Measurement-device-independent quantum communication without encryption

October 11 2018

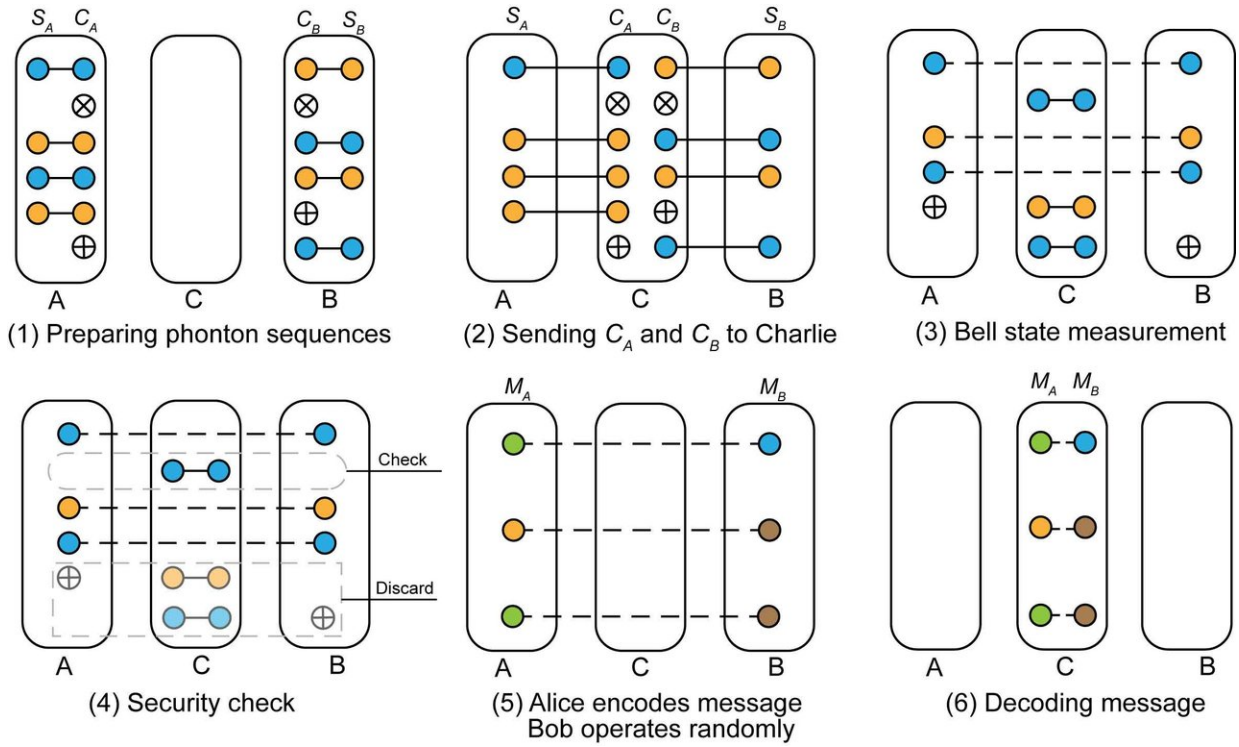

Illustration of the MDI-QSDC protocol. Credit: ©Science China Press

Quantum secure direct communication transmits secret information directly without encryption. Recently, a research team led by Prof. Gui-Lu Long from Tsinghua University proposed a measurement-and-device-independent quantum secure direct communication protocol using Einstein-Podolsky-Rosen pairs. This protocol eliminates all loopholes

related to measurement devices, which solves a key obstacle in practical quantum secure direct communication. The protocol has also an extended communication distance, and a high communication capacity.

Confidential communication is vital in modern society. Quantum secure direct communication is a new kind of secure communication with no encryption. In a classical secure communication, the sender and the receiver have to share a secret key in advance. Then a plaintext message is encoded into ciphertext and sent to the receiver through a classical channel. The ciphertext is then decoded to plaintext by the receiver to complete the communication. In this structure, there exist three potential security loopholes: (1) loss of the key during the distribution process; (2) loss of the key in storage and management; (3) interception of the ciphertext by Eve for later cryptanalysis. With the development of supercomputers and quantum computers, these threats become increasingly serious.

Quantum communication secured by quantum physics principles is an important scheme to resist these attacks. Quantum secure direct communication (QSDC) is a unique type of secure communication that does not require key distribution or key storage and management, and does not use ciphertext. It eliminates the three loopholes in classical secure communication efficiently.

The key problem of practical QSDC is that apparatuses used in practical quantum communication systems have some defects, and these imperfections, especially defects in the measurement devices, can lead to leakage of information and affect the security of practical QSDC. Recently, a research team led by Prof. Gui-Lu Long from Tsinghua University proposed a measurement- and device-independent (MDI) QSDC protocol using Einstein-Podolsky-Rosen pairs. This protocol eliminates all loopholes related to measurement devices, overcoming a key obstacle of practical QSDC. Additionally, the MDI-QSDC works

over long distances and has high communication capacity.

More information: Peng-Hao Niu et al, Measurement-device-independent quantum communication without encryption, *Science Bulletin* (2018). DOI: 10.1016/j.scib.2018.09.009

Provided by Science China Press