GUEST EDITORIAL

QUANTUM COMMUNICATIONS

Sándor Imre

Paulo Mateus

Péter Nagy

Anton Zavriyev

Join the online discussion group for this Feature Topic here:
http://community.comsoc.org/forums/commag-features-and-series

The main goal of quantum communication is to transfer a quantum state between two geographically separated agents. From a practical and simplistic point of view, this problem can be restated as that of sending a single photon with a particular polarization via, say, an optical fiber connecting the agents. The difference between classical and quantum communications follows from the fact that quantum states are ruled by different physical laws; hence, quantum communications exhibits particular properties not found in its classical counterpart. On one hand, by the laws of quantum mechanics, quantum states can be neither cloned nor modified when observed. On the other hand, it is hard to experimentally generate a particular quantum state, and it is even harder to preserve it. These properties constitute a bottleneck for cheap and robust quantum networks but are essential to address the main applications in mind.

Currently, the most relevant application of quantum communication is security. This follows because it is possible to achieve usable perfect security via a public quantum channel, whereas classically, only computational security is achieved, and under the assumption of several mathematical conjectures. Making quantum communications a practical and usable technology, but keeping it within the theoretical advantages, is a challenge that is being tackled by many researchers. This effort may lead to a new generation of communications technology based on advanced photonics; moreover, it is also boosting other experimental research areas, such as development of quantum memory and quantum computation, linked with nanotechnology, cold atoms, solid state matter, and other fields. Due to the wide range of problems to be addressed, quantum communication is an interdisciplinary field, requiring expertise from different research areas: electrical engineering, physics, computer science, and mathematics.

In this Feature Topic we have selected six articles that cover the practical problems of quantum communication. The first article, "Quantum Communications: Explained for Communication Engineers," written by Imre, introduces motivations of why and how the special phenomena of quantum mechanics can be utilized from a communication point of view. It bridges the classical and quantum world via several simple examples. [Note from Sean Moore, Editor-in-Chief, *IEEE Communications Magazine*: This article was written by Sandor Imre, who is also a Guest Editor for this Feature Topic. The policy of the magazine is that guest editors cannot submit articles to their feature topic. In this case, however, the article was originally submitted to our open call. After reading it, I subsequently contacted Dr. Imre about doing a Feature Topic on Quantum Communications. The article was reviewed independently through the open call process, and then included in this Feature Topic as introductory material. The magazine policy's has not been compromised.]

The backbone of this Feature Topic consists of four articles focusing on the most promising communication application — security guaranteed by encoding to quantum states.

Niemiec and Pach's "Management of Security in Quantum Cryptography" addresses quantum key distribution, the major application of quantum communications. It starts by reviewing the basic BB84 quantum key distribution protocol. Then it discusses how to measure the security of the network and proposes a method to tune the low-level parameters of the network with the security requirements of the end user.

Pinto *et al.*, in "Using Quantum Technologies to Improve Fiber Optics Communication Systems," discuss how quantum technology is improving optical communications in general. It first points out that since each photon is a potential carrier of information, it is in principle possible to drastically decrease the amount of energy used per transmitted bit. The bottlenecks for the current capacity of optical fiber are presented, and its application in security is analyzed from a practical point of view.

The fourth article, from Bacsardi, "On the Way to Quantum-Based Satellite Communication" addresses free space quantum communication via satellites. Quantum communication is not restricted to optical fibers, as it is possible to send photons through free space. The article presents current achievements and challenges: the nanoscale synchronization and high-precision optical devices required. It ends by posing several open questions in the field.

Humble's contribution, "Quantum Security for the Physical Layer," addresses quantum seals, an application of quantum communication orthogonal to quantum key distribution. The main purpose of quantum seals is to monitor whether the physical layer has been compromised. The application scenarios are discussed, and the feasibility of the implementation is analyzed.

We end this Feature Topic with Van Meter and Touch, whose article, "Designing Quantum Repeater Networks," addresses quantum network deployment, especially the major bottleneck of implementation, quantum repeaters. A fundamental aspect of quantum networks is to rely on the composition of link and multihop mechanisms into a coherent system. The article explores quantum networking in terms of fundamental network architecture principles and discusses the differences with its classical counterparts. It presents engineering principles that ensure robust and interoperable communication, and proposes new protocol layers to support quantum sessions.

Finally, we wish to thank all the authors and reviewers who contributed to this Quantum Communications Feature Topic. We would like to express our gratitude to Editor-in-Chief, Dr. Sean Moore for the initiation of this feature topic and his continuous encouragement. Our special thanks go to Ms. Jennifer Porcello for her assistance in preparing the articles for publication in this issue.

BIOGRAPHIES

SANDOR IMRE [SM] (imre@hit.bme.hu) received his M.Sc. degree in electrical engineering from the Budapest University of Technology (BME) in 1993. Next he started his Ph.D. studies at BME and obtained a Dr.Univ. degree in probability theory and mathematical statistics in 1996, a Ph.D. degree in telecommunications in 1999, and a D.Sc. degree from the Hungarian Academy of Sciences in 2007. Currently, he is carrying on his activities as a professor and head of the Department of Networked Systems and Services. He is Chairman of the Telecommunication Scientific Committee of the Hungarian Academy of Sciences. He was invited to join the Mobile Innovation Centre as R&D director in 2005. His research interest includes mobile and wireless systems, and quantum computing and communications. He has made contributions on different wireless access technologies, mobility protocols, security and privacy, reconfigurable systems, and quantum-computing-based algorithms and protocols.

PAULO MATEUS (pmat@math.ist.utl.pt) is an associate professor in the Maththematics Department of Instituto Superior Técnico of Technical University of Lisbon and a researcher from Instituto de Telecomunicações, where he coordinates the Security and Quantum Information group. He obtained his doctorate degree in mathematics in 2001 from the Technical University of Lisbon and was a postdoctoral researcher at the University of Pennsylvania. He was awarded the IBM scientific prize, Portugal, in 2005 for his Habilitation thesis where he showed how to use quantum systems to attack privacy protocols. His research is focused on using quantum resources for security and communication, and he has been author and co-author of around 60 international publications. He has been a Guest Editor of the *Logic Journal of the IGPL* and part of the program committee of several workshops and conferences. He is also a member of the Managing Board of the European Network and the Information Security Agency, and Vice-President of Centro Internacional de Matemática.

PETER NAGY [M] (nagy.peter@hte.hu) received his M.Sc. degree in electrical engineering from the Budapest University of Technology and Economics (BME) in 2000, and his M.B.A. in 2005. Next he started to work for the National Regulatory Authority of Hungary (presently National Media and Infocommunications Authority). He has been involved in many international projects and a liaison with international organizations. He has held more positions in the IEEE Hungary Section (Student Counselor, Industry Relations). He was a main local organizer, patron, or finance chair of WTC 2006, MobileSummit 2007, Networks 2008, WCNC 2009, WMNC 2010, Future Internet Week 2011, and VTC Spring 2011. Since 2000 he is the Managing Director of the Scientific Association for Infocommunications, Hungary (HTE), which is a Sister Society of IEEE ComSoc. His most recent project was to organize IEEE ICC 2013 in Budapest with the support of the Organizing Committee, and was involved in Patronage issues and served as Finance Chair.

ANTON ZAVRIYEV (anton@magiqtech.com) is a vice president of research and development at MagiQ Technologies, where he is responsible for all aspects of company R&D. Since joining MagiQ in 2003, he has published more than 15 research papers and patent applications, and was awarded two patents. Before joining MagiQ he was with Astral Point Communications (later acquired by Alcatel) where he led incorporation of optical amplifiers into Astral Point ON5000 and ON7000 metro nodes and was instrumental in developing the design rules for amplified DWDM networks. Prior to that he was involved in solid state laser development and laser physics research at Q-Peak, Textron Systems, National Research Council of Canada, and Bell Labs. He has authored and co-authored over 40 publications including a book chapter on the behavior of small molecules in intense laser fields. He holds an Eng.Sc.D. degree in applied physics from Columbia University.