frontiers | Frontiers in Physics

TYPE Editorial
PUBLISHED 28 February 2023
DOI 10.3389/fphy.2023.1139505

OPEN ACCESS

EDITED BY
Omar Magana-Loaiza,
Louisiana State University, United States

REVIEWED BY
H. Z. Shen,
Northeast Normal University, China

*CORRESPONDENCE
Tianyu Ye,
yetianyu@mail.zjgsu.edu.cn

SPECIALTY SECTION
This article was submitted to Quantum Engineering and Technology, a section of the journal Frontiers in Physics

RECEIVED 07 January 2023
ACCEPTED 20 February 2023
PUBLISHED 28 February 2023

CITATION
Ye T (2023), Editorial: Multiparty secure quantum and semiquantum computations. *Front. Phys.* 11:1139505. doi: 10.3389/fphy.2023.1139505

Editorial: Multiparty secure quantum and semiquantum computations

Tianyu Ye*

Zhejiang Gongshang University, Hangzhou, China

KEYWORDS

multi-party secure quantum and semiquantum computation, multiparty quantum key agreement, multi-party quantum and semiquantum private comparison, multi-party quantum secret sharing, quantum voting, multi-party semiquantum key distribution

Editorial on the Research Topic
Multiparty secure quantum and semiquantum computations

During recent 2 decades, multi-party secure quantum computation and multi-party secure semiquantum computation have successfully attracted the attentions of researchers and have been greatly developed, whose security is decided by the fundamental laws of quantum mechanics, such as the uncertainty principle, the non-orthogonal state indistinguishable theorem, the quantum non-cloning theorem et al. However, there are still important and difficult Research Topic on them need to be solved. This Research Topic aims to show the recent achievements and the future challenges in *Multiparty secure quantum and semiquantum computations*. Research Topic of interest includes: multiparty secure quantum computation, containing multiparty quantum key agreement, multiparty quantum summation, multiparty quantum multiplication, multiparty quantum private comparison, multiparty quantum sealed-bid auction, multiparty quantum voting, multiparty quantum ranking, etc., multiparty secure semiquantum computation, containing multiparty semiquantum key agreement, multiparty semiquantum summation, multiparty semiquantum private comparison, multiparty semiquantum sealed-bid auction, multiparty semiquantum voting, etc., and quantum network and quantum Internet.

There are 18 papers published totally in this Research Topic. In order to solve the problem of generating temporary session key for secure communication in optical-ring quantum networks, an authenticated multiparty quantum key agreement method for optical-ring quantum communication networks was proposed by Gao et al. A novel multi-party quantum private comparison protocol with d-dimensional Bell states was proposed, where a semi-honest quantum third party can determine the size relationship of all participants' privacies without knowing the private information (Wang et al.). A new non-entangled quantum secret sharing protocol among different nodes based on locally indistinguishable orthogonal product states was designed, which promotes the development of quantum secure communication in the future (Fu et al.). In order to solve the problem that most of the quantum voting protocols are impractical due to the currently limited quantum storage capabilities, based on the interference principle of light, a new quantum voting protocol without quantum memory was constructed (Xu et al.). An original multi-party semiquantum key distribution protocol based on hyperentangled Bell states simultaneously in polarization and spatial degrees of freedom was put forward, which enhances the channel capacity (Tian et al.). A semiquantum key distribution protocol which allows one quantum user to distribute two different private secret keys to two classical users respectively at the same time

was proposed (Wu et al.). Two joint photon-number splitting attacks against a single-state semiquantum key distribution system were put forward, with which Eve can obtain key information without being detected by Alice or Bob (Mi et al.). A multi-party semiquantum private comparison protocol based on the maximally entangled GHZ-type state was designed, which can compare the equality of n parties within one execution of the protocol (Wu et al.). We hope that these research achievements can help promote the developments of multi-party secure quantum computation and multi-party secure semiquantum computation.

Author contributions

This Editorial is written by T Y Ye.

Conflict of interest

The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note