurement outcome, and maximally shared quantum entanglement between remote users. In dense coding, Pauli operations and maximally shared quantum entanglement can be utilised for the transferral of encoded classical information among remote users, since every quantum bit is able to transfer two classical bits.

There are numerous types of protocols and techniques for the development of the quantum laws of physics to guarantee the secured communication for users of environments with two or more participants. Although these techniques employ several approaches for realising a secret transmission between legitimate users, the majority of them rely on generation of a randomised private keys. Currently, there are two procedures for building a quantum-secured communication system. The first is a combined architecture of classical and quantum. The use of encrypting and decrypting algorithms depend on the classical methods, whilst the employed keys for message encrypting and decrypting, which operate as key function in the cryptographic system, are obtained from a quantum key distribution (QKD) protocol. The second approach is performed in an entirely quantum cryptographic system according to the laws of quantum mechanics. In this situation, the encrypting, decrypting and keys algorithms are derived from quantum principles. Furthermore, the transmission of quantum information is denoted by a quantum state, which can be pure or mixed.

Recently, many research groups are working on expanding the power of quantum communication to reach longer distances. Optical communication systems are the perfect technology to achieve the characteristics of quantum communication across long distances, because they have the ability to interact with the surrounding environment and keep the speed at a high rate. The most two popular approaches for distributing the photons between remote users are via fiber optics or via free-space. In fiber optics, the photons of the entangled pair have been distributed and shared over 50 km. The same approach has been employed by various systems to investigate a Bell inequality test that blocked the locality loophole. On the other hand, the technology of free-space provides another inspiring way to form a quantum channel in the case where there is a direct link between the communicating parties. To transmit light through longer distance across the air, at least a transmitter and a receiver telescopes are required. The BB84 is implemented over a distance of 23.4 km by combining free-space links with weak laser pulses. The theoretical research has been demonstrated that the quantum communication can be expanded until around 100 km in the case of using the fiber optic, prior to the attenuation overcoming the signal strength. Similarly, free-space deteriorates from weakening in the atmosphere as a result of scattering and from atmospheric disturbances, which are ultimately restricted by the curvature of the Earth. Quantum information experiences a weakness which does not exist in its equivalent in classical information, since the encoded classical information can be identified and amplified through the optical network to effectively achieve an enlarging range of optical communication. Unfortunately, the quantum state cannot be accurately amplified according to the no-cloning theory, which causes the fabrication of quantum repeaters as a considerable challenge and a complicated aspect for building the quantum internet. To overcome the distance limit is to combine both free-space and satellite, which would enable us to transmit entangled photons from space to Earth.

Building a quantum internet is a big step to in ensuring the security of the backbone for our communication, since the security of current and upcoming applications and technologies will suffer from the threats of quantum computing and algorithms. Quantum communications have incredible consequences for how we will do business in the future. It will dramatically change how we secure our data, and this will affect our technology infrastructure, which means it will affect everything in our life. The absence of security and loss of confidentiality can have overwhelming consequences, including our day-to-day transactions and transfer of sensitive information. Currently, there are many real-world applications of quantum communication and cryptography, such as banking and financial industries, government and defense, and protecting sensitive data in remote data centers.

Therefore, to address the above challenges in Quantum Communication, we are pleased to promote the new IET Quantum Communication journal as a high-quality and open-access platform for disseminating cutting-edge Quantum research addressing these issues, and to accelerate the adoption of such Quantum technologies in practice. The topics of interest include, but are not limited to, the following domains:

- Quantum Internet
- Quantum Blockchain
- Quantum Machine Learning
- Quantum Cybersecurity
- Post-Quantum Cryptographic Protocols
- Quantum Nanomechanics
- Quantum Optomechanics
- Quantum Secured Direct Communication
- Quantum Communication Protocols
- Quantum Relays and Repeaters
- Quantum Networking
- Quantum Channel Capacities
- Quantum Coding
- Quantum Private Comparison

- Quantum Secret Sharing
- Quantum Delegated Computing
- Quantum Cryptography
- Quantum Key Distribution and beyond
- Cryptanalysis of Quantum Communication Protocols.
- Quantum Error Correction & Modulation
- Quantum Algorithms and Applications
- Entanglement Distillation and Purification
- Experimental Results and Demonstrations
- Prototypes and Testbeds
- Quantum State Preparation
- Modeling and Simulation of Quantum Information Processing Systems
- Quantum Detection and Estimation
- Role of Entanglement in Encoding and Decoding of Information
- Quantum Sensing and Measurements.

The editorial board is organized by Quantum subject areas and consists of world-leading experts in their research domains from internationally renowned universities and organizations. We aim to ensure a rigorous peer-review process for every manuscript that fits the journal's scope. The target submission-to-first-decision time is six weeks.

We welcome and encourage submissions of original research results in these research areas, and also welcome submissions of any original results that may cross disciplines, e.g., Quantum for power systems including communications and networking, artificial intelligence, data analytics, and cyber-physical security and architectures for power systems.

For this inaugural issue, there are five papers selected for publication. They have undergone the peer review process, and we thank the authors and peer reviewers for their timely and important contributions.

The first paper (*Turbo-coded Secure and Reliable Quantum Teleportation*) by Xin et al.; proposed and investigated a secure and reliable quantum teleportation scheme when both classical and quantum channels exhibit errors. The authors found that the security and reliability of the teleportation could be improved when robust turbo codes are employed. The second paper (*Towards a Distributed Quantum Computing Ecosystem*) by Cuomo et al.; provides the reader with an overview of the Quantum Internet as the fundamental underlying infrastructure for the design and the realisation of a distributed quantum computing ecosystem. The third paper (*General upper bounds for distributing conferencing keys in arbitrary quantum networks)* by Stefano et al.; provided the analysis that allows to bound the ultimate rates that are achievable by general multiple-multicast protocols, where N senders distribute N independent secret keys, and each key is to be shared with an ensemble of M receivers. The fourth paper (*Tracking Cryptographic Keys and Encrypted Data Using Position Verification*) by Galambos et al., showed that how a practically secure position verification algorithm–assuming it exists–might be used to track (i.e., repeatedly verify the position) of some unique key or cipher text. Lastly, in the fifth paper by Bahram et al., discussed some of the major practical limiting factors for QKD performance such as Spontaneous Raman Scattering (SRS), Four-Wave Mixing (FWM) and Amplified Spontaneous Emission (ASE).

We would like to thank the authors and reviewers again for their contributions, and welcome new submissions to IET Quantum communication from academic, research, and industrial audiences in all fields of quantum information and computation.

Editor Biographies:

Shahid Mumtaz is an ACM Distinguished Speaker, IEEE Senior member, founder and EiC of IET journal "Quantum Communication," Vice-Chair: Europe/Africa Region-IEEE ComSoc: Green Communications & Computing society and Vice-chair for IEEE standard on P1932.1: Standard for Licensed/ Unlicensed Spectrum Interoperability in Wireless Mobile Networks. He is the founder of two Journals. He has more than 12 years of wireless industry/academic experience. He has received his Master's and Ph.D. degrees in Electrical & Electronic Engineering from Blekinge Institute of Technology, Sweden, and University of Aveiro, Portugal in 2006 and 2011.

He is the author of 4 technical books, 12 book chapters, 220+ technical papers (150+ Journal/transaction, 80+ conference, 2 IEEE best paper award- in the area of mobile communications. Most of his publication is in the field of cybersecurity and network security.

He is serving as Scientific Expert and Evaluator for various Research Funding Agencies. He was awarded an "Alain Bensoussan fellowship "in 2012. He is the recipient of the NSFC Researcher Fund for Young Scientist in 2017 from China.

Mohsen Guizani (S'85–M'89–SM'99–F'09) received the B.S. (with distinction) and M.S. degrees in electrical engineering, the M.S. and Ph.D. degrees in computer engineering from Syracuse University, Syracuse, NY, USA, in 1984, 1986, 1987, and 1990, respectively. He is currently a Professor at the Computer Science and Engineering Department in Qatar University, Qatar. Previously, he served in different academic and administrative positions at the University of Idaho, Western Michigan University, University of West Florida, University of Missouri-Kansas City, University of Colorado-Boulder, and Syracuse University. His research interests include wireless communications and mobile computing, computer networks, mobile cloud computing, security, and smart grid. He is currently the Editor-in-Chief of the IEEE Network Magazine, serves on the editorial boards of several international technical journals and the Founder and Editor-in-Chief of Wireless Communications and Mobile Computing journal (Wiley). He is the author of nine books and more than 600 publications in refereed journals and conferences. He guest edited a number of special issues in IEEE journals and magazines. He also served as a member, Chair, and General Chair of a number of international conferences. Throughout his career, he received three teaching awards and four research awards. He is the recipient of the 2017 IEEE Communications Society Wireless Technical Committee (WTC) Recognition Award, the 2018 AdHoc Technical Committee Recognition Award for his contribution to outstanding research in wireless communications and Ad-Hoc Sensor networks and the 2019 IEEE Communications and Information Security Technical Recognition (CISTC) Award for outstanding contributions to the technological advancement of security. He was the Chair of the IEEE Communications Society Wireless Technical Committee and the Chair of the TAOS Technical Committee. He served as the IEEE Computer Society Distinguished Speaker and is currently the IEEE ComSoc Distinguished Lecturer. He is a Fellow of IEEE and a Senior Member of ACM.