International Journal of Optics

Hindawi

Special Issue on

The Limitations and Solutions of Practical Quantum Secure Protocols

CALL FOR PAPERS

Quantum secure protocols allow higher security than classical secure protocols as they are based on the laws of physics instead of the difficulty of solving mathematical problems. They have been researched and developed in both theoretics and experiments. In theoretics, many secure protocols have been designed for quantum key distribution (QKD), quantum secret sharing (QSS), quantum secure direct communication (QSDC), quantum teleportation (QT), quantum secure multiparty computation (QSMPC), and so on. A number of them are proved as theoretic unconditional secure (such as BB84 QKD) or more secure than classical cryptography schemes (such as quantum bit commitment). In experiments, some quantum secure communications have been tested successfully with a long distance, and some quantum cryptanalysis algorithms have ran quickly in the newest quantum computer.

In the process from the theoretical stage to the experimental stage, quantum cryptography schemes have met a lot of technical limitations, such as the imperfect optical source, difficult long-term quantum storage, imperfect detector, and loss and noise in channel. Under these limitations, practical quantum secure schemes have more possible security loopholes and have suffered from some attacks, such as photon number splitting (PNS) attack, Trojan-horse attack, and faked state attack. On the other hand, some solutions, such as decoy states and device-independent method, have been proposed to secure practical quantum secure schemes.

The present special issue aims to attract contributions in all areas of quantum secure protocols and their optical bases, with special focus on the limitations and the opposite solutions.

Potential topics include but are not limited to the following:

- Quantum secure protocols based on optics interferometry
- Quantum secure protocols with continuous variable
- Device-independent quantum secure schemes
- Quantum key distribution (QKD), including both discrete and continuous-variable quantum key distribution systems (CVQKD) and optical transmission technology for CVQKD, especially coherent reception techniques for QAM quantum edgy level
- Quantum secure communication protocols, including quantum secret sharing (QSS), quantum secure direct communication (QSDC), and quantum teleportation (QT)
- Cryptanalysis of quantum cryptography, quantum complexity theory, and quantum algorithms
- Quantum communication network, including practical optical networks, free-space optical network, optical switch, optical amplifier, and quantum repeaters
- Quantum secure multiparty computation (QSMPC), including quantum bit commitment (QBC), quantum coin flipping (QCF), quantum oblivious transfer (QOT), quantum private comparison (QPC), and quantum private query
- Optimization and error correction theory and technology in quantum communication, including FEC for enhancing quantum reception rate, electronic noises and effects on quantum reception systems, training sequence and quantum reception protocols, and quantum error rejection
- Foundational quantum physics, including uncertainty of quantum detection, quantum correlations, nonlocal games, and prepare-and-measure experiments
- Cotransmission of CVQKD and real data channels for optical networking security
- Quantum transmission technology for software defined networks and aspects for new protocols and simulation of quantum systems

Authors can submit their manuscripts through the Manuscript Tracking System at http://mts.hindawi.com/submit/journals/ijo/pqs/.

Lead Guest Editor
Yanbing Li, Northwestern University, Evanston, USA
liyanbing1981@gmail.com

Guest Editors
Jamie Sikora, Centre for Quantum Technologies, Singapore
cqtjwjs@nus.edu.sg

Song Lin, Fujian Normal University, Fuzhou, China
lins95@gmail.com

Ahmed F. Metwaly, Al-Zahra College for Women, Muscat, Oman
dr.ahmedfarouk85@yahoo.com

Le Nguyen Binh, Huawei Technologies European Research Center, Munich, Germany
le.nguyen.binh@huawei.com

Hengyue Jia, Central University of Finance and Economics, Beijing, China
jiahengyue@cufe.edu.cn

Manuscript Due
Friday, 2 June 2017

First Round of Reviews
Friday, 25 August 2017

Publication Date
Friday, 20 October 2017