INVITED PAPER

# Survey on Quantum Information Security

**Huanguo Zhang[1,*], Zhaoxu Ji[1], Houzhen Wang[1], Wanqing Wu[2]**

[1] Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China

[2] School of Cyber Security and Computer, Hebei University, Baoding 071002, China

* The corresponding author, email: Huanguo Zhang, liss@whu.edu.cn

***Huanguo Zhang***
Professor, Wuhan University

**Abstract:** The security of classical cryptography based on computational complexity assumptions has been severely challenged with the rapid development of quantum computers and quantum algorithms. Quantum cryptography, which offers unconditional security based on some principles of quantum mechanics, has become a significant branch and hotspot in the field of modern cryptography research. In this paper, we review the research and development of several important and well-studied branches of quantum cryptography in terms of theory and experiment, including quantum key distribution, quantum secret sharing, quantum secure direct communication, quantum signature, and quantum private query. We also briefly review the research and development of some other branches which are currently in the stage of theoretical research but receive widespread concern from academia, including quantum private comparison, quantum anonymous voting, quantum secure multi-party summation, quantum sealed-bid auction, quantum public key cryptosystem, quantum key agreement, quantum dialogue, and quantum identity authentication. In addition, we discuss some open issues and future research directions for the branches referred to above.

**Keywords:** quantum information; information security; quantum cryptography; quantum key distribution

## I. Introduction

The 21st century is an information age. With the rapid development of information technology and related industries, information security has been playing a vital role in national security and social stability for decades [1]. Information security has penetrated into all areas of national economic and social development, including politics, military affairs, medical treatment, as well as personal bank accounts, e-mail passwords, online shopping etc. However, with the emegence of various security issues, the demand for information security is becoming more and more intense, and the requirements are also getting higher and higher.

Cryptography is the theoretical basis and core technology of information security, which includes various technologies of encryption and decryption, entity authentication, message authentication etc. Cryptography consists of the symmetric cryptosystem (A.K.A. private key cryptosystem) and the asymmetric crypto-

Received: Jan. 27, 2019
Revised: Jun. 22, 2019
Editor: Yueming Cai

We have reviewed the research and development of some branches in quantum cryptography domain, including QKD, QSS, QSDC as well as QPC, QAV, QSMS, etc.

system (A.K.A. public key cryptosystem) [2]. In a symmetric cryptosystem, the encryption and decryption keys are the same, or one can be deducted from the other although there are some differences between them, while two different keys are respectively used for encryption and decryption in an asymmetric cryptosystem and it is impossible to infer the corresponding decryption key from the encryption key. The security of these cryptosystems is based on the assumption of opponents' computing power. However, with the rapid development of computer software and special hardware, especially the emergence of quantum algorithms and quantum computers, human computing power is becoming stronger and stronger, which poses a huge threat to the security. Many cryptosystems, such as the famous RSA proposed by Ron Rivest, Adi Shamir and Leonard Adleman in 1977 ("RSA" is the combination of the initial letters of their surnames), have been proved unsafe, which has aroused serious concern from all walks of life, including academia.

So far, quantum information technology has been quite mature in some areas, especially in cryptography. Quantum cryptography [3,4] is the combination of classical cryptography and quantum mechanics, which provides the first provable unconditional security for both sides of communication in principle. With the development of technology, quantum cryptography is expected to become the first commercial application of quantum communication [5]. The security of quantum cryptography is guaranteed by the fundamental laws of quantum mechanics, rather than by unproven computational assumptions [4,6,7]. The idea of quantum cryptography was first proposed by Wiesner in his paper entitled "Conjugated Coding" in the late 60s and early 70s [8]. Wiesner showed that quantum mechanics can be used to accomplish two tasks that are impossible from the perspective of classical physics in his paper. One is to generate unforgeable bank notes, another is the use of quantum mechanics to store or transmit two messages by encoding them in two "conjugate observables" such as linear and circular polarization of light. Unfortunately, his paper was rejected by IEEE Information Theory because his idea was considered too bizarre, but was eventually published in SIGACT News in 1983.

In 1979, Charles Bennet of IBM and Gilles Brassard of the University of Montreal learned Wiesner's point of view, then began to consider the specific implementation of quantum cryptography, and proposed the first quantum key distribution scheme in 1984, which has been called BB84 ever since [3]. Later, they built a complete functional prototype at IBM Thomas J. wstson Research Center in 1989. Up to now, the research on quantum cryptography has attracted much interest from researchers in the fields of theoretical and experimental physics, mathematics and computer science. Significant progress has been made both in theory and in experiment. Several companies, such as IdQuantique, MagiQ and SmartQuantum, have commercially developed quantum cryptography prototypes, which are combined with current encryption and decryption technologies to introduce quantum cryptography into practical applications. Quantum cryptography is undoubtedly a promising technology for adoption in realistic cryptographic applications, and its practical application is just around the corner.

In this paper, we first review the theoretical and experimental research and development of several important and well-studied branches in the quantum cryptography domain, including quantum key distribution, quantum secret sharing, quantum secure direct communication, quantum signature, and quantum private query, with emphasis on a number of open questions and technical issues. Then, we review the research and development of some other branches which are still at the stage of theoretical research, but have attracted wide attention, including quantum private comparison, quantum anonymous voting, quantum secure multi-party summation, quantum sealed-bid auction, quantum public key cryptosystem, quantum key agreement, quantum dialogue, and quantum identity authentication. We also discuss the future challenges and research directions of these branches. For saving space, we would only like to give a brief review of some important work in each research branch, and give relevant references to the technical terms involved in this paper without making specific explanations. The organization of the remainder of this paper is as follows: We devote Sec. 2 to 7 to review the research and development of the branches mentioned above, analyze the shortcomings of the research on them and look forward to the future research. In Sec. 8, we provide an outlook to quantum cryptography and conclude this paper.

## II. Quantum Key Distribution

Quantum key distribution (QKD) is a technology which allows two parties (commonly called Alice and Bob) to share a common key or a key sequence for encryption. In 1984, Charles Bennet and Gilles Brassard proposed the first QKD protocol, which was known as BB84 after publication. BB84 is the most famous and practical quantum cryptography protocol at present, which uses photon polarization states to transmit information.

In a QKD protocol, if an eavesdropper (conventionally called Eve) tries to steal the key, the communicators will detect her using appropriate quantum laws (e.g. the famous Heisenberg uncertainty principle). QKD is usually based on the impossibility of observing a quantum mechanics system without disturbing it. If Eve tries to eavesdrop on the quantum communication between Alice and Bob, she will inevitably leaves some traces that can be detected. Therefore, a QKD protocol achieves the following types of security: On the one hand, as long as Eve is passive (this is called robustness), the protocol generates arbitrarily long keys. On the other hand, if Eve tampers with quantum channels, the protocol identifies the attack and terminates the generation of the keys. In other words, as long as Eve is passive, the protocol will not be suspended. In addition, for any attack on quantum channels, the probability that the protocol does not stop and Eve steals the generated keys is negligible.

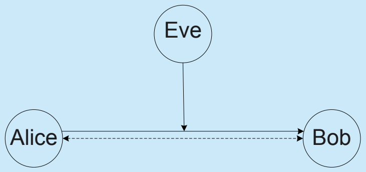
In the past two decades, the rapid development of QKD in theory and experiment has been reflected through a series of successful demonstrations. However, the research on QKD still faces a number of challenges, such as the distance between communicators, quantum bit error rate, and practical security etc [7,9]. At present, the main research hotspots in the field of QKD include QKD networks, device-independent (DI) QKD, measurement-device-independent (MDI) QKD, detector-device-independent (DDI) QKD, security proof for QKD, and semi-QKD (SQKD).

### 2.1 Theoretical research

In recent years, prolific theoretical research work has been conducted, which focus on the security of QKD including the finite-key security analysis and security proof for various protocols, the design and analysis of semi, DI, MDI, DDI protocols.

#### 2.1.1 Security of QKD

It is known that the appeal of QKD comes mainly from the fact that it can provide unconditional security in principle. However, its security is a complex subject with several open questions still remain [10,11]. Most the theoretical studies of security involve BB84 protocol. Early studies showed that, based on various assumptions, attacks against several restricted types are secure. Later, security was proved for the most general individual attacks.



As a universal convention in quantum cryptography, Alice sends quantum states to Bob through a quantum channel. An external eavesdropper (Eve) is suspected of eavesdropping on the quantum channel.

**Fig. 1.** *Generally, a quantum key distribution protocol comprises a quantum channel (the solid arrow line) and a public classical authenticated channel (the dashed arrow line).*

Since Peter W. Shor and John Preskill [12] gave the simpler proof of BB84 by relating its security to the entanglement purification protocol and the quantum error correction code, the security proof of QKD has attracted wide attention and a series of important improvements have been made. The security of two quantum cryptography schemes using d-Level Systems against individual attacks as well as coherent attacks is analyzed in Ref. [13], where the first cryptosystem uses two mutually unbiased bases, and the second exploits d+1 mutually unbiased bases. The security proof for the protocols with entangled photons which can be applied to practical systems is presented in Ref. [14], where the proof is restricted to individual eavesdropping attacks with the assumption that the detection apparatus is trustful. Ref. [15] proposes a decoy-pulse method to overcome the photon-number-splitting attack for BB84 protocol in the presence of high loss: A legitimate user intentionally and randomly replaces signal pulses by multiphoton pulses (decoy pulses). The security proof of coherent-state protocols against arbitrary coherent attacks is provided in Ref. [16], which is based on the transmission of Gaussian-modulated coherent states and homodyne detection. Ref. [17] theoretically proves the security against the most general attacks, such as individual-particle attacks and joint attacks which can be performed on quantum channels by an eavesdropper who has unlimited technology (e.g. unlimited computing power, quantum memory and quantum computers). Ref. [18] proves the security of DI QKD against collective attacks, which is extended by Ref. [19] to a more general class of attacks. Ref. [20] provides the passive approach to the security analysis using a beam splitter to split each input pulse, and presents the complete proof of its unconditional security. Ref. [21] proves the security of BB84 with arbitrary individual imperfections simultaneously in the quantum sources and detectors. Ref. [22] provides the security bounds against coherent attacks for the protocols which use d-dimensional alphabets, and shows that the security bounds are valid in the nonasymptotic regime of finite-length keys. Ref. [23] demonstrates the semi-device-independent security of one-way QKD against individual attacks, in which the devices are noncharacterized but only assumed to produce the quantum systems of a given dimension. Ref. [24] provides the general security proof for a large class of protocols in the model where the raw key is generated by independent measurements. Ref. [25] presents the generic method to prove the security of practical distributed-phase-reference QKD against general attacks. Ref. [26] proves the security of Gaussian continuous-variable QKD with coherent states against arbitrary attacks in the finite-size regime, which is applicable in the practically relevant finite-size regime. Ref. [27] provides the strategy to prove the security of two-way QKD protocols against the most general quantum attack of an eavesdropper, which is based on an entropic uncertainty relation. Ref. [28] provides the security proof of DI QKD protocols which can be applied to generic DI QKD protocols based on arbitrary Bell inequalities, and has the same efficiency and tolerance to noise as previous proofs using memoryless devices. Ref. [29] analyzes the protocol for generating a distributed secret key from correlations that violate a Bell inequality by a sufficient amount, and proves its security against eavesdroppers under the assumption that any information accessible to them must be compatible with the non-signaling principle. Ref. [30] rigorously proves the DI QKD security of a slight variant of Ekert's original entanglement-based protocol [4] against the most general attacks. Ref. [31] presents a scheme for continuous-variable QKD using the orthogonal frequency division multiplexing technique, and gives the security analysis of the protocol with imperfect modulation. The rigorous security analysis of continuous-variable MDI QKD in a finite-size scenario is presented in Ref. [32].

In recent decade, the finite key analysis method proposed by Hayashi [33] has become a hotspot in the field of security analysis for QKD, and has been integrated into the composable unconditional security proof. Ref. [34] provides the security bounds of the finite length keys for several practical implementations of the BB84 coding, including the ones for prepare-and-measure implementations without decoy states and the ones for entanglement-based implementations which guarantee unconditional security, and the one for prepare-and-measure implementations with decoy states. Ref. [35] gives the finite-key analysis of MDI QKD, which removes all detector side channels and generates many orders of key rate higher than that of full-device-independent QKD. Ref. [36] provides the rigorous security proof against general attacks in the finite-key regime, and demonstrates the feasibility of the long-distance implementations of MDI QKD within a reasonable time frame of signal transmission. Ref. [37] proposes the practical prepare-and-measure semi-device-independent BB84 protocol with finite resources, and obtains the finite-key bound in terms of the value of dimension witnesses against collective attack for it. The finite-key security analysis which is valid against arbitrary information leakage from the state preparation process is provided by Ref. [38].

### 2.1.2 DI, MDI and DDI QKD

DI QKD [39] aims to narrow the gap between the theoretical analysis and the practical realization of QKD without making assumptions about the internal work of the quantum devices used. It requires the violation of the Bell inequality between Alice and Bob, and can provide higher security than traditional schemes by reducing the number of required security assumptions. In other words, Alice and Bob only need to observe the full violation of Bell inequality to prove the security. DI refers to the fact that no knowledge of the internal mechanism of the devices is necessary. In fact, the devices may be provided by an adversary. Alice and Bob regard their physical device models as “black boxes” without assuming the size of the Hilbert space of quantum signals and the type of measurements performed on them. In other words, they just need to know what elements are in their boxes, not how to implement quantum processes [40]. So far, it has been proved that DI QKD can resist various attacks such as time-shift attacks [41], phase remapping attacks [42], blinding attacks [43], and wavelength-dependent attacks [44]. In addition, the detection loophole caused by the losses in quantum channels can be avoided [45]. The DI QKD protocol with generalized two-mode Schrodinger cat states is presented in Ref. [46].

MDI QKD, first proposed by Lo et al. in 2012 [47], is an important step to achieve the practical information theoretical security of the key sharing between remote legitimate users (Alice and Bob), in which the key is established by measuring untrustworthy relays. Compared with DI QKD, MDI QKD has several advantages. First, the key rate of MDI QKD is many orders of magnitude higher than that of DI QKD. Secondly, the detector side channels can be successfully removed. Thirdly, in a MDI QKD protocol, Alice and Bob do not need to perform any measurements, they just need to send quantum signals to be measured. Therefore, Alice and Bob do not need to hold measurement devices, and can regard the measurement devices as “black boxes” which may be completely controlled by Eve. This is important because it eliminates the need to authenticate the detectors in the QKD standardization process. Therefore, the bit strings generated by Alice and Bob will not be attacked by the detector side channel because no detectors are used. They only need to characterize the quantum states they send through the channels, and this characterization should occur in a protected environment that is not affected by an adversary, which is feasible in principle.

MDI QKD has been widely studied in recent years since its invention. Ref. [48] proposes two schemes for the phase encoding: one employs a phase locking technique with the use of non-phase-randomized coherent pulses, and the other one uses the conversion of standard BB84 phase encoding pulses into polarization modes. Ref. [49] proposes the practical protocol using phase and path or time encoding, in which the setup employs simple encoding and decoding modules without relying on polarization maintenance or optical switches. The continuous-variable MDI protocol where the detection is conducted by an untrusted third party is presented in Ref. [50]. Ref. [51] presents the scheme to implement MDI protocols with the source of Gaussian-modulated coherent states, which is based on the principle of continuous-variable entanglement swapping. Ref. [52] proposes the decoy-state protocol where the measuring basis is chosen with a biased probability and the intensities of the different types of states are selected properly to optimize the achievable finite secret key rate. Ref. [53] gives the method to improve the performance of coherent-state continuous-variable MDI protocols by virtual photon subtraction via non-Gaussian postselection. Ref. [54] proposes the method to improve the performance of the continuous-variable MDI protocol by using photon subtraction, which can be implemented under current technology. Two modified MDI protocols based on the decoherence-free subspace are proposed in Ref. [55], both of two are tolerant of the fault with collective-rotation noise and collective-dephasing noise. Ref. [56] presents the protocol without vacuum source using the heralded single-photon source and global optimization, which is able to provide a high key rate and avoid the security problem caused by the vacuum source or extremely weak source.

Compared with MDI QKD, DDI QKD [57] can construct a more efficient detector side-channel-free system, which can overcome the main shortcomings of MDI QKD. One of the drawbacks is that MDI QKD systems usually require high visibility two-photon interference between independent sources, which makes their implementation more demanding than traditional QKD systems. Secondly, MDI QKD requires larger post-processing data block sizes than standard QKD for the finite-key security bounds of general attacks. Thirdly, compared with the point-to-point QKD system, the secure key rate is significantly lower [58]. In general, the security of DDI QKD is based on the following assumptions: First, the random number generator and classical post-processing of Alice and Bob are credible. Secondly, Alice's and Bob's linear optical circuits are fully characterized and cannot be affected by Eve. Thirdly, Eve can use imperfect detectors through optical fibers, but she can't access detectors and interferometers. Finally, the detectors provided by trusted providers may have some defects, which is, however, not related to Eve. In recent years, several important achievements have been made in the research of DDI QKD. Ref. [59] analyzes the security of DDI QKD and demonstrates that it is vulnerable to detector side-channel attacks as well as other side-channel attacks that exploit the imperfections of Bob's receiver, and proposes a new scheme which guarantees robustness against detector-side channel attacks in order to solve this problem. Ref. [60] analyzes the security of DDI QKD and implements the complete high-speed version clocked at 625 MHz, based on polarization encoded qubits. Ref. [61] proposes the attack method which combines the detector blind attack with the intrinsic defects of single photon detectors, and verifies the feasibility of this method through experiments.

### 2.1.3 SQKD

SQKD, also known as QKD with classical Bob, is a new QKD mode with the restricted quantum capabilities of at least one party, which can reduce not only the computational burden of the parties but also the cost of the quantum devices in practical implementations. SQKD allows Alice and Bob to complete the task of QKD, in which only Alice is quantum while Bob has only classical capabilities. Specifically, Alice is allowed to perform following operations:

(1) prepare any quantum states, such as Bell states,

(2) perform any quantum measurement, such as single-particle measurement and Bell measurement, and

(3) store quantum states in a quantum memory.

Bob is restricted to perform the following operations:

(1) prepare new qubits in the Z basis ($\{|0\rangle, |1\rangle\}$),

(2) measure qubits in the Z basis,

(3) reorder the qubits, and

(4) send or reflect the qubits without disturbing quantum channels.

In SQKD, the party with limited quantum capacity is called classical party, and the one with full quantum ability is called quantum party.

The first SOKD protocol was proposed by Boyer et al. in 2007 in which only single photons are used and the robustness of the protocol is showed [62]. Subsequently, they further extended their work by first generalizing the conditions under which the results of their work hold for the measure-resend SQKD, specifically, proved that complete robustness still holds when the qubits are sent one by one and are attacked collectively [63]. Boyer et al. also proposed a experimentally feasible protocol using four-level systems instead of qubits [64]. Similar to first SOKD protocol, Ref. [65] presents a protocol with classical Alice in which Alice has only classical capacities and always encodes her key bits in the Z basis. Ref. [66] proposes five SQKD protocols with complete robustness via sending less than four quantum states. Ref. [67] investigates the two-way eavesdropping strategy against a SQKD protocol. Ref. [68] presents a protocol which allows two limited classical users to establish a shared secret key with the help of a untrusted fully quantum server. Ref. [69] constructs a protocol without invoking the measurement capability of the classical party Alice and also proves it to be completely robust against quantum joint attacks, which shows that the measurement capability of the classical party is not necessary in SQKD. Ref. [70] proposes a protocol with the help of an untrusted quantum server who may try to reveal the session key of the participants through various possible attacks, in which the entanglement correlation between Bell states and Z-basis particles is used to share the session key and to detect the malicious behavior of the quantum server or eavesdroppers without invoking quantum measurement for the classical participants. In recent years, based on different quantum states and different quantum technologies, many protocols have been proposed [71-76]. In addition, some work focus on to the security analysis of SQKD [77-79].

## 2.2 Experimental research

Since the first demonstration of QKD systems in 1992 [80], researchers have been making a lot of efforts toward the implementation of such systems with the goals of making it more practical by extending the possible communication distance and achieving the highest possible communication rate [81]. After nearly 20 years of development, experimental QKD has made remarkable progress, mainly devoted to long-range communication, including fiber-based communication [82-100] and free-space communication [80,101-119]. Commercial QKD systems have successfully entered the market. In short, QKD is mature enough to be used in practical applications.

### 2.2.1 Fiber-based QKD

At present, quantum communication networks based on optical fibers have been widely installed. In the future, the quantum channels in the global quantum communication network will mainly consist of optical fibers. The fibre-based QKD has increased the transmission distance from 32 cm [80] to 260 km [95] and the speed (or the system clock rate) from 200 Hz [80] to 10 GHz [96,97]. The proof-of principle experiment over 50 km of optical fibers is realized with entangled photon [98]. Ref. [99] implements the differential phase shift protocol where the keys are generated at the practical rate of 166 bit/s over 100 km of fibers, which is based on the security analysis of the protocol against all general individual attacks, including photon number splitting attacks, beam-splitter, intercept-resend and photon number splitting attacks. Ref. [97] realizes the experiment over 42.1 dB channel loss and 200 km of distance with dispersion-shifted fiber. Ref. [100] implements the experiment over 250 km of distance with 42.6 dB channel loss with ultra-low-loss fiber. The experiment over 260 km with 52.9 dB channel loss is realized in Ref. [95].

### 2.2.2 Free-space-based QKD

Free-space connections will allow remote legitimate parties to quickly build up connections with direct line-of-sight [80,103-107,109-119]. Additionally, orbital-free space links, such as satellite-to-ground links and inter-satellite links, can achieve the effective global interconnection of regional quantum networks [111,112]. The expected attenuation of satellite single link grounding connections is at least 30 dB, and its feasibility has been proved in the first ground test [103,108]. Ref. [108] realizes the experimental implementation of BB84 type QKD over a 144 km free-space link using weak coherent laser pulses. Ref. [113] experimentally studies the important advantage of entanglement-based QKD systems by implementing different setups on a 144 km free-space link between the two Canary Islands of La Palma and Tenerife, which can tolerate higher channel losses than the systems based on weak coherent laser pulses. Ref. [114] experimentally demonstrates the feasibility of reference frame independent QKD over a free-space link in a prepare and measure scheme using polarization encoding. Ref. [115] reports three independent experiments with a decoy-state QKD system, which addresses wide ranges of all leading parameters relevant to low Earth orbit satellites, and which paves the way towards ground-satellite QKD and a global quantum communication network. Ref. [116] proves the feasibility of BB84 QKD between an aeroplane moving at 290 km/h at a distance of 20 km and a ground station, which guarantees stable transmission of QKD signals at the single-photon level and will also significantly improve the performance of future applications of the classical communication link. Ref. [117] demonstrates quantum communication with polarization encoding from space to ground by exploiting satellite corner cube retroreflectors as quantum transmitters in orbit and the Matera Laser Ranging Observatory of the Italian Space Agency in Matera, Italy, as a quantum receiver, the scheme of which paves the way toward the implementation of a quantum communication worldwide network leveraging existing receivers. Recently, Liao et al. reported the development and launch of a low-Earth-orbit satellite for implementing decoy-state QKD, which achieves a kilohertz key rate from the satellite to the ground over a distance of up to 1,200 km [118]. In addition, they demonstrated the feasibility of satellite-based quantum communication in daylight by choosing a working wavelength of 1,550 nm and developing free-space single-mode fibre-coupling technology and ultralow-noise upconversion single-photon detectors [119].

### 2.2.3 QKD network

QKD network [120,121] is proposed to meet the needs of future demands for large-scale and multiuser secure communications, and provides the vision of future secure communication facilities. Ref. [122] proposes the architecture for implementing a fiber-based QKD network using optical wavelength division multiplexing in the fiber. Ref. [123] experimentally demonstrates a six-user network implemented on a bus topology, in which the network employs BB84 to transmit keys. Ref. [124] presents the scheme to build a star topology network based on wavelength division multiplexing, in which all users can exchange keys directly and simultaneously, and the insertion loss of the network is independent of the number of users. Ref. [125] reports the realization of the star topology four-user network without trusted relays, which automatically addresses the quantum signal with a quantum router and every user in the network can receive and distribute quantum keys to any others simultaneously. Ref. [126] realizes the hierarchical network with decoy state method located in Wuhu, China, operated continuously beneath the streets of the city, where seven subsidiaries of the city are connected to form a secure communication network. Ref. [127] proposes the wavelength-saving topology of a network based on passive optical elements, and reports its field test on commercial telecom optical fiber at the frequency of 20 MHz. Ref. [128] proposes a QKD network model as well as the QKD node and link for easily analyzing and understanding this network, and proposes a secret-key-aware routing method to search the optimal relaying path.

### 2.2.4 Experimental MDI QKD

In recent years, experimental MDI QKD has also made remarkable progress. Ref. [129] reports the experimental implementation of MDI QKD, where Alice and Bob are each connected to Charlie via independent 8.5 km spooled fiber links, as originally proposed by Lo et al [47]. Ref. [130] presents the implementation of the time-bin phase-encoding MDI QKD scheme [47,49], which is immune to all hacking strategies on detection. Ref. [131] studies decoy-state MDI QKD using heralded single-photon sources, and proposes the improved method which can offer a secure transmission distance of more than 70 km. Ref. [132] proposes that MDI-QKD is highly practical and thus can be easily implemented with standard optical devices, and presents a simple analytical method with only two (general) decoy states for the finite decoy-state analysis, which can be used directly by experimentalists to demonstrate MDI-QKD. Ref. [133] proposes the phase-coding reference-frame-independent scheme which requires no phase alignment between the interferometers of two distant legitimate parties. Additionally, Ref. [133] reports the proof-of-principle experiment using Faraday-Michelson interferometers, where the experimental system worked at 1 MHz, and the average secure key rate of 8.309 bps is obtained at a fiber length of 20 km between Alice and Bob. Ref. [134] performs the field test in three adjacent sites located in Hefei City, China, via the deployed fiber network of 30 km total length achieving a 16.9 b/s secure key rate. Ref. [135] completes the implementation of MDI QKD over 404 km of ultralow-loss optical fiber and 311 km of a standard optical fiber by an optimized four-intensity decoy-state method. Ref. [136] performs the proof-of-principle experimental demonstration of plug-and-play MDI QKD over an asymmetric channel setting with a single signal laser, in which the whole system is automatically stabilized in spectrum, polarization, arrival time, and phase reference. Ref. [137] takes the modulation error into consideration and presents the experiment with state preparation imperfections over the fiber links of 40 km.

## 2.3 Problems and challenges

Despite the rapid progress in theoretical and experimental research in recent years, the research of QKD still faces many challenges. On the one hand, almost all the hypotheses about the current security proof of QKD are crucial. However, in practical applications, these hypotheses are difficult to prove correct, because quantum devices always have a number of defects, such as detector’s back-door pulse and dead-time [43,138-140]. Therefore, a proof with weaker hypotheses remains the subject of ongoing research. On the other hand, a practical QKD system still faces many challenges, such as the inefficiency of classical communication authentication, the limited size effect of data processing, the defects of significant setup, the fidelity of quantum states under the influence of quantum noise, and the lack of commercial use of entanglement in commercially available QKD systems. Especially the secret bit rate is usually very low, which is the main obstacle to metropolitan QKD networks. DI QKD can overcome the device imperfections that may lead to the existence of some security loopholes which enables an eavesdropper to acquire the secret key of the practical QKD system if quantum hacking strategies are smartly designed. Unfortunately, almost all DI QKD schemes impose strict restrictions on the specifications required for physical devices, such as the need for loophole-free Bell testing, which makes them challenging and difficult to implement with current technologies. In this case, a number of MDI QKD protocols are proposed in order to relax these constraints with the main additional assumption that the source used is trustful. However, MDI QKD still faces enormous difficulties and challenges. On the one hand, compared with standard point-to-point (PTP) QKD, the implementation of MDI QKD is more difficult. On the other hand, due to the need for the two-photon interference, its technical complexity is higher than the prepare-and-measure scheme which requires that the two photons are indistinguishable in all degrees of freedom. Future research should consider how to solve above problems.

## III. Quantum Secret Sharing

Secret sharing is an important cryptographic primitive in the field of secure multi-party computation, and it can be regarded as a special case of secure multi-party computation. It includes the method of dividing messages using mathematical algorithms and assigning shares to two or more legitimate users through classical communication. Only when a sufficient number of parties cooperate with each other by sharing their secret parts can they reconstruct the secret. Secret sharing has applications in password-authenticated key agreement, hardware security module, electronic voting, cloud computing, online auction, private querying of databases, establishment of restricted access code etc. The first classical secret sharing scheme is invented independently by Shamir [141] and Blakley [142].

The original message can be reconstructed if and only if at least $k(1 \le k \le N)$ shares are known. This is called $(k, N)$ secret sharing threshold scheme (the threshold is $k$), which comprises the distribution of the shares of a secret or a random key among $k$ users, in such a way that it can be reconstructed from at least $k$ shares. An example of such a secret sharing scheme is Shamir's scheme [141], which uses the concept of polynomial interpolation to generate and distribute secrets shared by a businessman, and then reconstructs them by users. Good (honest) users can successfully reconstruct secrets through cooperation, while bad (malicious) users cannot. [143]. Therefore, for the successful reconstruction of a secret, at most $N-k$ users can be bad.

Quantum secret sharing (QSS) expands the number of legitimate users in the "traditional" QKD to more than two [144-146]. Unlike classical secret sharing, the shared information in QSS can be classical or quantum. In particular, QSS is very useful for creating private keys in secure multi-party communications. QSS contains the behavior of splitting messages, which can only be retrieved through the cooperation of all receivers. In a QSS protocol, the sender named Alice distributes secret parts to two receivers named Bob and Charlie, respectively. In this way, neither Bob nor Charlie has any information about the key alone, but they have complete information together. In addition, eavesdroppers' attempts to obtain some information about the key will inevitably result in errors in data transmission, thus exposing their existence.

The first QSS scheme was proposed by Hillery et al. in 1999 by using three-particle and four-particle Greenberger-Horne-Zeilinger (GHZ) entangled states [144]. Although the scheme elegantly proposes a quantum mechanics method to realize the above secret sharing function, its implementation seems to be problematic due to the difficulty in preparing GHZ states. Up to now, QSS has been extensively studied both experimentally and theoretically. Based on various quantum states and quantum technology, a lot of protocols have been proposed [145-157]. In recent years, circular QSS, which is useful and efficient when one of the users is remote to the others who are adjacent, especially the number of the users are more than three, has attracted much attention and several protocols have been proposed [158-160]. In addition, semi-QSS has also become a research hotspot [161-163]. Moreover, several achievements have been made in the research of DDI and MDI QSS [164-166]. Future research in these directions will continue and receive wider attention.

After nearly 20 years of development, quite a few important progress has been made in the research of experimental QSS, although its experimental feasibility level is far from that of QKD. Ref. [167] presents the setup for QSS based on energy-time entanglement, and demonstrates the feasibility of QSS using pseudo-GHZ states which do not consist of three down-converted photons but only of two down-converted ones plus the pump photon. Ref. [168] develops the theory of continuous-variable (2,2) threshold QSS [169] and implements it by using optical interferometry and squeezed light sources. Ref. [170] extends continuous-variable (2,2) threshold QSS [169] and presents two schemes to perform continuous variable (2, 3) threshold QSS on the quadrature amplitudes of bright light beams, where the first scheme utilizes two phase sensitive optical amplifiers, and the second uses an electro-optic feedforward loop for the reconstruction of the secret. Ref. [171] presents the simple and practical protocol and its proof-of-principle experimental realization, in which a sequential single qubit communication between users is used. Ref. [172] presents the experimental realization of protocols by developing and exploiting the ultrastable high intensity source of four-photon entanglement. Ref. [173] presents the experimental demonstration of four-party quantum secret sharing via the resource of four-photon polarization-entangled states [174]. Ref. [175] realizes the single qubit QSS experiment over telecommunication fibers in an interferometric setup with the phase encoding in three, four, and five-party implementations. The three and four-party implementations over 1550 nm single mode fiber networks, using a single qubit protocol with phase encoding is reported in Ref. [176]. The proof-of-principle experiment of robust single-photon QSS over a single-mode fiber network in an interferometric setup using Schmid's scheme [171] with phase encoding in three and four-party implementations, is presented in Ref. [177]. Ref. [178] presents the robust single-photon circular QSS experiment for three users over 50 km single mode fiber network using the single qubit protocol proposed by Deng et al [158] with phase encoding.

At present, there is still a certain gap between QSS and its classic counterpart. In particular, there are few research results on QSS with extended functions, such as more general threshold QSS, full dynamic QSS, and QSS with verification function. In addition, due to the lack of theoretical models of quantum information, the research results with quantum and classical information theory methods are not enough. In the future, more attention should be paid to these issues.

## IV. Quantum Secure Direct Communication

Quantum secure direct communication (QSDC) is an important branch of quantum communication, which aims to send secret information directly through quantum channels without setting prior keys [179-182]. Different from the two-channel (key distribution, ciphertext transmission channels) structure of general secure communication, QSDC requires only a single quantum channel, which is a fundamental change to secure communication structure. QSDC can eliminate the security loopholes associated with key distribution, key storage and management, and ciphertext transmission [183] in theory, and improve the security and instantaneity of communications by transmitting information directly over quantum channels. QSDC is also the basic cryptographic primitive for constructing other quantum communication tasks, such as quantum authentication and quantum dialogue.

Using Einstein-Podolsky-Rosen (EPR) pairs, Long et al. proposed the first QSDC protocol in 2002 [179], and then proposed a two-step protocol in 2003 [180]. Since then, QSDC has become one of the research hotspots in the field of quantum communication. Nowadays, a lot of schemes based on a variety of different quantum states and techniques have been proposed. The quantum states used include hyperentangled states [184,185], single photons [186,187], Bell states [188-191], W states [192], five-particle cluster states [193], GHZ states [194-198], seven-Qubit entangled states [199], six-qubit maximally entangled states [200], non-orthogonal states [201], cluster states [202,203], pure entangled states [204], and $\chi$-type entangled states [205] etc. The techniques used include quantum superdense coding [198,200,206-208], unitary operations [191,192], teleportation [193,201], entanglement swapping [189,194,196,209], quantum search algorithm [210], phase encryption [211], authentication [212], quantum one-time pads [181] etc. MDI QSDC has also been proposed and attracted much attention in recent years. The first MDI QSDC protocol was proposed by Zhou et al. in 2018 [183], in which sequences of EPR pairs and single photons are used. In the same year, Niu et al. proposed another protocol using EPR pairs, which eradicates the security vulnerabilities associated with the measurement device, and greatly enhances the practical security of QSDC [213].

The experimental research progress of QSDC is very fast, and some excellent research results have been obtained in recent years. In 2016, Hu et al. reported the first experimental demonstration based on the DL04 [181] protocol and equipped with single-photon frequency coding that explicitly demonstrated block transmission [214]. In 2017, Zhang et al. reported the experimental proof-of-principle demonstration with state-of-the-art atomic quantum memory, in which the polarization degrees of freedom of photons are used as information carriers, and the fidelity of entanglement decoding is verified as approximately 90% [215]. In the same year, Zhu et al. reported the long-distance entanglement-based QSDC experiment, including the security test, information encoding, fiber transmission and decoding, in which the entangled photon pairs are stored in fiber coils and transferred over optical fibers of 0.5 km [216]. More recently, using delay-coding technique instead of a quantum memory which is indispensable in original QSDC protocols, Sun et al. proposed a practical system scheme based on the DL04 protocol and wiretap channel theory, through which their experiment result shows that the reliable communication between two legitimate sides can be implemented [217]. Qi et al. reported an experimental implementation of a practical quantum secure communication system using a protocol based on the DL04 protocol [181], where the system operates with a repetition rate of 1 MHz, and a secure information rate of 50 bps is achieved at a practical meaningful distance of 1.5 km [218].

In the past research, the diversity of QSDC protocol design is mainly studied. However, little attention is paid to the difficulties of protocol implementation, and the security analysis in noisy environment and how to effectively resist noise interference. The protocol may be theoretically secure, but it may be unsafe and difficult to implement in real environment. For example, it is difficult to prepare and manipulate some multi-particle entangled states using current techniques. Therefore, in the next step, in order to facilitate the implementation of the protocol, quantum states that are easy to prepare and manipulate, such as single photon states or Bell states, should be used as much as possible. Moreover, it is of great significance to study DI QSDC, MDI QSDC, DDI QSDC and semi-QSDC in the future.

## V. Quantum Signature

Signature [219] is a cryptographic technology, which is widely used to verify the authenticity and integrity of messages, software or digital documents in real life. Signature is designed to provide a secure method of signing (classical) messages so that the signer can neither deny the messages nor forge recipients or possible attackers of the messages.

Crucially, in a signature scheme, the message is also transferable, which means that if a message is accepted by an honest recipient, it will also be accepted by another recipient if forwarded. Generally speaking, this property distinguishes a signature scheme from an authentication scheme, which ensures that a message is not tampered with by communicators, and which however, does not necessarily guarantee the transmission of messages.

A signature protocol has three goals:

(1) Message integrity: Messages are not changed during transmission;

(2) Message authentication: Message senders are trusted;

(3) Non-repudiation: Message senders cannot deny the creation of messages.

According to the dispute resolution mechanism, non-repudiation is related to transferability, which means that the recipient of the message can check whether it is likely to be accepted by other recipients if the message is forwarded. Informally, a signature protocol is secure if it has three attributes:

(1) Unforgeability: A message sender cannot send information successfully by pretending to be someone else.

(2) Non-repudiation: A signer should not be able to successfully deny that he sent the message signed with his signature.

(3) Transferability: If a recipient accepts the signature, he should be sure that any other recipient will accept the signature.

Unfortunately, the security of classical signature protocols depends on computational complexity assumptions such as the difficulty of finding discrete logarithms or decomposing large primes, which cannot be guaranteed with the emergence of quantum computers. This is the main motivation for developing unconditional secure signature schemes.

Quantum signature can be regarded as a generalization of classical signature protocols in quantum mechanics. It is considered to be a good choice because it can provide unconditional security. Current quantum signature protocols mainly include the following types: Arbitrated quantum signature (AQS) [220-225], quantum homomorphic signature (QHS) [226], blind quantum signature (BQS) [227-233], quantum digital signature (QDS) [234-237], quantum group signature (QGS) [238-241], and quantum proxy signature (QPS) [242].

In an AQS protocol, the signer signs the message and sends it to the recipient, then the recipient verifies the validity of the signature with the help of the arbitrator. A AQS protocol should satisfy [220]:

(1) No modifications and no forgery: Neither the recipient nor the possible attacker can change the signature or additional message after completion. And the signature must not be duplicated.

(2) No disavowals: The signer cannot successfully deny the signature and signature information, and the recipient can identify the signature. Moreover, the recipient could not successfully refuse to receive mails and signatures.

(3) Firm assignments: Each message is reassigned to a signature and cannot be separated thereafter.

(4) Quantum nature: Signatures involve pure quantum mechanical properties without a classical analog. Therefore, signatures are essentially unproductive and can not be denied or forged.

The first AQS protocol was proposed by Zeng et al. in 2002, which takes advantage of the correlation of GHZ states, various qubit operations, and a symmetrical quantum key cryptosystem [220]. Similar to Zeng's scheme, Ref. [221] proposes the protocol using two-particle entangled Bell states. Two protocols with message recovery are proposed in Ref. [222], in which the signature is verified by a designated confirmer using GHZ states. The protocol with an untrusted arbitrator, which does not require a direct quantum link between any two users, is proposed in Ref. [223]. Ref. [224] presents the protocol based on the chained CNOT operations, which encrypts quantum message ensemble. The protocol using insecure quantum channels, which can tolerate more noise in the quantum channels is proposed in Ref. [243]. The protocols with continuous-variable quantum states are proposed in Refs. [225,244].

QDS aims to provide information-theoretic security for the unforgeability, undeniability and transferability of signatures based on the fundamental laws of quantum physics. Unforgeability means that the message is signed by a legitimate signer and has not been modified. Undeniability means that once the signer signed a message, he could not successfully deny that he had done it. Transferability means that when the honest recipient of the signature message accepts the signature, the other honest recipients will also accept it. QDS plays a vital role in many applications such as software distribution, financial transactions and e-mail. Generally, a QDS protocol has two phases, namely, the distribution phase and the message delivery phase. In the distribution phase, the sender sends quantum signatures (a series of quantum states) to the recipient. Then, in the subsequent messaging phase, the sender attaches the message he wants to send to the classical information about the corresponding quantum state sequence. The first QDS protocol was proposed by Gottesman and Chung in 2001 [234]. In this protocol, a sender is allowed to sign a message so that one or more different recipients can verify the signature, and all recipients agree either that the message comes from the sender or that it has been tampered with. The protocol without quantum memory is presented in Ref. [236], which can be implemented using just linear optics and photodetectors that distinguish only between zero and nonzero photons. Ref. [237] presents two schemes which require neither quantum memory nor a multiport, and provides a security proof for the presented QDS schemes against coherent forging attacks.

BQS is a special type of QDS. For the purpose of privacy protection, the message content is disguised before it is signed. That is to say, the anonymity of the message owner can be protected to ensure privacy. In a BQS protocol, the message owner can always get the authentic signature of his message, even if the signer knows nothing about the content he signed. Moreover, the signature can neither be forged nor disavowed by malicious attackers. So far, several BQS protocols have been proposed. Ref. [231] presents the protocol based on the entanglement property of EPR pairs, which uses QKD and one-time pad to ensure the unconditional security and anonymity. Ref. [232] proposes the protocol based on the entangled GHZ states. The protocol based on Two-State Vector Formalism [245] is presented in Ref.[227], in which QKD and one-time pad are adopted to guarantee the unconditional security and signature anonymity. Ref. [229] proposes the batch proxy scheme based on three-dimensional two-particle-entangled quantum system, where a third fully trusted participant (the arbitrator and proxy) is involved. The fair protocol using single photons and hash functions is proposed in Ref. [228]. The protocol with entanglement permutation encryption algorithm is proposed in Ref. [233].

In recent years, several important advances have also been made in experiments. The experimental quantum signature system based on the interference of phase-encoded coherent states of light is demonstrated in Ref. [246], which distributes quantum signatures from one sender to two receivers and prevents messages from forging and repudiation through polarization maintaining optical fiber and photons with a wavelength of 850 nm. Ref. [247] presents the first realization of QDS without quantum memory using only standard linear optical components and photodetectors. Ref. [248] reports the experimental demonstration of QDS over installed optical fiber, which uses the 90 km long differential phase shift QKD technology to achieve approximately one signed bit per second. Ref. [249] reports the realization of the experimental transmission over channel losses of up to 42.8 ± 1.2 dB in a link comprised of 90 km of installed fiber. Ref. [250] presents the experimental realization of quantum signature protocols, in which the transmission distance reaches 2 kilometers. Ref. [235] proposes the first protocol which removes the impractical assumption of authenticated quantum channels, and implements it over a distance of more than 100 km based on single-photon qubit states and phase-randomized weak coherent states. Ref. [251] experimentally signs a one-bit message through an up to 102 km optical fiber. Ref. [252] reports the experimental demonstration of a three-party MDI QDS protocol, which allows the signature of binary messages with a security level of $10^{-7}$. The proof-of-principle demonstration of QDS mediated by MDI QKD is reported in Ref. [253]. The experimental demonstration of quantum signature protocols through a noisy 1.6 km free-space channel is reported in Ref. [254]. Ref. [255] reports the proof-of-principle demonstration of the passive decoy-state QDS system that can avoid leaking the modulation information of decoy states, in which the transmission distance of the system can reach up to 200 km.

Although the theory and experiment of quantum signature have made rapid progress in the past two decades, there are few protocols for multi-user quantum signature, MDI quantum signature and continuous variable quantum signature, all of which deserves more attention. In addition, the research of DDI quantum signature is still blank, which deserves attention because the DDI schemes introduced in QKD have special advantages [57]. What's more, existing BQS protocols fail to verify each party involved, while classical blind signature protocols can do this. The main reason is that classical signature protocols are mainly based on public key systems, while BQS protocols are mainly based on symmetric key systems, which limits the need for multi-party verification. Therefore, the multi-party verification of the protocols still needs a lot of work. Last but not least, designing protocols which can resist various quantum noises is also noteworthy.

## VI. Quantum Private Query

Quantum private query (QPQ) is the quantum scheme of symmetric private information retrieval (SPIR) [256,257], while SPIR is the generalization of the problem of private information retrieval (PIR) problem [258]. A QPQ protocol usually includes two legitimate users: a client (Alice) and a server (Bob). Alice wants to query an element of Bob's remote database to get the value corresponding to the query, and neither revealing which element she is interested in (user privacy) nor knowing anything else about the database (data privacy). In generally, Bob can test the amount of information published, and Alice is assumed to know the address of this element in Bob's database, and the content of it is usually a bit for the sake of simplicity [257].

In 2008, Giovannetti et al. [259] proposed the first QPQ protocol, which allows an exponential reduction in the communication and computational complexity compared with the (quantum or classical) SPIR protocols. Later, they gave a security analysis based on information-disturbance tradeoffs. Since then, QPQ has attracted widespread attention in academia, and many schemes have been proposed in recent years. Ref. [260] proposes the quantum solution to the classical PIR problem, which is more efficient in terms of communication complexity and the number of rounds in comparison with Giovannetti's scheme [259]. Ref. [261] proposes the practical protocol based on QKD, where its basic security is guaranteed by the impossibility to deterministically discriminate nonorthogonal quantum states and the impossibility of superluminal communication. Ref. [262] generalizes the work of Ref. [261] and proposes the flexible protocol based on QKD, where the average number of the key bits Alice obtains can be located on any fixed value the users wanted for any database size. Likewise, based on the protocol proposed in Ref. [261], Ref. [263] proposes the multi-bit protocol which allows the retrieval of several bits in one query. The protocol based on B92 protocol is presented in [264]. Ref. [265] presents the first DI QPQ protocol, which shows that the existing protocols fail to maintain the database security if the entangled states shared between the client and the server are not of a certain form. Ref. [266] proposes the DI protocol with finite number of entangled qubits. Ref. [267] proposes a two-way-four-state-QKD-based protocol to ensure the privacy of both sides of communication. The MDI QPQ protocol with qutrits is proposed in Ref. [268]. Ref. [269] presents the loss-tolerant MDI protocols with single-photon sources. The strategies for resisting joint-measurement attack is presented in Refs. [270,271].

So far, the number of QPQ schemes is very small. In addition, experimental QPQ research has only achieved a few preliminary results [272,273], and there is a long way to go to make them into practice. In the future, more attention should be paid to DI, DDI, MDI protocols, protocols with better noise tolerance, protocol security proof and the security under imperfect sources.

## VII. Some Other Branches

In fact, in addition to QKD, the research of quantum cryptography focuses on various branches of quantum secure multi-party computing, among which QSS is certainly the most widely studied. In recent years, quantum private comparison [274], quantum secure multi-party summation [275], quantum key agreement [276], quantum anonymous voting [277], quantum sealed-bid auction [278], etc., have also received extensive attention. In what follows we first briefly survey these research branches, then introduce some problems and challenges in these branches, by which we wish that it can provide directions for future research.

### 7.1 Quantum private comparison

Assuming that there are $n(n \geq 2)$ participants $P_1, P_2, \cdots, P_n$ and each party $P_i$ $(i \in \{0,1,\ldots,n\})$ has the secret data $x_i$, how to judge whether their data $x_1, x_2, \ldots, x_n$ are the same while protecting the privacy of the data? This problem is called the “Tierce problem” [279], which is essentially a variant of the “millionaires’ problem” proposed by Yao et al. in 1982 [280]. Quantum private comparison (QPC), proposed by Yang et al. in 2009 [274], aims to solve the “Tierce problem” by using the laws of quantum mechanics.

Generally, a QPC protocol should satisfy the following two conditions [281]:

(1) Fairness: All participants get the comparison result simultaneously, in no particular order.

(2) Security: The secret data of each participant is confidential and unavailable to both the other participants and TP. In addition, external attackers (outside the protocol) cannot steal the data of the participants. There are two assumptions about the reliability of TP in QPC protocols [281,282]:

(1) TP is completely honest, that is, he faithfully implements the protocol; He will neither attempt to steal participants’ secret data, nor conspire with dishonest participants to help them steal other participants’ secret data.

(2) TP is semi-honest, that is, he faithfully implements the processes of the protocol without conspiring with any participants, but he can take any possible means to steal the participants’ secret data. From the security point of view, the first assumption is not reasonable, because it is often impossible to find such a person in reality. Therefore, the second assumption is preferred in most existing QPC protocols.

In 2009, Yang et al. [274] proposed the first QPC protocol based on decoy photons and two-photon entangled Einstein-Podolsky-Rosen (EPR) pairs. Later, Chen et al. [283] proposed a new protocol based on triplet entangled GHZ states in 2010. Since then, more and more entangled states, such as GHZ states [284], $\chi$-type states [285], cluster states [286], W states [287,288] and some others [289-293], have been exploited for designing QPC protocols. The early protocols aim to complete the equality comparison between two parties, and then extend to the multi-party situation [292-295] and size comparison [296,297]. In recent years, research on QPC based on various quantum techniques has been extensively studied [298-302]. In addition, there has been a considerable amount of research into the security analysis of protocols [303-322].

## 7.2 Quantum anonymous voting and quantum secure multi-party summation

Quantum anonymous voting (QAV) allows $n(n \geq 2)$ to vote "yes" or "no" on some questions, or vote for some candidates [323]. A tallyman who in charge of counting the votes is usually assumed to honestly follow the protocol, but if any information is available to her, she will have a look. A reliable QAV protocol should satisfy four conditions: privacy, security, verifiability, and eligibility [277]. The first protocol was proposed by Vaccaro et al. in 2007 [323], where entangled states are employed to ensure that the votes are anonymous, and to allow the votes to be tallied. Later, Hillery et al. proposed the protocols where each party (voter) makes a vote through performing one of the two different operations on his(her) qubits [277,324]. Since then, QAV has attracted widespread attention and a series of schemes have been proposed [325-335].

Quantum secure multi-party summation (QSMS) allows $n(n \geq 2)$ parties $P_1, P_2, \cdots, P_n$ to compute a summation function $F(x_1, x_2, \cdots, x_n)$ where $x_i$ is the private datum of $P_i$. In fact, the counting process of votes is the summation process of several binary numbers in QAV protocols. From this point, Du et al. proposed the first quantum secure multi-party summation protocol based on non-orthogonal states, which allows a number to be added to an unknown number secretly [275]. Since then, several protocols were proposed based on various quantum states and technology [337-343].

At present, there is not much work focused on the security analysis of QAV and QSMS, and only a few protocols have been proved unsafe [334], which however, does not mean that other protocols are secure. After all, it is extremely difficult to design a protocol that can resist all known types of attacks.

## 7.3 Quantum sealed-bid auction

Quantum sealed-bid auction (QSBA) was proposed by Naseri in 2009, through QSDC based on GHZ states [278]. A QSBA protocol includes a number of bidders, an auctioneer who sometimes plays the role of a third party or auction host. Bidders simultaneously submit bids to an auctioneer without knowing others' bids, and the highest bidder will ultimately win the bidding. A secure QSBA protocol should meet six basic requirements [278]:

(1) Anonymity: The personal information of a bidder should be kept secret even if the bid is opened. That is, no bidder can obtain others' personal information, except the auction host.

(2) Public verifiability: The winning prices can be verified by any bidder, i.e., every bidder should be able to verify the highest bid which is chosen by the auctioneer, and in this way to prevent the collusion attack between the malicious bidders and the dishonest auctioneer.

(3) Accountability of bidder: The auction cannot be interrupted by any dishonest bidders with fake bids without being detected.

(4) Fairness: The auctioneer cannot assist a malicious bidder in wining the auction without being found by other bidders.

(5) Non-repudiation: An bidder cannot deny the bid price she has cast, and the auction host cannot deny that he has received the bid from the bidder.

(6) Traceability: The bidder who wins the bidding can be identified after the auction.

In the past decade, several QSBA protocols have been designed since Naseri proposed the first protocol. Yang et al. demonstrated that Naseri's protocol is not secure, i.e, a dishonest bidder can obtain all bids of others through double controlled not attack or using fake entangled particles [343]. The protocol with post-confirmation is proposed in Ref. [344], which is a direct application of the multi-particle superdense coding scheme to the auction problem. The protocol in which bidders encode their bids with secret order is proposed in Ref. [345]. The protocols based on single photons and Bell states as the message carrier of bids are proposed in Refs. [346,347] and Ref. [348], respectively. The protocol based on four-particle cluster states is proposed in Ref. [349]. Several other works focus on the protocol security [350-354].

## 7.4 Quantum public key cryptosystem

The concept of public key cryptography (PKC), also known as asymmetric cryptography, was proposed in the 1970s [219,355]. In PKC schemes, such as RSA, ECC or Elgamal, the receiver sends a public key to the sender, and then the sender uses the key to encrypt the data sent to the receiver. The receiver can use his private key to retrieve encrypted data. The security of traditional PKC depends on the hardness of some computational problems, such as integer factorization problem, discrete logarithm problem, etc. However, most PKC schemes, such as RSA, will be broken by future quantum computers [356,357]. Quantum public key cryptosystem (QPKC), as the natural extension of the concept of PKC in the QTM model, has attracted extensive attention in the field of quantum cryptography on the basis of unconditional security and the ability to detect eavesdropping. The main difference between quantum cryptography and QPKC is that the former uses at least one quantum channel and one classical channel, while the latter only uses one classical channel.

The first QPKC protocol (also known as quantum trapdoor one-way function) was proposed by Okamoto et al. in 2000, in which all parties, including senders, receivers and adversaries are modeled as quantum poly-time Turing machines. In 2009, Gao et al. proposed a scheme to construct quantum asymmetric cryptosystems with symmetric keys [358]. In 2015, Parakh proposed the protocol that uses quantum entanglement to exchange arbitrary quantum bits between two parties without discarding any quantum bits during transmission [359]. In the same year, the protocol using non-orthogonal states was proposed [360], in which each party retains a group of non-orthogonal particles as public keys in the key management center and their quantum states as private keys. Almost at the same time, Vlachou et al. [361] proposed the protocol based on quantum walk [362], in which the public key is given by the quantum state generated by the execution of quantum walk. Wu et al. proposed the scheme based on the difficulty of NP-complete problems [363], then they proposed another protocol based on Bell states, which encrypts messages with public keys and decrypts ciphertexts with private keys [364].

In fact, contrary to the widespread concern of PKC in the field of classical cryptography, QPKC has not attracted much attention in academia. Indeed, the role of QPKC in quantum cryptography is less important than that of QKD in terms of current research.

## 7.5 Quantum key agreement

Quantum key agreement (QKA) was proposed by Zhou et al. [276] in 2004, which allow $n(n \geq 2)$ distrustful parties $P_1, P_2, \cdots, P_n$ to agree on a key or a key sequence through common quantum channels. Unlike the QKD in which one party decides the key and distributes it to the other, each party in a QKA protocol contributes to the final shared key, which cannot be determined entirely by some of them. At present, the number of parties involved in a protocol has extended from two [276,365-374] to $n(n > 2)$ [375-388]. In addition, many scholars also pay attention to the security of protocols [389-394].

Generally, in a QKA protocol, one of the participants, $P_i$ $(i \in \{1, 2, \ldots, n\})$ prepares a quantum state and encodes information on it. Then, he takes out part or all of the particles and sends them to the next participant. In this way, the particles eventually return to $P_i$. It can be seen that the particles in the protocol are transmitted in a circular path, in which case however, any participant can steal the secret data of other participants by preparing fake quantum states, making the protocol face great security risks [389-394]. In future research, a third party can be considered to prepare quantum states, and the distribution mode (see the first subgraph in figure 2) can be used to complete key agreement, by which there is no particle exchange between participants.

## 7.6 Quantum dialogue

Quantum dialogue (QD), or the so-called bidirectional QSDC, is an application of QSDC. Different from a system where Alice and Bob use two QSDC schemes to communicate (e.g., one QSDC scheme for Alice-to-Bob communication and the other for Bob-to-Alice communication), QD refers to the two-way quantum communication, i.e. duplex communication, which is carried out simultaneously by both sides, just like the classical telephone communication. In other words, Alice and Bob's messages need to be encoded simultaneously in the same quantum channel.

The first QD protocol was proposed by Nguyen [395], which was proven to be insecure later [396]. Since then, a lot of protocols were proposed, including protocols based on single photons [397-404], Bell states [405-408], GHZ states [409-411], W states [412,413], four-qubit cluster states [414,415]. In addition to the design of protocols, the security of protocols has also attracted a lot of attention in recent years [416-421]. Moreover, considerable efforts have been made in authenticated QD [422-425], and fault-tolerant QD [426-429].

## 7.7 Quantum identity authentication

The original intention of quantum identity authentication (QIA) is to verify the authenticity of the source, so as to protect the message from forgery and denial, and thus resist the attack of intermediaries [430]. That is to say, Eve pretends to be Alice, and then establishes a shared key with Bob. Similarly, she pretended to be Bob and then established a shared key with Alice. Therefore, Eve can easily retrieve messages from Alice and Bob without being detected using established keys. In the past two decades, much attention has been paid to the research of QIA. Many protocols have been proposed, including the hybrid quantum authentication protocol [431,432], the quantum information authentication protocols [433,434], the protocol requiring a trusted authority [435], the protocol without entanglement [436], the multiparty simultaneous protocols [437,438], the quantum deniable authentication protocols [439,440], the protocols based on ping-pong technique [441,442], the scheme in a centralized quantum communication network [443], and the protocols based on entanglement swapping [444,445]. It is noteworthy that most of the schemes are only applicable to specific quantum cryptography protocols, hence it is meaningful to study universal authentication schemes and related theories.

## 7.8 Problems and challenges

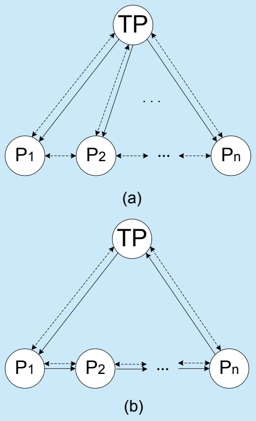
For the above branches of research, designing a secure and efficient protocol is still challenging. As we know, there are many known types of attacks against quantum cryptography protocols or systems. It is impossible to consider all the attacks when designing a protocol. Therefore, a protocol usually only analyze some well-known types of attacks. In addition, the processes of the protocol vary from protocol to protocol, and the tasks that participants undertake in the protocol also vary from protocol to protocol (e.g. whether participants are responsible for preparing quantum states and distributing particles to others, and different computational tasks that participants undertake). In this case, it is often not easy to take into account whether the process of the protocol and the tasks undertaken by the participants pose a potential threat to the security of the protocol. In other words, when designing a protocol, it is often difficult to grasp how external attackers and participants attack protocols. Because of this, a large number of existing protocols have proved unsafe. Moreover, despite the existing types of attacks, there may be many unknown types of attacks against protocols or cryptosystems that have not been invented. In short, designing a secure protocol is often difficult or even impossible.

It is known that cryptography research is oriented to commercial applications, hence the efficiency of protocols should be taken into account when designing protocols. From the perspective of protocol efficiency, how to make protocols more efficient under the condition of ensuring security is also challenging. At present, the common methods to ensure security are as follows:

(1) Preparing additional entangled states and using their entanglement correlation to verify the authenticity of the states, and judge whether there is eavesdropping in quantum channels.

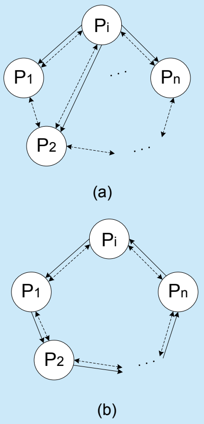
(2) Using QKD to generate keys to encrypt data, that is, quantum one-time pad encryption.

(3) Using decoy photon technology to judge whether there is eavesdropping.



For simplicity, external eavesdroppers are not considered. The solid arrow lines represent quantum channels, and the dashed arrow lines represent classical simultaneous broadcast channels. The model (a) is widely adopted in QPC, QAV and QSBA protocols, and the model (b) is usually adopted by a few QPC and QAV protocols.

**Fig. 2.** *Two typical models of multi-party quantum cryptography protocols with a third party (here we name it TP).*



The model (a) is adopted in some QAV and QSBA protocols, and the model (b) is usually used for QKA.

**Fig. 3.** *Two typical models of multi-party quantum cryptography protocols without a third party.*

(4) Using the entanglement correlation of entangled states to protect data privacy. Generally, a protocol using the method (1) to ensure security seems more effective than other methods, because it can check the authenticity of quantum states and whether there is eavesdropping in channels. However, from the difficulty of the preparation and manipulation of entangled states, this method cannot effectively improve the efficiency of the protocol. As information carriers, multi-particle entangled states are widely used in protocol design. However, the more qubits the entangled state contains, the more difficult it is to prepare, which makes it difficult for the protocol to meet the need of high efficiency. Fortunately, with the continuous progress of related technologies, many important advances have been achieved in the preparation and manipulation of multi-particle entangled states [446-448]. In the near future, the preparation of multi-particle entangled states may not be difficult. Method (2) is very effective in guaranteeing data privacy because it has been proved to be unconditionally secure. However, when both the amount of data and data value are large, this method often consumes a large number of keys, which makes the protocol difficult to meet the need of high efficiency. Method (3) is more effective than method (1) in eavesdropping checking because it is easier to prepare and manipulate a single photon than an entangled state. Method (4) often requires that the expression of a quantum state satisfy certain regularity, hence there are not many protocols designed by this method.

At present, the number of existing protocols in many branches is still very small, thus one can try to design new protocols using different quantum states (e.g. Bell states and GHZ states) in combination with different technologies (e.g. unitary operations and entanglement swapping). Generally, quantum measurement is necessary in a protocol, which is usually used to extract information carried by quantum states. In many cases, protocol design can be accomplished only by quantum measurement, such as semi-quantum cryptography protocols. In addition to measurements, the adoption of other quantum technologies will naturally increase the demand for corresponding devices and technologies. However, high qubit efficiency [449] often cannot be achieved by using quantum measurement alone, where the qubit efficiency usually determines how many states a protocol consumes. Dense coding technology is one of the effective means to improve the qubit efficiency, which has adopted by a lot of existing protocols. In addition, entanglement swapping among various quantum states has some interesting properties, which can provide new ideas and methods for protocol design.

## VIII. Outlook and Conclusion

At present, many research branches in the field of quantum cryptography, especially in the field of QSMC, such as QPC and QKA, do not authenticate the identity of participants. In this case, any outsider can impersonate a legitimate participant to steal the participants' secret data, or send a fake message to others, which seriously threatens the security of the protocol. Thus, it is meaningful to study and design protocols with authentication processes. In addition, the noise problem has always been a widespread concern in academia. Known noise types are diverse, such as the collective dephasing noise, collective-rotation noise, unitary collective noise, decoherence noise and collective amplitude damping noise. Many branches have less research on anti-noise protocols. Therefore, the research on anti-noise protocols is still one of the hot research directions in the future. In addition, one can pay attention to classical cryptography problems and try to find those classical schemes which have not been generalized to quantum mechanics, and which bases security on the assumption of mathematical complexity, and then solve these problems by quantum mechanics methods. Moreover, the research on QKD provide a lot of valuable ideas and solutions for other branches. Using these research results, one can design safer, more efficient and more feasible protocols in experiments. For example, the research and design of DI, MDI, DDI, semi-quantum and fault-tolerant protocols are all worthy of attention. What is more, most of the branches are still at the stage of theoretical research, and there is still a long way to go before the experimental implementation of protocols.

We have reviewed the research and development of some important and well-studied branches in quantum cryptography domain theoretically and experimentally, including QKD, QSS, QSDC etc. We have also reviewed the research and development of some other research branches which are still in the theoretical stage but have attracted wide attention, including QPC, QAV, QSMS, etc. We wish that readers can obtain a general understanding of the hot research directions and progress in quantum cryptography through this paper. We also wish that this paper can provoke the interests of more researchers and carry out research work.

## Acknowledgements

The authors thank the anonymous referees for their significant comments and suggestions to improve the quality of this paper. This work is partially supported by the State Key Program of National Natural Science of China No. 61332019, the Major State Basic Research Development Program of China (973 Program) No. 2014CB340601, the National Science Foundation of China No. 61202386, 61402339, the National Cryptography Development Fund No. MMJJ201701304, the Science and Technology Research Project of Hebei higher education No. QN2017020.

## References

[1] H. G. Zhang, W. B. Han, X. J. Lai, et al., "Survey on cyberspace security," *Science China Information Sciences*, vol. 58, no. 11, 2015, pp. 1-43.

[2] W. J. Luo, G. L. Liu, "Asymmetrical quantum encryption protocol based on quantum search algorithm," *China Communications*, vol. 11, no. 9, 2014, pp. 104-111.

[3] C. H. Bennett, "Quantum crytography," In *Proc.*

*IEEE Int. Conf. Computers, Systems, and Signal Processing*, Bangalore, India, 1984, pp. 175-179.

[4] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Physical review letters*, vol. 67, no. 6, 1991, p. 661.

[5] N. Gisin, et al., "Quantum cryptography," *Reviews of modern physics*, vol. 74, no. 1, 2002, p. 145.

[6] V. Scarani, et al., "The security of practical quantum key distribution," *Reviews of modern physics*, vol. 81, no. 3, 2009, p. 1301.

[7] H. K. Lo, et al., "Secure quantum key distribution," *Nature Photonics*, vol. 8, no. 8, 595, 2014, pp. 58-67.

[8] S. Wiesner, "Conjugate coding," *ACM Sigact News*, vol. 15, no. 1, 1983, pp. 78-88.

[9] E. Diamanti, et al., "Practical challenges in quantum key distribution," *npj Quantum Information*, vol. 2, 2016, p. 16025.

[10] V. Scarani, et al. "The security of practical quantum key distribution," *Reviews of modern physics*, vol. 81, no. 3, 2009, p. 1301.

[11] R. Renner, et al., "Security of quantum key distribution," *International Journal of Quantum Information*, vol. 6, no. 01, 2008, pp. 1-127.

[12] P. W. Shor, et al., "Simple proof of security of the BB84 quantum key distribution protocol," *Physical review letters*, vol. 85, no. 2, 2000, p. 441.

[13] N. J. Cerf, et al. "Security of quantum key distribution using d-level systems," *Physical Review Letters*, vol. 88, no. 12, 2002, p. 127902.

[14] E. Waks, et al., "Security of quantum key distribution with entangled photons against individual attacks," *Physical Review A*, vol. 65, no. 5, 2002, p. 052310.

[15] W. Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," *Physical Review Letters*, vol. 91, no. 5, 2003, p. 057901.

[16] S. Iblisdir, et al., "Security of quantum key distribution with coherent states and homodyne detection," *Physical review letters*, vol. 93, no. 17, 2004, p. 170502.

[17] E. Biham, et al., "A proof of the security of quantum key distribution," *Journal of cryptology*, vol. 19, no. 4, 2006, pp. 381-439.

[18] A. Acín, et al., "Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, vol. 98, no. 23, 2007, p. 230501.

[19] M. McKague, "Device independent quantum key distribution secure against coherent attacks with memoryless measurement devices," *New Journal of Physics*, vol. 11, no. 10, 2009, p. 103037.

[20] Y. Zhao, et al., "Security analysis of an untrusted source for quantum key distribution: passive approach," *New Journal of Physics*, vol. 12, no. 2, 2010, p. 023024.

[21] Ø. Marøy, et al., "Security of quantum key distribution with arbitrary individual imperfections," *Physical Review A*, vol. 82, no. 3, 2010, p. 032337.

[22] L. Sheridan, et al., "Security proof for quantum key distribution using qudit systems," *Physical Review A*, vol. 82, no. 3, 2010, p. 030301.

[23] M. Pawłowski, et al., "Semi-device-independent security of one-way quantum key distribution," *Physical Review A*, vol. 84, no. 1, 2011, p. 010302.

[24] L. Masanes, et al., "Secure device-independent quantum key distribution with causally independent measurement devices," *Nature communications*, vol, 2, 2011, p. 238.

[25] T. Moroder, et al., "Security of distributed-phase-reference quantum key distribution," *Physical review letters*, vol. 109, no. 26, 2012, p. 260501.

[26] A. Leverrier, et al., "Security of continuous-variable quantum key distribution against general attacks," *Physical review letters*, vol. 110, no. 3, 2013, p. 030502.

[27] N. J. Beaudry, et al., "Security of two-way quantum key distribution," *Physical Review A*, vol. 88, no. 6, 2013, p. 062302.

[28] S. Pironio, et al., "Security of device-independent quantum key d istribution in the bounded-quantum-storage model," *Physical Review X*, vol. 3, no. 3, 2013, p. 031007.

[29] L. Masanes, et al., "Full security of quantum key distribution from no-signaling constraints," *IEEE Transactions on Information Theory*, vol. 60, no. 8, 2014, pp. 4973-4986.

[30] U. Vazirani, et al., "Fully device independent quantum key distribution," *Communications of the ACM*, vol. 62, no. 4, 2019, pp. 133-133.

[31] H. Zhang, et al., "Security analysis of orthogonal-frequency-division-multiplexing–based continuous-variable quantum key distribution with imperfect modulation," *Physical Review A*, vol. 97, no. 5, 2018, p. 052328.

[32] C. Lupo, et al., "Continuous-variable measurement-device-independent quantum key distribution: Composable security against coherent attacks," *Physical Review A*, vol. 97, no. 5, 2018, p. 052327.

[33] M. Hayashi, "Upper bounds of eavesdropper's performances in finite-length code with the decoy method," *Physical Review A*, vol. 76, no. 1, 2007, p. 012329.

[34] R. Y. Cai, et al., "Finite-key analysis for practical implementations of quantum key distribution," *New Journal of Physics*, vol. 11, no. 4, 2009, p. 045024.

[35] T. T. Song, et al., "Finite-key analysis for measurement-device-independent quantum key distribution," *Physical Review A*, vol. 86, no. 2, 2012, p. 022332.

[36] M. Curty, et al., "Finite-key analysis for measurement-device-independent quantum key distri-

bution," *Nature communications*, vol. 5, 2014, p. 3732.

[37] C. Zhou, et al., "Finite-key bound for semi-device-independent quantum key distribution," *Optics express*, vol. 25, no. 15, 2017, pp. 16971-16980.

[38] W. Wang, et al., "Finite-key security analysis for quantum key distribution with leaky sources," *New Journal of Physics*, vol. 20, no. 8, 2018, p. 083027.

[39] A. Acín, et al., "Device-independent security of quantum cryptography against collective attacks," *Physical Review Letters*, vol. 98, no. 23, 2007, p. 230501.

[40] J. Barrett, et al., "Memory attacks on device-independent quantum cryptography," *Physical review letters*, vol. 110, no. 1, 2013, p. 010503.

[41] B. Qi, et al., "Time-shift attack in practical quantum cryptosystems," *arXiv preprint quant-ph/*0512080, 2005.

[42] C. H. F. Fung, et al., "Phase-remapping attack in practical quantum-key-distribution systems," *Physical Review A*, vol. 75, no. 3, 2007, p. 032314.

[43] L. Lydersen, et al., "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nature photonics*, vol. 4, no. 10, 2010, p. 686.

[44] H. W. Li, et al., "Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources," *Physical Review A*, vol. 84, no. 6, 2011, p. 062308.

[45] C. C. W. Lim, et al., "Device-independent quantum key distribution with local Bell test," *Physical Review X*, vol. 3, no. 3, 2013, p. 031006.

[46] C. J. Broadbent, et al., "Device-independent quantum key distribution with generalized two-mode Schrödinger cat states," *Physical Review A*, vol. 92, no. 5, 2015, p. 052318.

[47] H. K. Lo, et al., "Measurement-device-independent quantum key distribution," *Physical review letters*, vol. 108, no. 13, 2012, p. 130503.

[48] K. Tamaki, et al., "Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw," *Physical Review A*, vol. 85, no. 4, 2012, p. 042307.

[49] X. Ma, et al., "Alternative schemes for measurement-device-independent quantum key distribution," *Physical Review A*, vol. 86, no. 6, 2012, p. 062319.

[50] Z. Li, et al., "Continuous-variable measurement-device-independent quantum key distribution," *Physical Review A*, vol. 89, no. 5, 2014, p. 052301.

[51] X. C. Ma, et al., "Gaussian-modulated coherent-state measurement-device-independent quantum key distribution," *Physical Review A*, vol. 89, No. 4, 2014, p. 042335.

[52] C. Zhou, et al., "Biased decoy-state measurement-device-independent quantum key distribution with finite resources," *Physical Review A*, vol. 91, no. 2, 2015, p. 022313.

[53] Y. Zhao, et al., "Continuous-variable measurement-device-independent quantum key distribution with virtual photon subtraction," *Physical Review A*, vol. 97, no. 4, 2018, p. 042328.

[54] H. X. Ma, et al., "Continuous-variable measurement-device-independent quantum key distribution with photon subtraction," *Physical Review A*, vol. 97, no. 4, 2018, p. 042329.

[55] C. Y. Li, "Fault-tolerant measurement-device-independent quantum key distribution in a decoherence-free subspace," *Quantum Information Processing*, vol. 17, no. 10, 2018, p. 287.

[56] X. L. Hu, et al., "Efficient measurement-device-independent quantum key distribution without vacuum sources," *Physical Review A*, vol. 98, no. 3, 2018, p. 032303.

[57] C. C. W. Lim, et al., "Detector-device-independent quantum key distribution," *Applied Physics Letters*, vol. 105, no. 22, 2014, p. 221112.

[58] B. Fröhlich, et al., "quantum access network," *Nature*, vol. 501, no. 7465, 2013, p. 69.

[59] S. Sajeed, et al., "Insecurity of detector-device-independent quantum key distribution," *Physical review letters*, vol. 117, no. 25, 2016, p. 250505.

[60] A. Boaron, et al., "Detector-device-independent quantum key distribution: Security analysis and fast implementation," *Journal of Applied Physics*, vol. 120, no. 6, 2016, p. 063101.

[61] K. Wei, et al., "Feasible attack on detector-device-independent quantum key distribution," *Scientific reports*, vo. 7, no. 1, 2017, p. 449.

[62] Boyer, Michel, et al., "Quantum key distribution with classical Bob." *2007 First International Conference on Quantum, Nano, and Micro Technologies (ICQNM'07)*. IEEE, 2007.

[63] M. Boyer, et al., "Semiquantum key distribution," *Physical Review A*, vol. 79, no. 3, 2009, p. 032341.

[64] M. Boyer, et al., "Experimentally feasible protocol for semiquantum key distribution," *Physical Review A*, vol. 96, no. 6, 2017, p. 062335.

[65] H. Lu, et al., "Quantum key distribution with classical Alice," *International Journal of Quantum Information*, vol. 6, no. 06, 2008, pp. 1195-1202.

[66] X. Zou, et al., "Semiquantum-key distribution using less than four quantum states," *Physical Review A*, vol. 79, no. 5, 2009, p. 052312.

[67] A. Maitra, et al., "Eavesdropping in semiquantum key distribution protocol," *Information Processing Letters*, vol. 113, no. 12, 2013, pp. 418-422.

[68] W. O. Krawec, "Mediated semiquantum key distribution," *Physical Review A*, vol. 91, no. 3, 2015, p. 032323.

[69] X. Zou, et al., "Semiquantum key distribution without invoking the classical party's measurement capability," *Quantum Information Processing*, vol. 14, no. 8, 2015, pp. 2981-2996.

[70] Z. R. Liu, et al., "Mediated Semi-Quantum Key Distribution Without Invoking Quantum Measurement," *Annalen der Physik*, vol. 530, no. 4, 2018, p. 1700206.

[71] Z. Sun, et al., "Semi-quantum key distribution protocol using Bell state," *arXiv preprint arXiv:1106.2910* (2011).

[72] J. Wang, et al., "Semiquantum key distribution using entangled states," *Chinese Physics Letters*, vol. 28, no. 10, 2011, p. 100301.

[73] K. F. Yu, et al., "Authenticated semi-quantum key distribution protocol using Bell states," *Quantum Information Processing*, vol. 13, no. 6, 2014, pp. 1457-1465.

[74] Q. Li, et al., "Semiquantum key distribution with secure delegated quantum computation," *Scientific reports*, vol. 6, 2016, p. 19898.

[75] J. He, et al., "Measurement-device-independent semiquantum key distribution," *International Journal of Quantum Information*, vol. 16, no. 02, 2018, p. 1850012.

[76] K. N. Zhu, et al., "Semi-quantum key distribution protocols with GHZ states," *International Journal of Theoretical Physics*, vol. 57, no. 12, 2018, pp. 3621-3631.

[77] W. O. Krawec, "Restricted attacks on semi-quantum key distribution protocols," *Quantum Information Processing*, vol. 13, no. 11, 2014, pp. 2417-2436.

[78] Y. G. Yang, et al., "Trojan-horse attacks on quantum key distribution with classical Bob," *Quantum Information Processing*, vol. 14, no. 2, 2015, pp. 681-686.

[79] W. O. Krawec, "Security of a semi-quantum protocol where reflections contribute to the secret key," *Quantum Information Processing*, vol. 15, no. 5, 2016, pp. 2067-2090.

[80] C. H. Bennett, et al., "Experimental quantum cryptography," *Journal of cryptology*, vol 5, no. 1, 1992, pp. 3-28.

[81] B. K. Park, et al., "QKD system with fast active optical path length compensation," *SCIENCE CHINA Physics, Mechanics & Astronomy*, vol. 60, no. 6, 2017, p. 060311.

[82] A. Muller, et al., "Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km," *EPL (Europhysics Letters)*, vol. 23, no. 6, 1993, p. 383.

[83] J. C. Boileau, et al., "Robust polarization-based quantum key distribution over a collective-noise channel," *Physical review letters*, vol. 92, no. 1, 2004, p. 017901.

[84] C. Z. Peng, et al., "Experimental long-distance decoy-state quantum key distribution based on polarization encoding," *Physical review letters*, vol. 98, no. 1, 2007, p. 010505.

[85] J. Lodewyck, et al., "Quantum key distribution over 25 km with an all-fiber continuous-variable system," *Physical Review A*, vol. 76 no. 4, 2007, p. 042305.

[86] B. Qi, et al., "Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers," *Physical Review A*, vol. 76, no. 5, 2007, p. 052323.

[87] G. Ribordy, et al., "Long-distance entanglement-based quantum key distribution," *Physical Review A*, vol. 63, no. 1, 2000, p. 012309.

[88] M. Peev, et al., "The SECOQC quantum key distribution network in Vienna," *New Journal of Physics*, vol. 11, no. 7, 2009, p. 075001.

[89] A. Treiber, et al., "A fully automated entanglement-based quantum cryptography system for telecom fiber networks," *New Journal of Physics*, vol. 11, no. 4, 2009, p. 045013.

[90] D. Stucki, et al., "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," *New Journal of Physics*, vol. 13, no. 12, 2011, p. 123001.

[91] M. Sasaki, et al., "Field test of quantum key distribution in the Tokyo QKD Network," *Optics express*, vol. 19, no. 11, 2011, pp. 10387-10409.

[92] A. R. Dixon, et al., "Continuous operation of high bit rate quantum key distribution," *Applied Physics Letters*, vol. 96, no. 16, 2010, p. 161102.

[93] J. F. Dynes, et al., "Efficient entanglement distribution over 200 kilometers," *Optics express*, vol. 17, no. 14, 2009, p. 11440-11449.

[94] A. Mirza, et al., "Recent findings from the quantum network in Durban," *In AIP Conference Proceedings*, vol. 1363, no. 1, 2011, pp. 35-38.

[95] S. Wang, et al., "2 GHz clock quantum key distribution over 260 km of standard telecom fiber," *Optics letters*, vol. 37, no. 6, 2012, p. 1008-1010.

[96] H. Takesue, et al., "10-GHz clock differential phase shift quantum key distribution experiment," *Optics express*, vol. 14, no. 20, 2006, p. 9522-9530.

[97] Takesue, Hiroki, et al., "Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors," *Nature photonics*, vol. 1, no. 6, 2007, p. 343.

[98] Marcikic, Ivan, et al., "Distribution of time-bin entangled qubits over 50 km of optical fiber," *Physical Review Letters*, vol. 93, no. 18, 2004, p. 180502.

[99] Diamanti, Eleni, et al., "100 km differential phase shift quantum key distribution experiment with low jitter up-conversion detectors," *Optics express*, vol. 14, no. 26, 2006, pp. 13073-13082.

[100] Stucki, Damien, et al., "High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres," *New Journal of Physics*, vol. 11, no. 7, 2009, p. 075003.

[101] Hughes, Richard J., et al., "Practical free-space quantum key distribution over 10 km in day-

light and at night," *New journal of physics*, vol. 4, no. 1, 2002, p. 43.

[102] Alléaume, Romain, et al., "Experimental open-air quantum key distribution with a single-photon source," *New Journal of physics*, vol. 6, no. 1, 2004, p. 92.

[103] Ursin, Rupert, et al., "Entanglement-based quantum communication over 144 km," *Nature physics*, vol. 3, no. 7, 2007, p. 481.

[104] Jacobs, B. C., and J. D. Franson. "Quantum cryptography in free space," *Optics Letters*, vol. 21, no. 22, 1996, pp. 1854-1856.

[105] Buttler, W. T., et al., "Free-space quantum-key distribution," *Physical Review A*, vol. 57, no. 4, 1998, p. 2379.

[106] Buttler, William T., et al., "Daylight quantum key distribution over 1.6 km," *Physical Review Letters*, vol. 84, no. 24, 2000, p. 5652.

[107] Kurtsiefer, Christian, et al., "Quantum cryptography: A step towards global key distribution," *Nature*, vol. 419, no. 6906, 2002, p. 450.

[108] Schmitt-Manderbach, Tobias, et al., "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Physical Review Letters*, vol. 98, no, 1, 2007, p. 010504.

[109] C. Erven, et al., "Entangled quantum key distribution over two free-space optical links," *Optics express*, vol. 16, no. 21, 2008, pp. 16840-16853.

[110] Peloso, Matthew P., et al., "Daylight operation of a free space, entanglement-based quantum key distribution system," *New Journal of Physics*, vol. 11, no. 4, 2009, p. 045007.

[111] Buttler, W. T., et al., "Practical free-space quantum key distribution over 1 km," *Physical Review Letters*, vol. 81, no. 15, 1998, p. 3283.

[112] Ursin, Rupert, et al., "Space-quest, experiments with quantum entanglement in space," *Europhysics News*, vol. 40, no. 3, 2009, pp. 26-29.

[113] Scheidl, Thomas, et al., "Feasibility of 300 km quantum key distribution with entangled states," *New Journal of Physics*, vol. 11, no. 8, 2009, p. 085002.

[114] Laing, Anthony, et al., "Reference-frame-independent quantum key distribution," *Physical Review A*, vol. 82, no. 1, 2010, p. 012304.

[115] J. Y. Wang, et al., "Direct and full-scale experimental verifications towards ground–satellite quantum key distribution," *Nature Photonics*, vol. 7, no. 5, 2013, p. 387.

[116] Nauerth, Sebastian, et al., "Air-to-ground quantum communication," *Nature Photonics*, vol. 7, no. 5, 2013, p. 382.

[117] Vallone, Giuseppe, et al., "Experimental satellite quantum communications," *Physical Review Letters*, vol. 115, no. 4, 2015, p. 040502.

[118] Liao, Sheng-Kai, et al., "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, 2017, p. 43.

[119] S. K. Liao, et al., "Long-distance free-space quantum key distribution in daylight towards inter-satellite communication," *Nature Photonics*, vol. 11, no. 8, 2017, p. 509.

[120] Townsend, P. D., et al., "Design of quantum cryptography systems for passive optical networks," *Electronics Letters*, vol. 30, no. 22, 1994, pp. 1875-1877.

[121] Townsend, Paul D., "Quantum cryptography on multiuser optical fibre networks," *Nature*, vol. 385, no. 6611, 1997, p. 47.

[122] Brassard, Gilles, et al., "Multiuser quantum key distribution using wavelength division multiplexing," *Applications of Photonic Technology, International Society for Optics and Photonics*, vol. 5260, 2003.

[123] Kumavor, Patrick D., et al., "Experimental multiuser quantum key distribution network using a wavelength-addressed bus architecture," *Journal of lightwave technology*, vol. 24, no. 8, 2006, pp. 3103-3106.

[124] T. Zhang, et al., "Extensible router for a quantum key distribution network," *Physics Letters A*, vol. 372, no. 22, 2008, pp. 3957-3962.

[125] Chen, Wei, et al., "Field experiment on a "star type" metropolitan quantum key distribution network," *IEEE Photonics Technology Letters*, vol. 21, no. 9, 2009, pp. 575-577.

[126] F. X. Xu, et al., "Field experiment on a robust hierarchical metropolitan quantum cryptography network," *Chinese Science Bulletin*, vol. 54, no. 17, 2009, pp. 2991-2997.

[127] S. Wang, et al., "Field test of wavelength-saving quantum key distribution network," *Optics letters*, vol. 35, no. 14, 2010, pp. 2454-2456.

[128] C. Yang, et al., "Quantum key distribution network: Optimal secret-key-aware routing method for trust relaying," *China Communications*, vol. 15, no. 2, 2018, pp. 33-45.

[129] Da Silva, T. Ferreira, et al., "Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits," *Physical Review A*, vol. 88, no. 5 2013, p. 052303.

[130] Y. Liu, et al., "Experimental measurement-device-independent quantum key distribution," *Physical review letters*, vol. 111, no. 13, 2013, p. 130502.

[131] W. Qin, et al., "Efficient implementation of the decoy-state measurement-device-independent quantum key distribution with heralded single-photon sources," *Physical Review A*, vol. 88, no. 5, 2013, p. 052332.

[132] F. H. Xu, et al., "Practical aspects of measurement-device-independent quantum key distribution," *New Journal of Physics*, vol. 15, no. 11, 2013, p. 113007.

[133] C. Wang, et al., "Phase-reference-free experiment of measurement-device-independent quantum key distribution," *Physical review letters*, vol. 115, no. 16, 2015, p. 160502.

[134] Y. L. Tang, et al., "Field test of measurement-de-

vice-independent quantum key distribution," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, 2014, pp. 116-122.

[135] H. L. Yin, et al., "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Physical review letters*, vol. 117, no. 19, 2016, p. 190501.

[136] G. Z. Tang et al., "Experimental asymmetric plug-and-play measurement-device-independent quantum key distribution," *Physical Review A*, vol. 94, no. 3, 2016, p. 032326.

[137] Z. Y. Tang et al., "Experimental measurement-device-independent quantum key distribution with imperfect sources," *Physical Review A*, vol. 93, no. 4, 2016, p. 042308.

[138] Wiechers, Carlos, et al., "After-gate attack on a quantum cryptosystem," *New Journal of Physics*, vol. 13, no. 1, 2011, p. 013043.

[139] Weier, Henning, et al., "Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors," *New Journal of Physics*, vol. 13, no, 7, 2011, p. 073024.

[140] Jain, Nitin, et al., "Device calibration impacts security of quantum key distribution," *Physical Review Letters*, vol. 107, no. 11, 2011, p. 110501.

[141] Adi. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, 1979, pp. 612-613.

[142] George Robert. Blakley, "Safeguarding cryptographic keys," *Proceedings of the national computer conference*. vol. 48. no. 313. 1979.

[143] Halpern, Joseph, et al., "Rational secret sharing and multiparty computation," *Proceedings of the thirty-sixth annual ACM symposium on Theory of computing*. ACM, 2004.

[144] Hillery, Mark, et al., "Quantum secret sharing," *Physical Review A*, vol. 59, no. 3, 1999, p. 1829.

[145] Karlsson, Anders, et al., "Quantum entanglement for secret sharing and secret splitting," *Physical Review A*, vol. 59, no. 1, 1999, p. 162.

[146] Żukowski, M., et al., "Quest for GHZ states," *Acta Phys. Pol. A*, vol. 93, 1998, 187.

[147] Z. J. Zhang, et al., "Multiparty quantum secret sharing," *Physical Review A,* vol. 71, no. 4, 2005, P. 044301.

[148] F. L. Yan, and T. Gao. "Quantum secret sharing between multiparty and multiparty without entanglement," *Physical Review A*, vol. 72, no.1, 2005, p. 012304.

[149] Mohajer, Razieh, et al., "Quantum secret sharing using single states," 2016 8th *International Symposium on Telecommunications (IST)*. IEEE, 2016.

[150] Karimipour, Vahid, et al., "Quantum secret sharing and random hopping: using single states instead of entanglement," *Physical Review A*, vol. 92, no. 3, 2015, p. 030301.

[151] F. G. Deng, et al., "Bidirectional quantum secret sharing and secret splitting with polarized single photons.," *Physics Letters A*, vol. 337. No. 4-6, 2005, pp. 329-334.

[152] Z. J. Zhang, et al., "Multiparty quantum secret sharing of classical messages based on entanglement swapping," *Physical Review A*, vol. 72, no. 2, 2005, p. 022303.

[153] Y. M. Li, et al., "Multiparty secret sharing of quantum information based on entanglement swapping," *Physics Letters A*, vol. 324, no. 5-6, 2004, pp. 420-424.

[154] Karimipour, Vahid, et al., "Entanglement swapping of generalized cat states and secret sharing," *Physical Review A*, vol, 65, no. 4, 2002, p. 042320.

[155] Y. Q. Zhang, X. R. Jin, and S. Zhang. "Secret sharing of quantum information via entanglement swapping in cavity QED," *Physics Letters A*, vol. 341, no. 5-6, 2005, pp. 380-384.

[156] Y. Q. Zhang, et al., "Secret sharing of quantum information via entanglement swapping," *Chinese Physics* vol. 15, no. 10, 2006, p. 2252.

[157] L. Y. Hsu, et al., "Quantum secret sharing using product states," *Physical Review A*, vol. 71, no. 2, 2005, p. 022321.

[158] F. G. Deng, et al., "Circular quantum secret sharing," *Journal of Physics A: Mathematical and General*, vol. 39, no. 45, 2006, p. 14089.

[159] Y. G. Yang, and Q. Y. Wen, "Circular threshold quantum secret sharing," *Chinese Physics B*, vol. 17, no. 2, 2008, p. 419.

[160] Lin, Jason, and Tzonelih Hwang. "New circular quantum secret sharing for remote agents," *Quantum information processing*, vol. 12, no. 1, 2013, pp. 685-697.

[161] Q. Li, et al., "Semiquantum secret sharing using entangled states," *Physical Review A*, vol. 82, no. 2 2010, p. 022303.

[162] A. H. Yin, et al., "A novel semi-quantum secret sharing scheme using entangled states," *Modern Physics Letters B*, vol. 32, no. 22, 2018, p. 1850256.

[163] L. X. Li, et al., "Quantum secret sharing with classical Bobs," *Journal of Physics A: Mathematical and Theoretical*, vol. 46, no. 4, 2013, p. 045304.

[164] Y. WANG, et al. "Measurement-device-independent quantum secret sharing and quantum conference based on Gaussian cluster state," *SCIENCE CHINA Information Sciences*, vol. 62, no. 7, 2019, p. 072501.

[165] X. Q. Yang, et al. "Measurement-device-independent quantum secret sharing," *arXiv preprint arXiv:1608.00114*, 2016.

[166] X. Q. Yang, et al. "Detector-device-independent quantum secret sharing with source flaws," *Scientific reports*, vol. 8, no. 1, 2018, p. 5728.

[167] Tittel, Wolfgang, Hugo Zbinden, and Nicolas Gisin. "Experimental demonstration of quantum secret sharing," *Physical Review A*, vol. 63, no. 4, 2001, p. 042301.

[168] Walls, Dan. "Growing expectations from

squeezed states of light," Nature, vol. 324, no. 6094, 1986, p. 210.

[169] Tyc, Tomáš, and Barry C. Sanders. "How to share a continuous-variable quantum secret by optical interferometry," *Physical Review A*, vol. 65, no.4, 2002, p. 042310.

[170] Lance, Andrew M., et al. "Continuous variable (2, 3) threshold quantum secret sharing schemes," *New Journal of Physics*, vol. 5, no. 1, 2003, p. 4.

[171] Schmid, Christian, et al. "Experimental single qubit quantum secret sharing," *Physical review letters*, vol. 95, no. 23, 2005, p. 230505.

[172] Y. A. Chen et al., "Experimental quantum secret sharing and third-man quantum cryptography," *Physical review letters*, vol, 95, no. 20, 2005, p. 200502.

[173] Gaertner, Sascha, et al., "Experimental demonstration of four-party quantum secret sharing," *Physical Review Letters*, vol. 98, no. 2, 2007, p. 020503.

[174] Weinfurter, Harald, and Marek Żukowski. "Four-photon entanglement from down-conversion," *Physical Review A*, vol. 64, no. 1, 2001, p. 010102.

[175] Bogdanski, Jan, et al., "Experimental quantum secret sharing using telecommunication fiber," *Physical Review A*, vol. 78, no. 6, 2008, p. 062307.

[176] Bogdanski, Jan, et al., "Sagnac secret sharing over telecom fiber networks," *Optics express*, vol. 17, no. 2, 2009, pp. 1055-1063.

[177] H. Q. Ma, et al., "Experimental single qubit quantum secret sharing in a fiber network configuration," *Optics letters*, vol. 38, no. 13, 2013, pp. 4494-4497.

[178] K. J. Wei, et al., "Experimental circular quantum secret sharing over telecom fiber network," *Optics express*, vol. 21, no. 14, 2013, pp. 16663-16669.

[179] G. L. Long, and X. S. Liu, "Theoretically efficient high-capacity quantum-key-distribution scheme," *Physical Review A*, vol. 65, no. 3, 2002, p. 032302.

[180] F. G. Deng, G. L. Long, and X. S. Liu. "Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block," *Physical Review A*, vol. 68, no. 4, 2003, p. 042317.

[181] F. G. Deng, G. L. Long, "Secure direct communication with a quantum one-time pad." *Physical Review A*, vol. 69, no. 5, 2004, p. 052319.

[182] G. L. Long, et al., "Quantum secure direct communication and deterministic secure quantum communication," *Frontiers of Physics in China*, vol. 2, no. 3,2007, pp. 251-272.

[183] Z. R. Zhou, et al., "Measurement-device-independent quantum secure direct communication," *arXiv preprint arXiv:*1805.07228, 2018.

[184] F. Z. Wu, et al., "High-capacity quantum secure direct communication with two-photon six-qubit hyperentangled states," *Science China Physics, Mechanics & Astronomy*, vol. 60, no. 12, 2017, p. 120313.

[185] S. S. Chen, et al., "Three-step three-party quantum secure direct communication," *SCIENCE CHINA Physics, Mechanics & Astronomy*, vol. 61, no. 9, 2018, p. 90312.

[186] Y. Chang, et al., "Quantum secure direct communication and authentication protocol with single photons," *Chinese science bulletin*, vol. 58, no. 36, 2013, pp. 4571-4576.

[187] Y. G. Yang, et al., "Robust QKD-based private database queries based on alternative sequences of single-qubit measurements.," *SCIENCE CHINA Physics, Mechanics & Astronomy*, vol. 60, no. 12, 2017, p. 120311.

[188] Boström, Kim, and Timo Felbinger. "Deterministic secure direct communication using entanglement," *Physical Review Letters*, vol. 89, no. 18, 2002, p. 187902.

[189] G. Gao, M. Fang, and R. M. Yang, "Quantum secure direct communication by swapping entanglements of 3×3-dimensional Bell states," *International Journal of Theoretical Physic*s, vol. 50, no. 3, 2011, pp. 882-887.

[190] F. G. Deng, et al., "Quantum secure direct communication network with Einstein–Podolsky–Rosen pairs," *Physics Letters A*, vol. 359, no. 5, 2006, pp. 359-365.

[191] L. Yang, et al., "Quantum communication scheme based on quantum teleportation," *Acta Physica Sinica*, vol. 66, no. 23, 2017.

[192] H. J. Cao, and H. S. Song, "Quantum secure direct communication scheme using a W state and teleportation," *Physica Scripta*, vol. 74, no. 5, 2006, p. 572.

[193] J. Li, et al., "A quantum secure direct communication protocol based on a five-particle cluster state and classical XOR operation," *Chinese Physics C*, vol. 36, no. 1, 2012, p. 31.

[194] T. Gao, F. L. Yan, and Z. X. Wang, "Deterministic secure direct communication using GHZ states and swapping quantum entanglement," *Journal of Physics A: Mathematical and General*, vol. 38, no. 25, 2005, p. 5761.

[195] J. Wang, Q. Zhang, and C. J. Tang, "Multiparty controlled quantum secure direct communication using Greenberger–Horne–Zeilinger state," *Optics Communications*, vol. 266, no. 2, 2006, pp. 732-737.

[196] Z. X. Man, Y. J. Xia, and Nguyen Ba An. "Quantum secure direct communication by using GHZ states and entanglement swapping," *Journal of Physics B: Atomic, Molecular and Optical Physics*, vol. 39, no. 18, 2006, p. 3855.

[197] C. Wang, F. G. Deng, and G. L. Long, "Multi-step quantum secure direct communication using multi-particle Green–Horne–Zeilinger state," *Optics communications*, vol. 253, no. 1-3, 2005, pp. 15-20.

[198] Y. Xia, and H. S. Song, "Controlled quantum

secure direct communication using a non-symmetric quantum channel with quantum superdense coding," *Physics Letters A*, vol. 364, no. 2, 2007, pp. 117-122.

[199] S. K. Wang, X. W. Zha, and H. Wu. "Controlled secure direct communication with seven-qubit entangled states," *International Journal of Theoretical Physics*, vol. 57, no.1, 2018, pp. 48-58.

[200] D. Li, et al. "Quantum secure direct communication using a six-qubit maximally entangled state with dense coding," International Journal of Quantum Information, vol. 7, no. 03, 2009, pp. 645-651.

[201] C. H. Yu, G. D. Guo, and S. Lin. "Quantum secure direct communication with authentication using two nonorthogonal states," *International Journal of Theoretical Physics*, vol. 52, no. 6 , 2013, pp. 1937-1945.

[202] G. Y. Wang, X. M. Fang, and X. H. Tan, "Quantum secure direct communication with cluster state," *Chinese Physics Letters*, vol. 23, no. 10, 2006, p. 2658.

[203] W. F. Cao, et al., "Quantum secure direct communication with cluster states," *Science China Physics, Mechanics and Astronomy*, vol. 53, no. 7, 2010, pp. 1271-1275.

[204] X. H. Li, et al., "Quantum secure direct communication with quantum encryption based on pure entangled states," *Chinese Physics*, vol. 16, no. 8, 2007, p. 2149.

[205] L. Song, et al., "Quantum secure direct communication with χ-type entangled states," *Physical Review A*, vol. 78, no. 6, 2008, p. 064304.

[206] C. Wang, et al., "Quantum secure direct communication with high-dimension quantum superdense coding," *Physical Review A*, vol. 71, no. 4, 2005, p. 044305.

[207] F. G. Deng, et al., "Quantum secure direct communication network with superdense coding and decoy photons," P*hysica Scripta*, vol. 76, no. 1, 2007, p. 25.

[208] Z. H. Liu, et al., "Quantum secure direct communication with optimal quantum superdense coding by using general four-qubit states," *Quantum information processing*, vol. 12, no. 1, 2013, pp. 587-599.

[209] Y. B. Zhan, et al., "Quantum secure direct communication by entangled qutrits and entanglement swapping," *Optics Communications*, vol. 282, no. 23, 2009, pp. 4633-4636.

[210] Kao, Shih-Hung, and Tzonelih Hwang. "Multiparty controlled quantum secure direct communication based on quantum search algorithm," *Quantum information processing*, vol. 12, no. 12, 2013, pp. 3791-3805.

[211] T. Y. Wang, et al., "Multiparty controlled quantum secure direct communication with phase encryption," *International Journal of Quantum Information*, vol. 9, no. 02, 2011, pp. 801-807.

[212] Lee, Hwayean, et al., "Quantum direct communication with authentication," *Physical Review A*, vol. 73, no. 4, 2006, p. 042305.

[213] Niu, Peng-Hao, et al., "Measurement-device-independent quantum communication without encryption," *Science bulletin*, vol. 63, no. 20, 2018, pp. 1345-1350.

[214] J. Y. Hu, et al., "Experimental quantum secure direct communication with single photons," *Light: Science & Applications*, vol. 5, no. 9, 2016, p. e16144.

[215] W. Zhang, et al., "Quantum secure direct communication with quantum memory," *Physical review letters*, vol. 118, no. 22, 2017, p. 220501.

[216] F. Zhu, et al., "Experimental long-distance quantum secure direct communication," *Science Bulletin*, vol. 62, no. 22, 2017, pp. 1519-1524.

[217] Z. Sun, et al., "Design and Implementation of a Practical Quantum Secure Direct Communication System," 2018 *IEEE Globecom Workshops* (GC Wkshps). IEEE, 2018.

[218] R. Y. Qi, et al., "Implementation and security analysis of practical quantum secure direct communication," *Light: Science & Applications*, vol. 8, no. 1, 2019, p. 22.

[219] Diffie, Whitfield, and Martin Hellman. "New directions in cryptography," *IEEE transactions on Information Theory*, vol. 22, no. 6, 1976, pp. 644-654.

[220] G. H. Zeng, et al., "Arbitrated quantum-signature scheme," *Physical review A*, vol. 65, no. 4, 2002, p. 042312.

[221] Q. Li, et al. "Arbitrated quantum signature scheme using Bell states," *Physical Review A*, vol. 79, no. 5, 2009, p. 054307.

[222] Lee, Hwayean, et al., "Arbitrated quantum signature scheme with message recovery," *Physics Letters A*, vol. 321, no. 5-6, 2004, pp. 295-300.

[223] Y. G. Yang, et al., "Arbitrated quantum signature with an untrusted arbitrator," *The European Physical Journal D*, vol. 61, no. 3, 2011, pp. 773-778.

[224] F. G. Li, et al., "An arbitrated quantum signature protocol based on the chained CNOT operations encryption," *Quantum Information Processing*, vol. 14, no. 6, 2015, pp. 2171-2181.

[225] Y. Y. Feng, et al., "Arbitrated quantum signature scheme with continuous-variable squeezed vacuum states," *Chinese Physics B*, vol. 27, no. 2, 2018, p. 020302.

[226] T. Shang, et al., "Quantum homomorphic signature," *Quantum Information Processing*, vol. 14, no. 1, 2015, pp. 393-410.

[227] Q. Su, et al., "Quantum blind signature based on two-state vector formalism," *Optics Communications*, vol. 283, no. 21, 2010, pp. 4408-4410.

[228] T. Y. Wang, et al., "Fair quantum blind signatures," Chinese physics B, vol. 19, no. 6, 2010, p. 060307.

[229] J. J. Shi, et al., "Batch proxy quantum blind signature scheme," *Science China Information Sci-*

*ences*, vol. 56, no. 5, 2013, pp. 1-9.

[230] W. Li, et al., "Blind quantum signature with controlled Four-Particle cluster states," *International Journal of Theoretical Physics*, vol. 56, no. 8, 2017, pp. 2579-2587.

[231] X. J. Wen, et al., "A weak blind signature scheme based on quantum cryptography," *Optics Communications*, vol. 282, 2009, pp. 666-669.

[232] M. M. Wang, et al., "A blind quantum signature protocol using the GHZ states," *Science China Physics, Mechanics and Astronomy*, vol. 56, no. 9, 2013, pp. 1636-1641.

[233] X. P. Lou, et al., "A weak quantum blind signature with entanglement permutation," *International Journal of Theoretical Physics*, vol. 54, no. 9, 2015, pp. 3283-3292.

[234] Gottesman, Daniel, and Isaac Chuang, "Quantum digital signatures," *arXiv preprint quant-ph/*0105032, 2001.

[235] H. L. Yin, et al., "Practical quantum digital signature," *Physical Review A*, vol. 93, no. 3, 2016, p. 032316.

[236] Dunjko, Vedran, Petros Wallden, and Erika Andersson. "Quantum digital signatures without quantum memory," *Physical review letters*, vol. 112, no. 4, 2014, p. 040502.

[237] Wallden, Petros, et al., "Quantum digital signatures with quantum-key-distribution components," *Physical Review A*, vol. 91, no. 4, 2015, p. 042304.

[238] Y. G. Yang, et al., "Quantum threshold group signature," *Science in China Series G: Physics, Mechanics and Astronomy*, vol. 51, no. 10, 2008, pp. 1505-1514.

[239] X. J. Wen, et al., "A group signature scheme based on quantum teleportation," *Physica Scripta*, vol. 81, no. 5, 2010, p. 055001.

[240] J. J. Shi, et al., "A multiparty quantum proxy group signature scheme for the entangled-state message with quantum Fourier transform," *Quantum Information Processing*, vol. 10, no. 5, 2011, pp. 653-670.

[241] G. B. Xu, et al., "A novel quantum group signature scheme without using entangled states," *Quantum Information Processing*, vol. 14, no. 7, 2015, pp. 2577-2587.

[242] T. Y. Wang, et al., "One-time proxy signature based on quantum cryptography," *Quantum Information Processing*, vol. 11, no. 2, 2012, pp. 455-463.

[243] Amiri, Ryan, et al., "Secure quantum signatures using insecure quantum channels," *Physical Review A*, vol. 93, no. 3, 2016, p. 032325.

[244] Y. Guo, et al. "Arbitrated quantum signature scheme with continuous-variable coherent states," *International Journal of Theoretical Physics*, vol. 55, no. 4, 2016, pp. 2290-2302.

[245] Aharonov, Yakir, and Lev Vaidman. "The two-state vector formalism: an updated review," *Time in quantum mechanics*. Springer, Berlin, Heidelberg, 2008, pp.399-447.

[246] Clarke, Patrick J., et al., "Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light," *Nature communications*, vol. 3, no. 2012, p. 1174.

[247] Collins, Robert J., et al., "Realization of quantum digital signatures without the requirement of quantum memory," *Physical review letters*, vol. 113, no. 4, 2014, p. 040502.

[248] Collins, Robert J., et al., "Experimental transmission of quantum digital signatures over 90 km of installed optical fiber using a differential phase shift quantum key distribution system," *Optics letters*, vol. 41, no. 21, 2016, pp. 4883-4886.

[249] Collins, Robert J., et al., "Experimental demonstration of quantum digital signatures over 43 dB channel loss using differential phase shift quantum key distribution," *Scientific reports*, vol. 7, no. 1, 2017, p. 3235.

[250] Donaldson, Ross J., et al., "Experimental demonstration of kilometer-range quantum digital signatures," *Physical Review A*, vol. 93, no. 1, 2016, p. 012329.

[251] H. L. Yin, et al., "Experimental quantum digital signature over 102 km," *Physical Review A*, vol. 95, no. 3, 2017, p. 032334.

[252] H. L. Yin, et al., "Experimental measurement-device-independent quantum digital signatures over a metropolitan network," *Physical Review A*, vol. 95, no. 4, 2017, p. 042338.

[253] Roberts, G. L., et al., "Experimental measurement-device-independent quantum digital signatures," *Nature communications*, vol. 8, no. 1, 2017, p. 1098.

[254] Croal, Callum, et al., "Free-space quantum signatures using heterodyne measurements," *Physical review letters*, vol. 117, no. 10, 2016, p. 100503.

[255] C. H. Zhang, et al., "Proof-of-principle demonstration of passive decoy-state quantum digital signatures over 200 km.," *Physical Review Applied*, vol. 10, no. 3, 2018, p. 034033.

[256] Gertner, Yael, et al., "Protecting data privacy in private information retrieval schemes," *Journal of Computer and System Sciences*, vol. 60, no. 3, 2000, pp. 592-629.

[257] F. Gao, et al., "Quantum private query: A new kind of practical quantum cryptographic protocol," *SCIENCE CHINA Physics, Mechanics & Astronomy*, vol. 62, no. 7, 2019, p. 70301.

[258] Chor, Benny, et al., "Private information retrieval," *Proceedings of IEEE 36th Annual Foundations of Computer Science*. IEEE, 1995.

[259] Giovannetti, Vittorio, et al., "Quantum private queries," *Physical review letters*, vol. 100, no. 23, 2008, p. 230502.

[260] Olejnik, Lukasz. "Secure quantum private information retrieval using phase-encoded queries," *Physical Review A*, vol. 84, no. 2 2011, p. 022313.

[261] Jakobi, Markus, et al., “Practical private database queries based on a quantum-key-distribution protocol,” *Physical Review A*, vol. 83, no. 2, 2011, p. 022301.

[262] F. Gao, et al., “Flexible quantum private queries based on quantum key distribution,” *Optics express*, vol. 20, no. 16, 2012, pp. 17411-17420.

[263] W. X. Shi, et al., “Multi-bit quantum private query,” *Communications in Theoretical Physics*, vol. 64, no. 3, 2015, p. 299.

[264] Y. G. Yang, et al., “Flexible protocol for quantum private query based on B92 protocol,” *Quantum information p*rocessing, vol. 13, no. 3, 2014, pp. 805-813.

[265] Maitra, Arpita, et al., “Device-independent quantum private query,” *Physical Review A*, vol. 95, no. 4, 2017, p. 042344.

[266] Basak, Jyotirmoy, et al., “Device Independent Quantum Private Query with Finite Number of Entangled Qubits,” *arXiv preprint arXiv:*1705.04570, 2017.

[267] Y. H. Zhou, et al. “A quantum private query protocol for enhancing both user and database privacy,” *Communications in Theoretical Physics*, vol. 69, no. 1, 2018, p. 31.

[268] Roy, Sarbani, et al., “Measurement-device-independent quantum private query with qutrits,” *International Journal of Quantum Information*, vol. 16, no. 05, 2018, p. 1850045.

[269] L. Y. Zhao, et al., “Loss-tolerant measurement-device-independent quantum private queries,” *Scientific reports*, vol. 7, 2017, p. 39733.

[270] C. Y. Wei, et al., “Practical quantum private query with better performance in resisting joint-measurement attack,” *Physical Review A*, vol. 93, no. 4, 2016, p. 042318.

[271] Y. G. Yang, et al., “Quantum private query with perfect user privacy against a joint-measurement attack,” *Physics Letters A*, vol. 380, no. 48, 2016, pp. 4033-4038.

[272] De Martini, Francesco, et al., “Experimental quantum private queries with linear optics,” *Physical Review A*, vol. 80, no. 1, 2009, p. 010302.

[273] C. Wang, et al. “Implementation of quantum private queries using nuclear magnetic resonance,” *Chinese Physics Letters*, vol. 28, no. 8, 2011, p. 080302.

[274] Y. G. Yang, et al., “An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement,” *Journal of Physics A: Mathematical and Theoretical*, vol. 42, no. 5, 2009, p. 055305.

[275] J. Z. Du, et al., “Secure multiparty quantum summation,” *Acta Physica Sinica*, vol. 56, no. 11, 2007, pp. 6214-6219.

[276] N. R. Zhou, et al., “Quantum key agreement protocol,” *Electronics Letters*, vol. 40, no. 18, 2004, pp. 1149-1150.

[277] Bonanome, Marianna, et al., “Toward protocols for quantum-ensured privacy and secure voting,” *Physical Review A*, vol. 84, no. 2, 2011, p. 022331.

[278] Naseri, Mosayeb. “Secure quantum sealed-bid auction,” *Optics Communications*, vol. 282, no. 9, 2009, pp. 1939-1943.

[279] Boudot, Fabrice, Berry Schoenmakers, and Jacques Traore. “A fair and efficient solution to the socialist millionaires’ problem,” *Discrete Applied Mathematics*, vol. 111, no. 1-2, 2001, pp. 23-36.

[280] Yao, Andrew Chi-Chih. “Protocols for secure computations.” FOCS. vol. 82, 1982.

[281] Z. X. Ji, H. G. Zhang, and H. Z. Wang, “Quantum Private Comparison Protocols With a Number of Multi-Particle Entangled States,” *IEEE Access*, vol. 7 2019, pp. 44613-44621.

[282] Y. G. Yang, et al. “Comment on quantum private comparison protocols with a semi-honest third party,” *Quantum Information Processing*, vol. 12, no. 2, 2013, pp. 877-885.

[283] X. B. Chen, et al., “An efficient protocol for the private comparison of equal information based on the triplet entangled state and single-particle measurement,” *Optics communications*, vol. 283, no. 7, 2010, pp. 1561-1565.

[284] W. Liu, et al., “Quantum private comparison based on GHZ entangled states,” *International Journal of Theoretical Physics*, vol. 51, no. 11, 2012, pp. 3596-3604.

[285] W. Liu, et al., “A protocol for the quantum private comparison of equality with χ-type state,” *International Journal of Theoretical Physics*, vol. 51, no. 1, 2012, pp. 69-77.

[286] Z. W. Sun, et al., “Quantum private comparison protocol based on cluster states,” *International Journal of Theoretical Physics*, vol. 52, no. 1, 2013, pp. 212-218.

[287] W. W. Zhang, et al., “Quantum private comparison protocol with W States,” *International Journal of Theoretical Physics*, vol, 53, no. 5, 2014, pp. 1723-1729.

[288] J. Li, et al., “An efficient protocol for the private comparison of equal information based on four-particle entangled W state and Bell entangled states swapping,” *International Journal of Theoretical Physics*, vol. 53, no. 7, 2014, pp. 2167-2176.

[289] Z. X. Ji, et al., “Quantum private comparison of equal information based on highly entangled six-qubit genuine state,” *Communications in Theoretical Physics*, vol. 65, no. 6, 2016, p. 711.

[290] T. Y. Ye, et al., “Two-party quantum private comparison with five-qubit entangled states,” *International Journal of Theoretical* Physics, vol. 56, no. 5, 2017, pp. 1517-1529.

[291] Z. X. Ji, H. G. Zhang, and P. R. Fan, “Two-party quantum private comparison protocol with maximally entangled seven-qubit state,” *Modern Physics Letters A*, vol. 34, 2019, p. 1950229.

[292] Z. X. Ji, et al. "Multi-party quantum private comparison based on the entanglement swapping of d-level cat states and d-level Bell states," *Quantum Information Processing*, vol. 16, no. 7, 2017, p. 177.

[293] Q. L. Wang, et al. "Multi-party quatum private compariso protocol with n-level entangled states." *Quantum information processing*, vol. 13, no. 11, 2014, pp. 2375-2389.

[294] T. Y. Ye, and Z. X. Ji, "Multi-user quantum private comparison with scattered preparation and one-way convergent transmission of quantum states," *SCIENCE CHINA Physics, Mechanics & Astronomy*, vol. 60, no. 9, 2017, p. 090312.

[295] Y. J. Chang, et al., "Multi-user private comparison protocol using GHZ class states," *Quantum information processing*, vol. 12, no. 2, 2013, pp. 1077-1088.

[296] Q. B. Luo, et al., "Multi-party quantum private comparison protocol base on d-dimensional entangle states," *Quantum information processing*, vol. 13, no. 10, 2014, pp. 2343-2352.

[297] C. Q. Ye, et al., "Multi-party quantum private comparison of size relation with d-level single-particle states," *Quantum Information Processing*, vol. 17, no. 10, 2018, p. 252.

[298] W. J. Liu, et al., "Quantum private comparison: a review," IETE Technical Review, vol. 30, no. 5, 2013, pp. 439-445.

[299] Xiaoqing Tan, et al., "Big data quantum private comparison with the intelligent third party," *Journal of Ambient Intelligence and Humanized Computing*, vol. 6, no. 6, 2015, pp. 797-806.

[300] W. Liu, et al., "Dynamic multi-party quantum private comparison protocol with single photons in both polarization and spatial-mode degrees of freedom," *International Journal of Theoretical Physics*, vol. 55, no. 12, 2016, pp. 5307-5317.

[301] F. Wang, et al., "Quantum private comparison based on quantum dense coding," *Science China Information Sciences*, vol. 59, no. 11, 2016, p. 112501.

[302] G. P. He, et al., "Device-independent quantum private comparison protocol without a third party," *Physica Scripta*, vol. 93, no. 9, 2018, p. 095001.

[303] Y. B. Li, et al., "Information leak in Liu et al.'s quantum private comparison and a new protocol," *The European Physical Journal D*, vol. 66, no. 4, 2012, p. 110.

[304] Lin, Jason, et al., "Intercept–resend attacks on Chen et al.'s quantum private comparison protocol and the improvements," *Optics Communications*, vol. 284, no. 9, 2011, pp. 2412-2414.

[305] J. Gu, et al., "Statistics attack on 'quantum private comparison with a malicious third party' and its improvement," *Quantum Information Processing*, vol. 17, no. 2, 2018, p. 23.

[306] S. Ji, et al., "Twice-Hadamard-CNOT attack on Li et al.'s fault-tolerant quantum private comparison and the improved scheme," *Frontiers of Physics*, vol. 10, no. 2, 2015, pp. 192-197.

[307] G. P. He, "Comment on "Quantum private comparison of equality protocol without a third party"," *Quantum Information Processing*, vol.14, no. 6, 2015, pp. 2301-2305.

[308] M. K. Zhou, "Improvements of quantum private comparison protocol based on cluster states," *International Journal of Theoretical Physics*, vol. 57, no. 1, 2018, pp. 42-47.

[309] C. W. Yang, "Comment on "Efficient and feasible quantum private comparison of equality against the collective amplitude damping noise"," *Quantum information processing*, vol. 12, no. 8, 2013, pp. 2871-2875.

[310] Y. B. Li, et al., "Fault-tolerate quantum private comparison based on GHZ states and ECC," *International Journal of Theoretical Physics*, vol. 52, no. 8, 2013, pp. 2818-2825.

[311] W. W. Zhang, et al., "Cryptanalysis and improvement of the quantum private comparison protocol with semi-honest third party," *Quantum information processing*, vol. 12, no. 5, 2013, pp. 1981-1990.

[312] Y. T. Chen, et al., "Comment on the "Quantum private comparison protocol based on Bell entangled states"," International Journal of Theoretical Physics, vol. 53, no. 3, 2014, pp. 837-840.

[313] B. Zhang, et al., "Cryptanalysis and improvement of quantum private comparison of equality protocol without a third party," *Quantum Information Processing*, vol. 14, no. 12, 2015, pp. 4593-4600.

[314] W. J. Liu, et al., "Cryptanalysis and improvement of quantum private comparison protocol based on Bell entangled states," *Communications in Theoretical Physics*, vol. 62, no. 2, 2014, p. 210.

[315] Y. Chang, et al., "Cryptanalysis and improvement of the multi-user QPCE protocol with semi-honest third party," *Chinese Physics Letters*, vol. 33, no. 1, 2016, p. 010301.

[316] C. Wang, et al., "Cryptanalysis and improvements for the quantum private comparison protocol using EPR pairs," *International Journal of Quantum Information*, vol. 11, no. 04, 2013, p. 1350039.

[317] Z. W. Sun, et al., "Cryptanalysis of the efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement," *Journal of Physics A Mathematical & Theoretical*, vol. 42, no. 5, 2012, pp. 655-660.

[318] X. T. Liu, et al., "Cryptanalysis of the secure quantum private comparison protocol," *Physica Scripta*, vol. 87, no. 6, 2013, p. 065004.

[319] W. J. Liu, et al., "Improvement on "an efficient protocol for the quantum private comparison of equality with W state"," *International Journal of Quantum Information*, vol. 12, no. 01, 2014, p. 1450001.

[320] W. Q. Wu, et al., "Cryptanalysis and Improvement of Ye et al's Quantum Private Comparison Protocol." *International Journal of Theoretical Physics*, vol. 58, no. 6, 2019, pp. 1854-1860.

[321] W. Q. Wu, et al., "Cryptanalysis of Zhang et al's Quantum Private Comparison and the Improvement," International Journal of Theoretical Physics, vol. 58, no. 6, 2019, pp. 1892-1900.

[322] W. Q. Wu, et al., "Cryptanalysis of He's quantum private comparison protocol and a new protocol," *International Journal of Quantum Information*, 2019, p. 1950026.

[323] Vaccaro, Joan Alfina, et al., "Quantum protocols for anonymous voting and surveying," *Physical Review A*, vol. 75, no. 1, 2007, p. 012333.

[324] Hillery, Mark, et al., "Towards quantum-based privacy and voting," *Physics Letters A*, vol. 349, no. 1-4, 2006, pp. 75-81.

[325] Q. L. Wang, et al., "Self-tallying quantum anonymous voting," *Physical Review A*, vol. 94, no. 2, 2016, p. 022333.

[326] L. Jiang, et al., "Quantum anonymous voting for continuous variables," *Physical Review A*, vol. 85, no. 4, 2012, 042309.

[327] P. Xue, et al., "A simple quantum voting scheme with multi-qubit entanglement," *Scientific reports*, vol. 7, no. 1, 2017, p. 7586.

[328] Y. Guo, "Quantum anonymous voting with unweighted continuous-variable graph states," *Quantum Information Processing*, vol. 15, no. 8, 2016, pp. 3327-3345.

[329] J. L. Zhang, et al., "An elaborate secure quantum voting scheme," *International Journal of Theoretical Physics*, vol. 56, no. 10, 2017, pp. 3019-3028.

[330] Thapliyal, Kishore, et al., "Protocols for quantum binary voting," *International Journal of Quantum Information*, vol. 15, no. 01, 2017, p. 1750007.

[331] Z. Yi, et al., "Quantum voting protocol using two-mode squeezed states," *Acta Physica Sinica*, vol. 58, no. 5, 2009, pp. 3166-3172.

[332] Yuan Li, et al., "Quantum anonymous voting systems based on entangled state," *Optical review*, vol. 15, no. 5, 2008, pp. 219-223.

[333] J. H. Tian, et al., "A voting protocol based on the controlled quantum operation teleportation," *International Journal of Theoretical Physics*, vol. 55, no. 5, 2016, pp. 2303-2310.

[334] Q. J. Xu, et al., "Improvement of the security of quantum protocols for anonymous voting and surveying," *Science China Physics, Mechanics and Astronomy*, vol. 53, no. 11, 2010, pp. 2131-2134.

[335] R. H. Shi, et al., "Anonymous voting for multi-dimensional CV quantum system," *Chinese Physics B*, vol. 25, no. 6, 2016, p. 060301.

[336] X. B. Chen, et al., "An efficient protocol for the secure multi-party quantum summation," *International Journal of Theoretical Physics*, vol. 49, no. 11, 2010, pp. 2793-2804.

[337] W. Liu, et al., "An novel protocol for the quantum secure multi-party summation based on two-particle bell states," *International Journal of Theoretical Physics*, vol. 56, no. 9, 2017, pp. 2783-2791.

[338] C. Zhang, et al., "High-capacity quantum summation with single photons in both polarization and spatial-mode degrees of freedom," *International Journal of Theoretical Physics*, vol. 53, no. 3, 2014, pp. 933-941.

[339] C. Zhang, et al., "Multi-party quantum summation without a trusted third party based on single particles," *International Journal of Quantum Information*, vol. 15, no. 02, 2017, p. 1750010.

[340] R. H. Shi, et al., "Secure multiparty quantum computation for summation and multiplication," *Scientific reports*, vol. 6, 2016, p. 19655.

[341] C. Zhang, et al., "Three-party quantum summation without a trusted third party," *International Journal of Quantum Information*, vol. 13, no. 02, 2015, p. 1550011.

[342] Z. X. Ji, H. G. Zhang, et al., "Quantum protocols for secure multi-party summation," *Quantum Information Processing*, vol. 18, no. 6, 2019, p. 168.

[343] Y. G. Yang, et al., "Improved secure quantum sealed-bid auction," *Optics Communications*, vol. 282, no. 20, 2009, pp. 4167-4170.

[344] Z. W. Zhao, "Secure quantum sealed-bid auction with post-confirmation," *Optics Communications*, vol. 283, no. 16, 2010, pp. 3194-3197.

[345] J. T. Wang, et al., "A new quantum sealed-bid auction protocol with secret order in post-confirmation," *Quantum Information Processing*, vol. 14, no. 10, 2015, pp. 3899-3911.

[346] W. J. Liu, et al., "Multiparty quantum sealed-bid auction using single photons as message carrier," *Quantum Information Processing*, vol. 15, no. 2, 2016, pp. 869-879.

[347] R. Zhang, et al., "An economic and feasible Quantum Sealed-bid Auction protocol," *Quantum Information Processing*, vol. 17, no. 2, 2018, p. 35.

[348] Z. Y. Wang. "Quantum secure direct communication and quantum sealed-bid auction with EPR pairs," *Communications in Theoretical Physics*, vol. 54, no. 6, 2010, p. 997.

[349] G. Liu, et al., "Multiparty Sealed-Bid Auction Protocol Based on the Correlation of Four-Particle Entangled State," *International Journal of Theoretical Physics*, vol. 57, no. 10, 2018, pp. 3141-3148.

[350] W. J. Liu, et al., "Attacks and improvement of quantum sealed-bid auction with EPR pairs," *Communications in Theoretical Physics*, vol. 61, no. 6, 2014, p. 686.

[351] S. J. Qin, et al., "Cryptanalysis and improvement of a secure quantum sealed-bid auction," *Optics Communications*, vol. 282, no. 19, 2009, pp. 4014-4016.

[352] G. A. Xu, et al., "Cryptanalysis and improvement of the secure quantum sealed-bid auction with postconfirmation," *International Journal of Quantum Information*, vol. 9, no. 06, 2011, pp. 1383-1392.

[353] L. B. He, et al., "Cryptanalysis and melioration of secure quantum sealed-bid auction with post-confirmation," *Quantum Information Processing*, vol. 11, no. 6, 2012, pp. 1359-1369.

[354] Y. Luo, et al., "The loophole of the improved secure quantum sealed-bid auction with post-confirmation and solution," *Quantum information processing*, vol. 12, no. 1, 2013, pp. 295-302.

[355] Rivest, Ronald L., Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, 1978, pp. 120-126.

[356] Peter W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," *Proceedings 35th annual symposium on foundations of computer science*. Ieee, 1994.

[357] Lov K. Grover, "A fast quantum mechanical algorithm for database search," *arXiv preprint quant-ph/9605043* 1996.

[358] F. Gao, et al., "Quantum asymmetric cryptography with symmetric keys," *Science in China Series G: Physics, Mechanics and Astronomy*, vol. 52, no. 12, 2009, pp. 1925-1931.

[359] Abhishek. Parakh, "New protocol for quantum public key cryptography," *2015 IEEE International Conference on Advanced Networks and Telecommuncations Systems (ANTS)*. IEEE, 2015.

[360] X. Y. Li, et al., "Quantum Public-key Cryptosystem without Quantum Channels between Any Two Users using Non-orthogonal States," *International Journal of Security and Its Applications*, vol. 9, no. 9, 2015, pp. 253-264.

[361] Vlachou, Chrysoula, et al., "Quantum walk public-key cryptographic system," *International Journal of Quantum Information*, vol. 13, no. 07, 2015, p. 1550050.

[362] Aharonov, Yakir, et al., "Quantum random walks," *Physical Review A*, vol. 48, no. 2, 1993, p. 1687.

[363] W. Q. Wu, et al., "A public key cryptosystem based on data complexity under quantum environment," *Science China Information Sciences*, vol. 58, no. 11, 2015, pp. 1-11.

[364] W. Q. Wu, et al., "Quantum public key cryptosystem based on bell states," *International Journal of Theoretical Physics*, vol. 56, no. 11, 2017, pp. 3431-3440.

[365] S. K. Chong, and Tzonelih Hwang. "Quantum key agreement protocol based on BB84." *Optics Communications*, vol. 283, no. 6, 2010, pp. 1192-1195.

[366] Y. F. He, et al., "Two quantum key agreement protocols immune to collective noise," *International Journal of Theoretical Physics*, vol. 56, no. 2, 2017, pp. 328-338.

[367] Y. F. He, et al., "Two-party quantum key agreement against collective noise," *Quantum Information Processing*, vol. 15, no. 12, 2016, pp. 5023-5035.

[368] Y. F. He, et al., "Quantum key agreement protocols with four-qubit cluster states," *Quantum Information Processing*, vol. 14, no. 9, 2015, pp. 3483-3498.

[369] H. Gao, et al., "Two-party quantum key agreement protocols under collective noise channel," *Quantum Information Processing*, vol. 17, no. 6, 2018, p. 140.

[370] D. S. Shen, "Two-party quantum key agreement with four-qubit cluster states," *Quantum information processing*, vol. 13, no. 10, 2014, pp. 2313-2324.

[371] W. Huang, et al., "Quantum key agreement with EPR pairs and single-particle measurements," *Quantum information processing*, vol. 13, no. 3, 2014, pp. 649-663.

[372] Shukla, Chitra, et al., "Protocols of quantum key agreement solely using Bell states and Bell measurement," *Quantum information processing*, vol. 13, no. 11, 2014, pp. 2391-2405.

[373] J. H. He. et al., "High-dimensional quantum key agreement protocol with pairs of single qudits," *International Journal of Quantum Information*, vol. 16, no. 03, 2018, p. 1850024.

[374] S. M. Zhao, et al., "Multidimensional reconciliation protocol for continuous-variable quantum key agreement with polar coding." *SCIENCE CHINA Physics, Mechanics & Astronomy*, vol. 61, no. 9, 2018, p. 090323.

[375] Z. W. Sun, et al., "Efficient multi-party quantum key agreement by cluster states," *Quantum Information Processing*, vol. 15, no. 1, 2016, pp. 373-384.

[376] H. Cao. et al., "Efficient multi-party quantum key agreement protocol based on nonorthogonal quantum entangled pairs." *Laser Physics Letters*, vol. 15, no. 9, 2018, p. 095201.

[377] Y. H. Chou, et al., "Dynamic group multi-party quantum key agreement," *Scientific reports*, vol. 8, no. 1, 2018, p. 4633.

[378] H. Cao. et al., "Multiparty quantum key agreement based on quantum search algorithm," *Scientific reports*, vol. 7, 2017, p. 45046.

[379] Z. W. Sun, et al., "Multi-party quantum key agreement by an entangled six-qubit state," *International Journal of Theoretical Physics*, vol. 55, no. 3, 2016, pp. 1920-1929.

[380] P. Wang, et al., "Multi-party quantum key agreement protocol secure against collusion attacks," *Quantum Information Processing*, vol. 16, no. 7, 2017, p. 170.

[381] R. H. Shi, et al., "Multi-party quantum key agreement with bell states and bell measurements," *Quantum information processing*, vol.

12, no. 2, 2013, pp. 921-932.

[382] B. Liu, et al., “Multiparty quantum key agreement with single particles,” *Quantum information processing*, vol. 12, no. 4, 2013, p. 1797-1805.

[383] B. B. Cai, et al., “Multi-party quantum key agreement without entanglement,” *International Journal of Theoretical Physics*, vol. 56, no. 4, 2017, pp. 1039-1051.

[384] B. B. Cai, et al., “Multi-party quantum key agreement with teleportation,” *Modern Physics Letters B*, vol. 31, no. 10, 2017, p. 1750102.

[385] G. B. Xu, et al., “Novel multiparty quantum key agreement protocol with GHZ states,” *Quantum information processing*, vol. 13, no. 12, 2014, pp. 2587-2594.

[386] S. Q. Min, et al., “Novel multi-party quantum key agreement protocol with g-like states and bell states,” *International Journal of Theoretical Physics*, vol. 57, no. 6, 2018, pp. 1811-1822.

[387] N. R. Zhou, et al., “Three-Party Quantum Key Agreement Protocol with Seven-Qubit Entangled States,” *International Journal of Theoretical Physics*, vol. 57, no. 11, 2018, pp. 3505-3513.

[388] X. R. Yin, et al., “Three-party quantum key agreement with two-photon entanglement,” *International Journal of Theoretical Physics*, vol. 52, no. 11, 2013, pp. 3915-3921.

[389] S. K. Chong, et al., “Improvement on “quantum key agreement protocol with maximally entangled states”,” *International Journal of Theoretical Physics*, vol. 50, no. 6, 2011, pp. 1793-1802.

[390] Z. W. Sun, et al., “Improvements on “multiparty quantum key agreement with single particles”,” *Quantum information processing*, vol. 12, no. 11, 2013, pp. 3411-3420.

[391] Z. C. Zhu, et al., “Improving the security of protocols of quantum key agreement solely using Bell states and Bell measurement,” *Quantum Information Processing*, vol. 14, no. 11, 2015, pp. 4245-4254.

[392] Z. C. Zhu, et al., “Participant attack on three-party quantum key agreement with two-photon entanglement,” *International Journal of Theoretical Physics*, vol. 55, no. 1, 2016, pp. 55-61.

[393] B. Liu, et al., “Collusive attacks to “circle-type” multi-party quantum key agreement protocols,” *Quantum Information Processing*, vol. 15 no. 5, 2016, pp. 2113-2124.

[394] W. Huang, et al., “Cryptanalysis of a multi-party quantum key agreement protocol with single particles,” *Quantum information processing*, vol. 13, no. 7, 2014, pp. 1651-1657.

[395] Ba An. Nguyen, “Quantum dialogue.” *Physics Letters A*, vol. 328, no. 1, 2004, pp. 6-10.

[396] Z. X. Man, et al., “Quantum dialogue revisited,” *Chinese Physics Letters*, vol. 22, no. 1, 2005, p. 22.

[397] Mosayeb. Naseri, “An efficient protocol for quantum secure dialogue with authentication by using single photons,” *International Journal of Quantum Information*, vol. 9, no. 07, 2011, pp. 1677-1684.

[398] T. Y. Ye, “Quantum dialogue without information leakage using a single quantum entangled state,” International Journal of Theoretical Physics, vol. 53, no. 11, 2014, pp. 3719-3727.

[399] Y. P. Luo, et al., “Efficient quantum dialogue using single photons,” *Quantum information processing*, vol. 13, no. 11, 2014, pp. 2451-2461.

[400] G. F. Shi, et al., “Quantum secure dialogue based on single photons and controlled-not operations,” *Journal of Modern Optics*, vol. 57, no. 20, 2010, pp. 2027-2030.

[401] G. F. Shi, et al., “Quantum secure dialogue by using single photons,” *Optics Communications*, vol. 283, no. 9, 2010, p. 1984-1986.

[402] Y. G. Yang, et al., “Quasi-secure quantum dialogue using single photons,” *Science in China Series G: Physics, Mechanics and Astronomy*, vol. 50, no. 5, 2007, pp. 558-562.

[403] X. Ji, et al., “Secure quantum dialogue based on single-photon,” Chinese Physics, vol. 15, no. 7, 2006, p. 1418.

[404] N. R. Zhou, et al., “Single-photon secure quantum dialogue protocol without information leakage,” *International Journal of Theoretical Physics*, vol, 53, no. 11, 2014, pp. 3829-3837.

[405] D. S. Shen, et al., “Quantum dialogue with authentication based on Bell states,” *International Journal of Theoretical Physics* vol. 52, no. 6, 2013, pp. 1825-1835.

[406] T. Y. Ye, et al., “Quantum dialogue without information leakage based on the entanglement swapping between any two Bell states and the shared secret Bell state,” *Physica Scripta*, vol. 89, no. 1, 2013, p. 015103.

[407] C. Zheng, et al., “Quantum secure direct dialogue using Einstein-Podolsky-Rosen pairs,” *Science China Physics, Mechanics & Astronomy*, vol. 57, no. 7, 2014, pp. 1238-1243.

[408] C. Y. Lin, et al., “Authenticated quantum dialogue based on Bell states,” *International Journal of Theoretical Physics*, vol. 54, no. 3, 2015, pp. 780-786.

[409] Y. Xia, et al., “Controlled secure quantum dialogue using a pure entangled GHZ states,” *Communications in Theoretical Physics*, vol. 48, no. 5, 2007, p. 841.

[410] Y. Xia, et al., “Quantum dialogue by using the GHZ state,” *arXiv preprint quant-ph/0601127* (2006).

[411] C. H. Chang, et al., “Quantum dialogue protocols over collective noise using entanglement of GHZ state,” *Quantum Information Processing*, vol. 15, no. 7, 2016, pp. 2971-2991.

[412] A. H. Yin, et al., “Efficient quantum dialogue without information leakage,” *Modern Physics Letters B*, vol. 29, no. 05, 2015, p. 1550018.

[413] N. R. Zhou, et al., “Secure quantum dialogue

protocol based on W states without information leakage," *International Journal of Theoretical Physics*, vol. 52, no. 9, 2013, pp. 3204-3211.

[414] W. Li, et al., "Secure quantum dialogue protocol based on four-qubit cluster state," *International Journal of Theoretical Physics*, vol. 57, no. 2, 2018, pp. 371-380.

[415] R. J. Wang, et al., "Two ways of robust quantum dialogue by using four-qubit cluster state," *International Journal of Theoretical Physics*, vol. 55, no. 4, 2016, pp. 2110-2124.

[416] F. Gao, et al., "Revisiting the security of quantum dialogue and bidirectional quantum secure direct communication," *Science in China Series G: Physics, Mechanics and Astronomy*, vol. 51, no. 5, 2008, pp. 559-566.

[417] H. Liu, et al., "Eavesdropping on the quantum dialogue protocol in lossy channel," *Chinese Physics B*, vol. 20, no. 7, 2011, p. 070305.

[418] T. H. Lin, et al., "Man-in-the-middle attack on "quantum dialogue with authentication based on Bell states"," *International Journal of Theoretical Physics*, vol. 52, no. 9, 2013, pp. 3199-3203.

[419] T. Y. Ye, "Information leakage resistant quantum dialogue against collective noise," *SCIENCE CHINA Physics, Mechanics & Astronomy*, vol. 57, no. 12, 2014, pp. 2266-2275.

[420] Z. H. Liu, et al., "Cryptanalysis and improvement of efficient quantum dialogue using entangled states and entanglement swapping without information leakage," *Quantum Information Processing*, vol. 16, no. 9, 2017, p. 229.

[421] G. Gao, et al. "Information leakage in quantum dialogue by using non-symmetric quantum channel," *Communications in Theoretical Physics*, vol. 67, no. 5, 2017, p. 507.

[422] D. S. Shen, et al. "Quantum dialogue with authentication based on Bell states," *International Journal of Theoretical Physics*, vol. 52, no. 6, 2013, pp. 1825-1835.

[423] C. Y. Lin. "Authenticated quantum dialogue based on Bell states," *International Journal of Theoretical Physics*, vol. 54, no. 3, 2015, pp. 780-786.

[424] Hwang, Tzonelih, and Y. P. Luo. "Probabilistic authenticated quantum dialogue," *Quantum Information Processing*, vol. 14, no. 12, 2015, pp. 4631-4650.

[425] J. M. Qi, et al., "Two authenticated quantum dialogue protocols based on three-particle entangled states," *Quantum Information Processing*, vol. 17, no. 9, 2018, p. 247.

[426] T. Y. Ye, "Fault tolerant channel-encrypting quantum dialogue against collective noise," *SCIENCE CHINA Physics, Mechanics & Astronomy*, vol. 58, no. 4, 2015, pp. 1-10.

[427] M. H. Zhang, et al., "Fault-tolerant asymmetric quantum dialogue protocols against collective noise," *Quantum Information Processing*, vol. 17, no. 8, 2018, p. 204.

[428] X. Min, et al., "Fault-tolerant controlled quantum dialogue using logical qubit," *Chinese Journal of Electronics*, vol. 27, no. 2, 2018, pp. 263-269.

[429] T. Y. Ye, "Fault-tolerant authenticated quantum dialogue using logical Bell states," *Quantum Information Processing*, vol. 14, no. 9, 2015, pp. 3499-3514.

[430] Crépeau, Claude, et al., "Quantum oblivious mutual identification," *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, Berlin, Heidelberg, 1995.

[431] Dušek, Miloslav, et al., "Quantum identification system," *Physical Review A*, vol. 60, no. 1, 1999, p. 149.

[432] D. Richard. Kuhn, "A hybrid authentication protocol using quantum entanglement and symmetric cryptography," *arXiv preprint quant-ph/0301150* (2003).

[433] Bartkiewicz, Karol, et al., "Using quantum routers to implement quantum message authentication and Bell-state manipulation," *Physical Review A*, vol. 90, no. 2, 2014, p. 022335.

[434] M. S. Kang, et al., "Quantum message authentication scheme based on remote state preparation," *Physica Scripta*, vol. 93, no. 11, 2018, p. 115102.

[435] Mihara, Takashi. "Quantum identification schemes with entanglements," *Physical review A*, vol. 65, no. 5, 2002, p. 052326.

[436] X. L. Zhang, "One-way quantum identity authentication based on public key," *Chinese Science Bulletin*, vol. 54, no. 12, 2009, pp. 2018-2021.

[437] J. Wang, et al., "Multiparty simultaneous quantum identity authentication based on entanglement swapping," *Chinese Physics Letters*, vol. 23, no. 9, 2006, p. 2360.

[438] Y. G. Yang, et al., "Multiparty simultaneous quantum identity authentication with secret sharing." *Science in China Series G: Physics, Mechanics and Astronomy*, vol. 51, no. 3, 2008, pp. 321-327.

[439] W. M. Shi, et al., "Quantum deniable authentication protocol," *Quantum information processing*, vol. 13, no. 7, 2014, pp. 1501-1510.

[440] W. M. Shi, et al., "A novel quantum deniable authentication protocol without entanglement," *Quantum Information Processing*, vol. 14, no. 6, 2015, pp. 2183-2193.

[441] Z. S. Zhang, et al., "Quantum identity authentication based on ping-pong technique for photons," *Physics Letters A*, vol. 356, no. 3, 2006, pp. 199-205.

[442] H. Yuan, et al., "Quantum identity authentication based on ping-pong technique without entanglements," *Quantum information processing*, vol. 13, no. 11, 2014, pp. 2535-2549.

[443] Farouk, Ahmed, et al., "Robust general N user authentication scheme in a centralized quan-

tum communication network via generalized GHZ states," *Frontiers of Physics*, vol. 13, no. 2, 2018, p. 130306.

[444] P. H. Niu, et al., "Quantum authentication scheme based on entanglement swapping," *International Journal of Theoretical Physics,* vol. 55, no. 1, 2016, pp. 302-312.

[445] N. R. Zhou, et al., "Cross-center quantum identification scheme based on teleportation and entanglement swapping," *Optics communications*, vol. 254, no. 4-6, 2005, pp. 380-388.

[446] Monz, Thomas, et al., "14-qubit entanglement: Creation and coherence," *Physical Review Letters*, vol. 106, no. 13, 2011, p. 130506.

[447] X. L. Wang, et al., "18-qubit entanglement with six photons' three degrees of freedom," *Physical review letters*, vol. 120, no. 26, 2018, p. 260502.

[448] W. B. Gao, et al., "Experimental demonstration of a hyper-entangled ten-qubit Schrödinger cat state," *Nature physics*, vol. 6, no. 5, 2010, p. 331.

[449] G. L. Long, et al., "Theoretically efficient high-capacity quantum-key-distribution scheme." *Physical Review A*, vol. 65, no. 3, 2002, p. 032302.

## Biographies

***Huanguo Zhang,*** was born in 1945. He is currently a Professor and Ph.D. Supervisor with Wuhan University. His research interests include information security, quantum cryptography, trusted computing, cloud computing, fault tolerance. Email: liss@whu.edu.cn

***Zhaoxu Ji,*** is currently pursuing the Ph.D. degree from the School of Cyber Science and Engineering, Wuhan University, China. His research interests include quantum computation and quantum cryptography. Email: jizhaoxu@whu.edu.cn

***Houzhen Wang,*** is an associate professor with the School of Cyber Science and Engineering Wuhan University. His research interests include information security, cryptography, and quantum information. Email: whz@whu.edu.cn

***Wanqing Wu,*** is an associate professor with the School of Cyber Science and Engineering Wuhan University. His research interests include information security, cryptography, and quantum information. Email: wuwanqing8888@126.com