**\subsection{Quantum key distribution}**

With the development of quantum technology, quantum key distribution will gradually enter the practical stage. Bennett, one of the proposers of BB84 protocol, firstly demonstrated the protocol on an optical platform with distance of 30 cm [Journal of Cryptology, 1992, 5(1):3–28]. After that, Experiments have been developed rapidly from indoor to outdoors, and from short distance to long distance. In 1993, Muller experimentally demonstrated quantum cryptography using polarized photons in optical fiber over more than 1 km [Europhysics Letters, 1993, 23(6):383]; Townsend operated QKD experiment over 10 km using phase encoding [Electronics Letters, 1993, 29(7):634–635]. In 1995, Stucki et al. [quant-ph/0203118, 2002] in Gisin's group realized an experiment at outdoors over 67km using a plug&play system to keep stabilization automatically. In 2007, Janwei Pan's group [Phys. Rev. Lett. 98, 010505], Los Alamos Nation Laboratory [Phys. Rev. Lett. 98, 010503] and Zeilinger's group [Phys. Rev. Lett. 98, 010504] completed QKD experiments based on decoy-state over more than 100 km almost simultaneously, which marks the beginning of long-distance QKD. In 2010, Jianwei Pan’s group reported an implementation of decoy-state QKD over 200 km optical fiber cable through photon polarization with final key rate of 15 Hz [Optics express, 2010, 18(8):8587–8594]. In 2007, Takesue et al. firstly realized DPS protocol QKD over 42.1 dB channel loss and 200 km of optical dispersion-shifted fiber [Nature Photonics, 2007, 1(6):343–348]; In 2012, Guangcan Guo's group realized DPS protocol over 50 dB channel loss and 260 km optical fiber using superconductive detector, this is the first implementation of QKD over more than 50 dB channel loss [Opt. Lett., 2012, 37(6):1008–1010]. In 2009, Stucki et al. realized the coherent one way (COW) protocol QKD system with a maximum range of 250 km at 42.6 dB channel loss using ultra-low loss fiber, the secret bit rates is up to 15 bps. [New Journal of Physics, 2009, 11(7):075003].

Apart from using the QKD scheme based on state preparation and measurement, QKD schemes based on entanglement distribution mainly including E91 protocol [Phys. Rev. Lett., 1991, 67:661–663] and BBM92 protocol [Phys. Rev. Lett., 1992, 68:557–559], which also are developed and applied widely in many practical systems. In 2005, Zeilinger's group distributed entanglement and single photons through free-space quantum channel, demonstrated the feasibility of free-space quantum communication [Optics Express, 2005, 13(1):202–209]. In 2006, Ivan Marcikic et al. reported a complete experimental implementation of a QKD protocol through a free-space link using polarization-entangled photon pairs. [Applied Physics Letters, 2006, 89(10):101122]. In 2007, Zeilinger's group realized BBM92 protocol QKD based on polarization encoding over 144 km [Nature physics, 2007, 3(7):481–486]. The experiments listed above indicated the QKD protocols based on free-space entanglement distribution have the advantage of being less affected by decoherence, which lay solid foundation for global and satellite-to-ground quantum communication.

The fiber loss increases exponentially with distance increases. However, the loss of free-space transmission increases little with the increase of the distance, which is mainly related to the thickness of the atmosphere. Therefore, it is a perfect solution to construct the global quantum communication basing on the satellite. To verify the feasibility of a quantum channel between space and earth, a European Union group successfully received the weak light pulse emitted from a ground station and reflected by a mirror placed on a low orbiting satellites with orbital altitude of 1485 km in 2008[New Journal of Physics, 2008, 10(3):033038]. To verify the feasibility of QKD between satellite and ground with rapidly moving platforms, Weinfurter's group realized QKD over 20km from an airplane to the ground in 2013[Nature Photonics, 2013, 7(5):382–386]. In the same year, Jianwei Pan's group successfully accomplished quantum communication based on hot-air balloon floating platform [Nature Photonics, 2013, 7(4):387–393]. The experiments on airplane and hot-air balloon system demonstrate the feasibility under conditions of rapid motion, vibration, and random movement of satellites. At present, many countries including America, Canada, European Union, China and Japan pay high attention and support to accelerate the development of satellite-ground quantum communication. The first quantum satellite was launched in August 2016 in China will open a platform for satellite-ground quantum communication [Nature, 2016, 535: 478-479.]

In addition to the continuous expansion of the distance, the QKD is also developed from point-to-point experiment to the quantum communication network with multi-customers and various topological structure. There are many competition and cooperation in this area. The network of American Defense Advanced Research Projects Agency (DARPA) connected the three nodes, Harvard University and Boston University in Boston and BBN company in 2005, and then increased to 10 nodes [Quantum Communications and cryptography, 2006. 83–102]. Since 2006, the EU has established a "SECOQ" network, which unifying the efforts of 41 research and industrial organizations from 12 countries, including the UK, France, Germany, Austria, etc. A typical network used a trusted repeater paradigm including 6 nodes and 8 links was demonstrated in Vienna in 2008 [New J. Phys.,2009,11(7):075001]. In 2010, National Institute of Communication Technology, together with Nippon Telegraph and Telephone Corporation, Nippon Electric Company, Mitsubishi Electric Corporation, Toshiba European company, Switzerland IDQ Company and Austria All Vienna team constructed a Tokyo QKD Network in a metropolitan area and demonstrate the world-first secure TV conferencing over a distance of 45km [Opt. Express, 2011, 19(11):10387–10409]. The maximum distance is 90 km, and the point to point bit rate can reach 65kbps using superconductive detector over 45 km.

In China, the quantum network is also developed rapidly. In 2009, Jianwei Pan's group designed and constructed 3 nodes network with chained architecture, which demonstrated quantum unbreakable real-time voice telephone [Opt. Express, 2009, 17(8):6540–6549]. In the same year, Jianwei Pan's group designed metropolitan all-pass and inter-city quantum communication network in field fiber for four nodes, Any two nodes of them can be connected in the network to QKD [Optics Express, 2010, 18(26):27217–27225]. In 2009, Guangcan Guo's group constructed a topological structure with wavelength division multiplexers, realizing 4 nodes [Physics Letters A, 2008, 372(22):3957–3962] and 5 nodes star-type [Optics letters, 2010, 35(14):2454–6] QKD network. In 2012, Jianwei Pan's group constructed the largest metropolitan area quantum network in Hefei, linking 46 nodes to allow real-time voice communications, text messages and file transfers. A more than 2,000-km quantum communication used by government bodies and banks under construction in Beijing and Shanghai will be fully operational soon. With the help of the new satellite, scientists will be able to test quantum key distribution between the satellite and ground stations, and conduct secure quantum communications between Beijing and Xinjiang's Urumqi.

With distance and network coverage of quantum communication gradually increased, the security of QKD system draw more and more attention. Since 2012, the MDI-QKD protocol has been widely concerned, because of the features of safety and practicability. Tittel's group [Phys. Rev. Lett., 2013, 111:130501] demonstrated the protocol in the laboratory over more than 80 km of spooled fiber with time-bin encoding, they also tried outdoors experiment over 18.6 km. Brazilian Weid' group [Phys. Rev. A, 2013, 88:052303] demonstrated the protocol using polarization encoding scheme. However, these two demonstrations did not really distribute random key bits between two parties, and thus were not full MDI-QKD demonstrations. Additionally, the system of Tittel's group can be attacked by PNS or USD sources and cannot generate secure code in principle. A full demonstration of time-bin phase encoding MDI-QKD was reported by Jianwei Pan's group [Phys. Rev. Lett. 111, 130502] over 50 km fiber link. Lo's group [Phys. Rev. Lett., 2014, 112:190503] implemented polarization encoding MDI-QKD with commercial off-the-shelf devices over 10 km, and the secure key rate is 0.0047 bps. Subsequently, Jianwei Pan’s group continue to upgrade the performance of MDI-QKD system, making the distance of the experiments has reached 200 km [Phys. Rev. Lett. 113, 190501] and 400 km [arXiv:1606.06821].

**\subsection{Entanglement purification}**

Entanglement purification is originally proposed in [Phys. Rev. A 53, 2046, Phys. Rev. A 54, 3824, Phys. Rev. Lett. 77, 2818] in 1996, which is essential to distil highly entangled states from less entangled ones. In order to meet the experimental requirements, a more feasible purification scheme only needed polarizing beam splitter and post-selection was proposed and demonstrated by Jianwei Pan et al. [Nature 410, 1067]. Then the scheme was demonstrated by Jianwei Pan et al. [Nature 423, 417] in 2003, they prepared a mixed state with fidelity of 0.75 (0.8), a significant improvement of entanglement fidelity to the value 0.92 (0.94) is achieved after the purification operation. In 2005, Walther et al. performed a Bell experiment with purified states, a state below the threshold of Bell inequality successfully passed the Bell test after entanglement purification [Phys. Rev. Lett. 94, 040504]. Unfortunately, the theoretical efficiency of the purification scheme [Nature 410, 1067] is only 1/4, which still need to improve in theory and experiment.

**\subsection{Superdense coding}**

The idea of quantum dense coding was introduced by Bennett and Wiesner [Phys. Rev. Lett. 69, 2881], which can be used to send two bits of classical information using only one particle in a Bell state. In 1996, Mattle et al. [Phys. Rev. Lett. 76, 4656 (1996)] realized quantum dense coding experimentally for the first time in photonic system. However, they cannot realized a complete Bell-state analyzer, only three different messages could be encoded by a single qubit. Thus, an increase of channel capacity to  bits was possible.

To distinguish between all four polarization Bell states of two photons, Schuck et al. [Phys. Rev. Lett. 96, 190501 (2006)] developed a method that using hyperentangled source to realize a complete linear-optical Bell state analyzer in 2006, and achieved an overall channel capacity of 1.18(3) bits per photon in their experiment. In 2008, Kwiat's group [Nature Phys. 4, 282 (2008)] achieved channel capacity of 1.63 bits using pairs of photons simultaneously entangled in spin and orbital angular momentum, successfully beating the channel capacity limit for linear photonic superdense coding.

In other aspect, due to the noises in channel, researches hope to successfully achieve high efficiency dense coding over the noise channel. In 2013, A. Chiuri et al. successfully demonstrated dense coding over a depolarising channel [Phys. Rev. A, 87 (2013) 022333]. In 2014, Liu et al. [Europhysics Letters, 114(1), 10005(2016)] developed a superdense coding protocol in the presence of non-Markovian noise, they proved that loss of entanglement during encoding procedure will not reduce efficiency of information transmission. Their experiment reached the values of mutual information close to 1.52±0.02 (1.89±0.05) with 3-state (4-state) encoding.

Besides photonic system, superdense coding are also implemented in other systems, such as NMR system [Phys. Rev. A 61, 022307 (2000)] and atomic qubits [Phys. Rev. Lett. 93, 040505 (2004)]. In 2002, Li et al. [Phys. Rev. Lett. 88, 047904 (2002)] realized quantum dense coding by using continuous variables optics.

**\subsection{Quantum secret sharing}**

In 1999, Richard Cleve, Daniel Gottesman, and Hoi-Kwong Lo firstly proposed the concept of quantum secret sharing [Phys. Rev. Lett. 83, 648 (1999)]. Quantum secret sharing can enhance the security of classical information. In 2001, Gisin's group demonstrated the protocol for the first time based on energy-time entanglement, and this is also the first application of a quantum communication protocol based on more than two qubits [Phys. Rev. A 63,042301 (2001)]. In 2005, Jianwei Pan's group developed an ultra-stable four-photon GHZ states, and then realized 3-party quantum secret sharing [Phys. Rev. Lett. 95, 200502 (2005)]. In the same year, Weinfurter's group proposed and demonstrated a new quantum secret sharing protocol by sequential transformation of single qubit, without involving multiparticle GHZ states [Phys. Rev. Lett. 95, 230505 (2005)]. In 2007, Weinfurter's group realized four-party quantum secret sharing for the first time via the resource of four-photon entanglement [Phys. Rev. Lett. 98, 020503 (2007)]. In 2014, Tame's group realized four-party graph-state quantum secret sharing with a five-qubit graph state, which is meaningful to the integration of quantum networks via the measurement-based paradigm .[Nat. Commun. 5, 5480 (2014)].

The protocol can also be utilized as distribute quantum state securely, named as quantum state sharing. In 2004, Lam 's group demonstrated a multipartite protocol to securely distribute to 3 parties and reconstruct a quantum state with a fidelity average of 0.73 [Phys. Rev. Lett. 92, 177903 (2004)].

Theoretically, quantum secret sharing should satisfy three criteria: reliability, confidentiality [Commun. ACM 22, 612 (1979)] [G. R. Blakley, Safeguarding cryptographic keys, in Proc. Of the National Computer Conference, 1979, Vol. 48 (1979), p. 313], and capability of sharing entangled states. However, the experiments stated above cannot satisfy the second and third criterions simultaneously. In 2016, Jianwei Pan's group realized the fully quantum secret sharing, satisfying all of the three criteria simultaneously [PRL 117, 030501 (2016)].