Quantum Inf Process (2014) 13:2153–2154
DOI 10.1007/s11128-014-0813-z

EDITORIAL

Introduction to special issue on secure quantum communication

Osamu Hirota · Horace P. Yuen

Published online: 28 August 2014

This special issue on secure quantum communication was proposed to us by Dr. Howard Brandt, then Editor of Quantum Information Processing, and we would like to take this opportunity to commemorate his contributions to quantum physics and quantum cryptography over his many years of service in various roles. We had the understanding that this special issue may be broader in scope than strictly "quantum" and "communication", to include related topics that bear on "secure quantum communication" in one way or another, such as classical noise protocol and quantum bit commitment. A total of twenty-six papers were submitted and twelve were accepted.

Quantum key distribution (QKD) is widely considered the most mature area of quantum information science and especially technology. The typical perception [1] is that long perfect key bits can be generated between two users in the information theoretic sense, in contrast to the unproved complexity-based security of public key cryptography. However, the probabilistic foundation of such claim is shakier than it may first appear and the numerical security levels that can be obtained experimentally and theoretically are far from adequate [2]. We do not go into such dispute in this special issue, but in the paper of Yuen, some physics and systems security issues that have been neglected in the QKD literature are noted. Another case of QKD protocol's

O. Hirota (✉)
Quantum ICT Research Institute, Tamagawa University, Tamagawa Gakuen 6-1-1, Machida,
Tokyo 194-8610, Japan
e-mail: hirota@lab.tamagawa.ac.jp

H. P. Yuen (✉)
Department of Electrical Engineering and Computer Science, Northwestern University, Evanston,
IL 60208, USA
e-mail: hyuen081@gmail.com, yuen@eecs.northwestern.edu

H. P. Yuen
Department of Physics and Astronomy, Northwestern University, Evanston, IL 60208, USA

insecurity is given in the paper of Li, and QKD network's insecurity is studied in the paper of Turkanovic and Holbl.

For comparison with the well-known QKD protocols, the security of a classical physical protocol is developed in the invited paper of Kish and Granqvist, and that of an unusual kind of quantum protocol in the invited paper of Shapiro, Zhang, and Wong. Much experimental results have been obtained in both approaches, some described in the latter paper on the Shapiro scheme. The paper of Kotlicki and Scheuer is of a similar nature with experimental demonstration, but fundamental security analysis is yet to be provided. The paper of Shen, Ma, and Wang gives a novel theoretic scheme, as is the paper of Lou, Yang, She, Niu, and Wang. These papers show that security of key generation is a very complicated and subtle matter. There will no doubt be further refinement and development of these results and applications.

There has been an alternative approach to QKD that employs a shared secret key explicitly for signal set selection for the data communication. It has the advantage that much larger energy signals may be employed, but so far only restricted security proofs have been obtained [3]. The paper by Sohma and Hirota develops such approach for one particularly convenient signaling scheme. The paper by Futami reports recent experimental results on another such approach.

The paper of Abidin and Larsson gives basic results on the security of standard information theoretically secure message authentication from imperfect keys. It points to a major limit on such use of QKD-generated keys [2]. In general, since the QKD key is necessarily imperfect, it is important to examine how the obtainable security level in any application of the key would deteriorate quantitatively, which is not something that can be simply declared from some "universal composition" claim.

Quantum bit commitment is widely considered to have been proved impossible, though more general impossibility proofs keep appearing. For the contrary possibility view, see [4]. In the paper by He, a previous quantum bit commitment protocol is modified and further developed for security and efficiency.

Security is a very serious matter. It is hoped that the papers of this special issue would stimulate the final development and resolution of many security issues for efficient and secure communication.

References

1. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., Dusek, M., Lukenhaus, N., Peev, M.: The security of quantum key distribution. Rev. Mod. Phys. **81**, 1301 (2009)
2. Yuen, H.P.: Essential lack of security proof in quantum key distribution. arXiv:1310.0842 (2013). Also in Proceedings of the SPIE Conference on Quantum Physics-Based Information Security held in Dresden, Germany, Sept 23–24, 2013
3. Yuen, H.P.: Key generation: foundations and a new quantum approach. IEEE J. Sel. Top. Quantum Electron. **15**, 1630 (2009)
4. Yuen, H.P.: An unconditionally secure quantum bit commitment protocol. arXiv:1212.0938 (2012)