DOI 10.15302/J-SSCAE-2022.04.015

Current Status and Future Development of Quantum Cryptographic Protocols

Zhang Xue, Gao Fei, Qin Sujuan, Zhang Ping

State Key Laboratory of Networking and Switching Technology (Beijing University of Posts and Telecommunications), Beijing 100876, China

Abstract: Quantum computing has parallel computing capability and is superior to classical computing for solving specific problems. Once a large-scale quantum computer is developed, the security of classical cryptographic algorithms and protocols, based on the assumption of computational complexity, will be significantly challenged. Quantum cryptography is a new cryptosystem based on the principles of quantum mechanics that can resist quantum computing attacks. This paper focuses on almost 40 years of development of quantum cryptographic protocols, including quantum key distribution, secure direct communication, secret sharing, identity authentication, private query, and two-party secure computation. Additionally, challenges for the development process are summarized. The analysis shows that quantum cryptographic protocols are in an unbalanced state: QKD is significantly ahead of other protocols, which have difficulty achieving breakthroughs. In the future, practical quantum protocols for digital signatures and two-party secure computation are core issues that must be urgently addressed. Therefore, research on quantum and post-quantum cryptography should be conducted synchronously, crossover study and talent cultivation for quantum science and cryptography disciplines should be strengthened, and the examination and evaluation mechanism of relevant basic research must be optimized.

Keywords: quantum cryptography; protocols; quantum key distribution; quantum digital signature; quantum private query

1 Introduction

Since ancient times, information exchange has become an indispensable part of daily life. Information transmission security is a basic requirement in many communication scenarios, especially diplomacy, military, and economy. Cryptography is the theoretical basis for ensuring network and information security, among which various cryptographic algorithms and protocols play an important role in ensuring confidentiality, integrity, non-repudiation, and identity authentication. Classical cryptography (i.e., mathematical cryptography based on mathematical complexity theory) can be divided into symmetric and public-key cryptography, each of which has advantages and is widely used. However, in the 1990s, the Shor and Grover algorithms were proposed, which became a critical security threat to the classical cryptosystem. Essentially, if a universal quantum computer was developed, the Shor algorithm could easily break a variety of public-key cryptography algorithms based on integer factorization and discrete logarithm problems. The Grover algorithm also challenges the security of symmetric cryptography. Therefore, building a new cryptosystem capable of resisting quantum computing attacks has become a key task.

Quantum technology offers a potential approach to address these quantum computing attacks (i.e., quantum cryptography). Quantum cryptography is the product of the fusion of quantum mechanics and cryptography, and

Received date: May 11, 2022; **revised date:** June 20, 2022

Corresponding author: Gao Fei, professor at the School of Cyberspace Security, Beijing University of Posts and Telecommunications. Major research fields include quantum cryptography and quantum algorithms. E-mail: gaof@bupt.edu.cn

Funding program: CAE Advisory Project “Research on the Development Strategy for the Engineering Application of Quantum Information Technology” (2021-HYZD-01); National Natural Science Foundation of China (61972048, 61976024)

Chinese version: Strategic Study of CAE 2022, 24 (4): 145–155

Cited item: Zhang Xue et al. Current Status and Future Development of Quantum Cryptographic Protocols. *Strategic Study of CAE*, https://doi.org/10.15302/J-SSCAE-2022.04.015

uses quantum states as information carriers to transmit information between users. According to the properties of quantum states, all effective eavesdropping/attack behaviors can be discovered by communicating with parties in a secure quantum cryptographic protocol. It can be observed that the security of quantum cryptography is guaranteed by the basic principles of quantum mechanics rather than that by the mathematical complexity problem. A well-designed quantum cryptographic protocol can achieve information-theoretical security. In recent years, various unique quantum cryptographic protocols were proposed with the gradual enrichment and maturity of quantum information technology. It should be noted that classical cryptography typically builds various protocols based on cryptographic algorithms, whereas quantum cryptography frequently directly uses quantum properties to design similar protocols. Therefore, compared with algorithms, protocols are the main research topic in quantum cryptography.

The research significance of quantum cryptographic protocols can be explained using the wooden bucket theory (Fig. 1). In classical cryptography, the wooden stave sides represent all types of cryptographic algorithms and protocols. In quantum cryptography, the wooden stave sides represent various protocols. It can be observed that protocols are crucial to quantum cryptography and that all cryptographic tasks are accomplished through relevant protocols. Moreover, compared with classical cryptographic algorithms and protocols, the security of quantum cryptographic protocols is significantly improved, which can resist quantum computing attacks. Researchers aim to use quantum properties to realize various cryptographic protocol functions to improve information systems security.

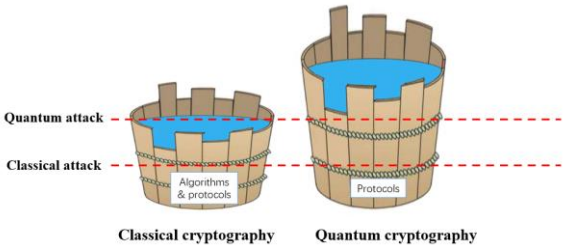

Fig. 1. Quantum cryptographic protocol research significance.
Note: Barrel capacity represents information system security strength.

In this study, the development trends of quantum cryptographic protocols are investigated. Based on different protocol functions, we organize the development status of six mainstream quantum cryptographic protocols (Fig. 2) and subsequently analyze their practical potential and limitations. Considering the overall practical application requirements of quantum cryptography, we highlight key future scientific problems that must be solved and predict potential technical approaches. To provide a fundamental reference for in-depth research on quantum cryptographic protocols, suggestions for technical development are also proposed.

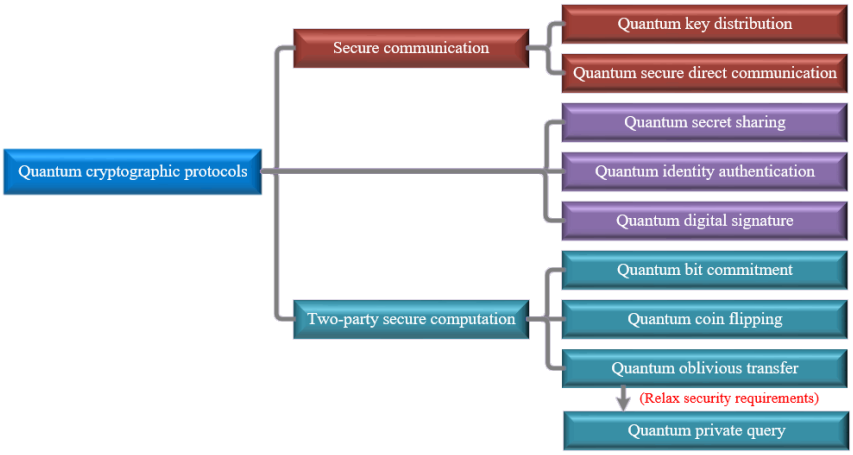

Fig. 2. Representative quantum cryptographic protocols.

2 Quantum key distribution protocol

Quantum key distribution (QKD) is a protocol in which two communicating parties establish a symmetric key by transmitting quantum states where the key string is known only to these two parties. This string (consisting of

DOI 10.15302/J-SSCAE-2022.04.015

classical random bits) is also called the "quantum key", as it is established in a quantum manner. Because both QKD and the one-time pad (OTP) have information-theoretic security, perfect secure communication can be achieved using this combination.

According to different dimensions of the light source coding space, QKD can be divided into discrete variable QKD and continuous variable QKD. A QKD system consists of a transmitter, a receiver, and the channels that connect each. QKD channels include quantum and classical channels, used to transmit quantum and classical messages, respectively. In quantum cryptographic protocols, classical communication is generally assumed to be tamper-proof and can be achieved using classical message authentication code (MAC) with information-theoretic security. To obtain information-theoretic security in a noisy reality, the QKD protocol generally includes error correction and privacy amplification processes. The former is used to correct the key error caused by noise, and the latter to compress key information obtained by the eavesdropper under the cover of noise.

In 1984, Bennett and Brassard first proposed the concept of quantum cryptography and provided the first QKD protocol, the BB84 protocol [1]. After almost 40 years of development, various QKD protocols have been proposed based on different quantum mechanical properties, and the security of typical QKD protocols was strictly proven. However, some security loopholes in actual QKD systems remain owing to imperfect devices. A device-independent (DI) QKD protocol can fundamentally eliminate these vulnerabilities [2,3]. Such protocols do not require perfect QKD devices and the devices may even be untrustworthy. By observing the correlation between input and output classical bit information and calculating the violation value of the Bell inequality, communication parties can judge device reliability and estimate the maximum information the eavesdropper can obtain. As long as the violation value observed in the experiment is sufficiently large, this indicates that the device is sufficiently credible, and communication parties can obtain the key to information-theoretic security. The DI-QKD protocol process is equivalent to a "self-test" of its device's credibility. Only the trusted device can pass the test, and communicating parties can successfully establish the key. Since then, a measurement-device-independent QKD protocol was proposed, which achieves secure key distribution in the case of untrusted measurement devices [4,5], and the implementation difficulty is lower than that of DI-QKD.

Practical research on QKD is also rapidly developing. Pan et al. demonstrated an integrated air-to-ground quantum communication network in 2021. Based on the "Micius" quantum satellite, any user in this QKD network can communicate with another through an integrated optical fiber and free-space QKD link with a total distance of 4600 km [6]. In the same year, Feng et al. demonstrated a QKD experiment based on polarization coding for a 10-m underwater channel, where the security key generation rate exceeded 700 kbps [7]. In 2022, Guo et al. achieved an 833 km optical fiber QKD, which increased the world record of relating-free QKD secure transmission distance by over 200 km. This is an important step toward realizing 1000 km of land-based quantum secure communication [8].

In summary, QKD is the earliest and most theoretically mature component of quantum cryptography. Many countries established communication networks based on QKD, such as the defense advanced research projects agency (DARPA) in the United States, the Europe project Secure Communication Based on Quantum Cryptography (i.e., SECOQC), the Tokyo QKD Network in Japan, and the Beijing–Shanghai Trunk Line in China. With the launch of the "Micius" quantum satellite and the completion of the Beijing–Shanghai and Shanghai–Hangzhou trunk lines, QKD has been equipped with the conditions for practical application to a certain extent. However, limited by technical conditions, the current QKD system cannot meet the requirements of large-scale applications in terms of transmission rate and distance. In specific applications, compromise is frequently necessary. For example, the QKD key is regularly used in advanced encryption standards and other encryption algorithms to solve the low key generation rate problem; however, this type of communication will no longer possess information-theoretic security. To solve the transmission distance problem, the QKD network frequently requires "trusted relays" (Fig. 3), which assume that the relay is credible (if the relay node is not credible, it will be relatively straightforward to obtain the distribution of the key, and subsequently obtain the encrypted message with the transferred key). This will damage QKD and limit its large-scale application to a certain extent.

In the trusted relay model, the relay node performs QKD with both communication parties, encrypts Alice's key using Bob's key, and transmits it to Bob; thus, Alice and Bob can establish the key at a distance. In addition to this type of trusted relay, "quantum relay" is also being studied [9], which can improve the distance of entangled state distribution through quantum storage, entanglement switching, and other technologies. Quantum relay does not compromise QKD security and has better application potential. However, the related technology is not sufficiently mature and cannot currently reach the degree of practical application.

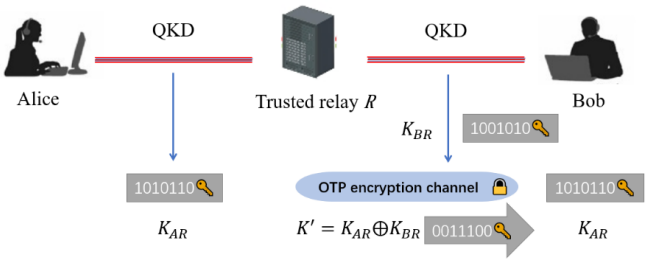

Fig. 3. QKD trusted relay model.

3 Quantum secure direct communication protocol

Quantum secure direct communication (QSDC) is another important quantum communication protocol that transmits private information directly between communicating parties without producing secret keys in advance. Unlike transmitting random keys, to ensure the integrity of messages, using quantum states to transmit secret messages directly will not be conducive to eavesdropping detection, error correction, and privacy amplification. The QSDC protocol solves this problem using block transmission, quantum privacy amplification, and other technologies.

In 2000, Long and Liu first proposed a quantum secure communication model for transmitting secret information using entangled state block transmission technology [10]. In 2004, Deng et al. combined non-orthogonal quantum state block transmission and classical OTP, and proposed a QSDC protocol based on single photons [11]. Compared to the protocol based on entanglement, the operation of the single-photon state is easier to achieve. Subsequently, the QSDC communication mode has become a research hotspot for international quantum secure communication [12].

In recent years, significant progress has been made in QSDC implementation. In 2016, Hu et al. demonstrated a QSDC protocol based on single photons [13]. In 2021, Qi et al. used the QSDC principle to achieve secure communication among 15 users in a network with a transmission distance of 40 km [14].

Based on the current research status, QSDC has been close to the degree of practical technology required. Functionally, QSDC is the same as QKD and OTP, both of which belong to the secure communication category.

4 Quantum secret sharing protocol

Secret sharing is a procedure that involves splitting a message into several parts in an appropriate manner. Subsequently, each share is managed by different participants such that secret information cannot be recovered by a single participant, rather, cooperation by several participants is required to recover this information. The fundamental idea of secret sharing is to prevent the concentration of secrets to diversify the risk. The most common secret-sharing protocol is the (k, n) threshold protocol, that is, the distributor encrypts the secret message into n copies and sends them to n receivers. It requires the cooperation of any k participants to reconstruct the message, whereas any combination of fewer than k participants cannot obtain information regarding the message. In classical cryptography, common secret-sharing protocols include the Shamir threshold scheme based on the polynomial Lagrange interpolation formula and the threshold scheme based on the Chinese remainder theorem. With the development of quantum cryptography, quantum secret sharing (QSS) protocols have been extensively studied.

In 1999, Hillery et al. proposed the first QSS protocol by taking advantage of the entanglement properties of GHZ states [15]. Subsequent scholars proposed a variety of QSS protocols using different quantum properties [16]. In terms of experimental progress, in 2014, Bell et al. realized the secret sharing of classical and quantum information based on graph states using photons in linear optical devices [17]. In 2018, Zhou et al. implemented a QSS protocol using the multipartite bound entanglement of an optical field, which realized secret sharing among four participants [18]. In 2021, Liao et al. proposed a CV-QSS protocol based on discrete modulated coherent states and a maximum transmission distance greater than 100 km [19].

Theoretically, QSS has broad research prospects, such as the (k, n) threshold scheme, multi-party to multi-party secret sharing, and rational secret sharing protocols. However, low practical application value remains for the QSS protocol. First, most research on this protocol focuses on the (n, n) threshold protocol. It is difficult to achieve (k, n) threshold secret sharing; therefore, QSS application scenarios are limited. Second, error correction and privacy amplification methods are lacking in the QSS protocol, making it difficult to realize information-theoretic security.

DOI 10.15302/J-SSCAE-2022.04.015

In fact, the combination of the QKD protocol and the classical threshold scheme can realize secret sharing of information-theoretic security. Therefore, the QSS can be regarded as a direct application of QKD.

5 Quantum identity authentication protocol

Quantum identity authentication (QIA) refers to the authentication of the participant's identity in a quantum cryptographic protocol to prevent attackers from impersonating an authentic identity to steal information. A series of QIA protocols have been proposed to achieve information-theoretic security authentication in QKD. These protocols can be approximately divided into two types: type 1 shares the classical key, and type 2 shares entanglement.

In the shared classical key QIA protocol, communication parties share a predetermined string in advance to show their identities. In 1999, Dušek et al. first proposed the use of a classical message authentication protocol to authenticate classical information transmitted in QKD [20]. Subsequently, other protocols use the classical key to represent the position and measurement basis of eavesdropping detection particles, which can also achieve the function to authenticate the identities of both parties.

In the shared entanglement QIA protocol, communication parties share a set of entangled particles, of which each party has one of each pair. Corresponding operations on entangled particles were performed to identify each other. This method is difficult to implement because it requires the storage of a large number of entangled particles for a significant amount of time.

To achieve information-theoretic security using the QIA protocol, it should be ensured that the classical key or entanglement state shared by users in advance, cannot be generally reused or obtained by eavesdroppers. In addition, identity authentication should be performed simultaneously with QKD or other protocols to prevent eavesdroppers from directly distributing the key by skipping the authentication stage.

It is clear that the implementation of QIA is similar to classical identity authentication; both are certificates where participants hold the identity key without disclosing it. The difference is that the identity key can be either classical or quantum in the former, whereas it is always classical in the latter. However, the practical application of QIA protocol is currently limited. This is because QIA is generally used in conjunction with quantum cryptographic protocols that implement other cryptographic functions, such as QKD. However, in most quantum cryptographic protocols, the classical channel frequently uses an information-theoretic secure MAC to ensure message integrity. This technique not only guarantees that the classic message does not tamper with but also realizes the function of identity authentication. Therefore, typically, there is no requirement to perform additional authentication using quantum cryptographic protocols.

6 Quantum digital signature protocol

In 2001, Gottesman and Chuang first proposed the concept of a quantum digital signature (QDS) and provided the first QDS protocol based on a quantum one-way function [21]. Although the protocol requires difficult techniques, such as quantum storage, quantum state exchange comparison testing, and secure quantum channels, it has attracted significant interest in QDS research owing to its advantages for information-theoretic security. Unfortunately, Barnum et al. proved that the digital signature of quantum messages is not feasible even if it is computationally secure [22]. Subsequently, attempts have been made to reduce restrictions on existing QDS requirements and propose the concept of an arbitrated quantum signature. Arbitration quantum signatures require arbitration assistance to complete digital signature verification, which is different from the practical application of a digital signature. QDS has attracted attention because it signs not only classical but also quantum messages.

Similar to other quantum cryptographic protocols, attackers will also violate the QDS protocol by exploiting physical device imperfections in practical applications. To overcome practical security problems, the DI-QDS protocol [23] has been proposed. Recently, to further improve the practicality and security of QDS, some protocols based on continuous variables and decoy states have also been proposed [24,25]. In addition, various QDS protocols have been proposed for practical application scenarios. For example, Qiu et al. proposed a QDS protocol for sensitive data access control [26], and Singh et al. used QDS to design a secure blockchain transaction protocol [27].

Currently, QDS primarily focuses on a special case of the tripartite protocol, including a signer, receiver, and verifier. The verifier must share the authentication key in advance, which cannot meet the convenience requirement that any user can verify the classical digital signature. In addition, few experimental and practical

results have been reported on QDS. In summary, QDS remains far from practical, both in technical and theoretical terms.

7 Quantum two-party secure computation protocol

7.1 Quantum bit commitment

Bit commitment is a two-party cryptography technique that includes the following phases: In the commit phase, Alice (the sender of the commitment) decides the value of bit b ($b = 0$ or 1) that he/she intends to commit and sends Bob (the receiver of the commitment) a piece of evidence. Later, in the unveil phase, Alice announces the value of b and Bob checks it with the evidence. This concept was first proposed by Blum, who achieved the Turing prize in 1995. Bit commitment can be used to build zero-knowledge proof, verifiable secret sharing, coin flipping, and other protocols. This is considered one of the most important basic protocols for secure multi-party computation. Researchers expect to explore the feasibility of realizing information-theoretic secure bit commitment through quantum methods.

In 1997, Lo and Chau constructed a standard model of the quantum bit commitment (QBC) protocol and proved that the bit commitment protocol under the standard model could not achieve information-theoretic security in both classical and quantum environments [28]. Mayers independently demonstrated this conclusion [29]. The conclusion, known as the no-go theorem, has become a major obstacle to the development of the QBC and other quantum two-party secure computation protocols. Thereafter, researchers have attempted to relax the QBC protocol conditional to evade the no-go theorem, such as the noisy quantum storage model and special relativity model proposals.

Ng et al. completed the QBC experiment under the noisy quantum storage model in 2012 [30]. In 2013 and 2014, Lunghi et al. and Liu et al. completed QBC experiments using a special relativity model [31,32].

In summary, the correctness of the no-go theorem has been recognized by a vast majority of researchers, and critical theoretical obstacles remain for realizing QBC protocol information-theoretic security. Although the noisy quantum storage and special relativity models evade the no-go theorem, the former cannot achieve information-theoretic security while the latter lacks practical potential.

7.2 Quantum coin flipping

Coin-flipping is defined as a problem in which two mutually distrustful and remote players intend to agree on a random bit without relying on a third party. According to whether the participants have a fixed preference for the result, the coin-flipping protocol can be divided into strong coin-flipping and weak coin-flipping protocol. In the strong coin-flipping protocol, the dishonest party's attack cannot make the probability of either flipping result greater than $p = 1/2 + \varepsilon$. In the weak coin-flipping protocol, the two parties have different preferred outcomes, and the dishonest party's attack cannot make the probability of his/her preferred flipping result greater than $p = 1/2 + \varepsilon$. Parameter ε is called the bias of a party (or protocol). ε measures the protocol security, the smaller the ε, the greater the protocol security. ε should be strictly less than $1/2$ to ensure that the cheater does not gain complete control over the flipping result. A coin-flipping protocol is fair if and only if the biases of both parties are equal. Therefore, the coin-flipping protocol is perfect when both sides have a bias of 0.

The quantum coin-flipping protocol was first proposed by Bennett and Brassard in 1984 [1]. However, 10 years later, Lo and Chau proved that no perfect quantum coin-flipping protocol exists. Subsequently, researchers have focused on the quantum coin-flipping protocol with a smaller bias. Kitaev proved that the bias of any strong quantum coin-flipping protocol could not be less than 0.207. In 2007, Mochon proved that the bias of the quantum weak coin-flipping protocol could be arbitrarily small [33]. In 2009, Berlín et al. proposed and defined a loss-tolerant quantum coin-flipping protocol and proved that the bias obtained by either party through cheating was 0.4 [34]. In 2010, Chailloux et al. proved that either party of the loss-tolerant quantum coin-flipping protocol can obtain a bias of at least 0.359 through cheating [35].

In an experimental implementation, in 2010, Chailloux et al. implemented a strong quantum coin-flipping protocol with a bias of 0.207 [36]. In 2020, Bozzio et al. proposed a practical weak quantum coin-flipping protocol requiring only single-photon and linear optical devices with a bias of 0.207 [37].

Currently, the quantum strong coin-flipping protocol bias cannot be less than 0.207 (i.e., the cheating probability of both parties is 0.707), and in the case of noise and loss, the bias is at least 0.35 [38]. This probability is too high, which makes the quantum coin-flipping protocol impractical.

DOI 10.15302/J-SSCAE-2022.04.015

7.3 Quantum oblivious transfer

As a privacy-preserving communication protocol, the oblivious transfer (OT) protocol is widely used in many privacy-sensitive fields, such as secure multiparty computation and authentication protocols. Similar to research on other cryptographic protocols, researchers aim to use quantum technology to realize the information-theoretic secure OT protocol, namely quantum oblivious transfer (QOT).

In 1988, Crépeau et al. proposed the first QOT protocol, which assumes that Bob cannot delay the quantum measurement process [39]. Subsequently, scholars proposed a variety of QOT protocols based on QBC, albeit with the proposal of the no-go theorem, these protocols are no longer secure. Meanwhile, researchers have been exploring the QOT, which breaks the no-go theorem. In 2002, Shimizu et al. proposed a protocol to transmit secret messages with a 50% probability of success (all-or-nothing OT). In this protocol, Bob cannot obtain a secret message with 100% probability, thereby avoiding the limitation of the no-go theorem [40]. In 2005, Damgard et al. considered three special scenarios to overcome the no-go theorem and realized all-or-nothing QOT and QBC protocols based on the BB84 protocol [41]. In 2016, Pitalúa-García proposed a spacetime-constrained 1-out-of-2 QOT protocol, which was experimentally verified in 2018 [42].

Currently, the optimal cheating probability of the QOT protocol can reach $2/3$ for semi-honest participants [43]. In 2021, Amiri et al. proposed a 1-out-of-2 semi-random QOT protocol that achieved a cheating probability of $2/3$ when the participant was dishonest [44]. The semi-random QOT protocol is defined as follows: receiver Bob randomly obtains one of sender Alice's bit messages in (x_0,x_1), that is, (b,x_b). Alice cannot obtain Bob's output message, (b,x_b).

In summary, the 1-out-of-2 QOT protocol could never avoid the no-go theorem. To overcome this limitation, multiple proposed protocols are based on the assumption that the technical conditions of users are limited, and frequently no longer information-theoretic secure. In addition, quantum channel noise is a significant challenge in the practical application of QOT. Therefore, the QOT protocol requires significant research before practical implementation is feasible.

7.4 Quantum private query

In many scenarios, it is not only necessary to protect transmitted information from external attackers, but also to protect the private data of communication parties from being obtained by each other. Symmetric private information retrieval (SPIR) is a cryptographic task. In essence, SPIR implements 1-out-of-n OT. According to the no-go theorem, an ideal SPIR cannot be realized using quantum cryptography. Currently, the most practical approach is to relax the privacy requirements in SPIR to the "cheating sensitive" (that is, all effective cheating behaviors have a non-zero probability to be discovered by the other party), which is usually called quantum private query (QPQ) [45].

The security requirements of QPQ are as follows: (1) Alice identifies the cheating behavior of database owner Bob attempting to obtain the user Alice's search address with a non-zero probability. (2) Alice can obtain a limited number of database entries in addition to the retrieved entries. These extra items are random and not typically required by Alice, and Bob typically does not attempt to attack at the risk of being discovered, as this will damage his reputation and possibly result in severe punishment. Therefore, these security requirements are not ideal; however, they can meet application requirements.

In 2008, Giovannetti et al. proposed the first QPQ protocol (GLM protocol) [46]. In this protocol, Bob encodes database information into unitary operations. After receiving Alice's query quantum state, he applies a unitary operation to the query state and returns it to Alice. Alice obtains the desired database entry through measurements. Such protocols make good sense in theory; however, their implementation is impractical. Contrastingly, the entire database (especially when the size is large) is encoded by unitary operations, which are difficult to implement under existing technologies because the unitary operation dimension is too high. However, this type of protocol cannot tolerate channel loss; that is, once channel loss occurs, it threatens the privacy of both parties. Additionally, imperfect signal sources and channel noise affect the success probability of the protocol in practice. To solve these challenges, considerable research has been conducted on the QPQ protocol.

In 2011, Jacobi et al. proposed a QPQ protocol (J protocol) based on Scarani et al.'s QKD protocol [47,48]. This is implemented with the assistance of existing QKD technology. Essentially, implementation difficulty is independent of database scale and can tolerate channel loss. Therefore, it is considered an outstanding practical potential cryptographic protocol, in addition to QKD. However, data items available to the protocol users are not sufficiently flexible. Either too many data items are not conducive to protecting database security or too few items

increase failure probability. In 2015, Liu et al. designed a QPQ protocol based on a round-robin differential-phase-shift QKD protocol to ensure that honest users could only obtain one database entry. This guarantees ideal database security, and the protocol has zero failure probability, implying that it will consistently execute successfully when noise is ignored [49].

In addition, researchers have also identified new problems encountered by QPQ in practice, each of which has been solved. Wei et al. proposed “low-shift and addition” (LSA) technology, which not only can be used to query from a large database but also retains the features of “ideal database security” and “zero-failure” even under a weak coherent source [50]. To overcome channel noise, Gao et al. [51] and Chan et al. [52] proposed the use of an error-correcting code and check matrix to post-process the original QPQ key. In 2019, Chen et al. proposed a protocol for a network private query in a quantum wireless network with multiple third parties, in which any user can query the database with the assistance of third parties by measuring each of the distant nodes that initially share entanglement [53].

In summary, the QPQ protocol can only be realized using the same light source and detector as in the BB84 protocol. This has good practical potential because the technology for error correction and privacy amplification is abundant. Compared with QKD, it has greater theoretical difficulty because the two parties in QPQ can cheat each other, and the privacy of both parties should be protected. One specific manifestation is that the current QPQ has a low error rate tolerance (4% under typical parameters [54]).

8 Future research directions

It is well known that quantum computing poses a significant challenge to modern cryptographic security. With the QKD protocol proposed and proven to have information-theoretic security, quantum cryptography has gradually become a pertinent option for the next generation of cryptographic technology that could resist quantum computing attacks.

In classical cryptography, algorithms and protocols have reached a state of mature development, including symmetric or public key encryption algorithms to ensure message confidentiality, MAC to ensure message integrity and source reliability, and the digital signature to ensure non-repudiation of the message. These mature algorithms and protocols with various functions constitute a complete wooden bucket (Fig. 1) that can ensure the secure operation of an information system in a complex network environment.

In view of major QKD security advantages, researchers anticipate learning from QKD concepts and comprehensively improving the security of various cryptographic protocols by introducing quantum technology with the aim of finally building an information-theoretic secure protocol system. However, from the perspective of large-scale experimental progress, QKD (also commonly called “quantum communication”) is the predominant quantum cryptographic protocol that has reached a practical level. In general, the quantum cryptographic protocol is currently in an unbalanced state as QKD is significantly more advanced than other protocols. Therefore, to achieve the goal of comprehensively improving information systems security, significant research on quantum cryptographic protocols is still required.

As yet, multiple scientific problems must be solved in quantum cryptographic protocols. For example, at the micro level, new theories are required to combat the influence of channel noise and identify new cryptographic tasks based on quantum cryptographic characteristics. At the macro level, it is necessary to solve the quantum public-key cryptography problem. At the application level, a new cryptographic system combining quantum and classical cryptography is required. The following points describe these key issues and discuss potential technical approaches to solving them.

(1) A new theory to manage channel noise is required. In quantum cryptographic protocols, eavesdropping typically causes uncontrollable interference in quantum states. Considering this feature, quantum cryptographic protocols involve steps to detect eavesdropping. Typically, measured results of quantum states are compared with their expected states to obtain the error rate, and subsequently determine whether eavesdropping has occurred. It is well known that channel noise itself will create a certain error rate, and the attacker can obtain illegal key information under the cover of noise. Therefore, to combat channel noise, quantum cryptographic protocols must have a classical post-processing process that aims to correct errors and compress information obtained illegally by attackers. This post-processing process is the crux of strictly proving the security of quantum cryptographic protocols and remains a challenge in related research. According to different protocol security requirements, providing a new theory to correctly deal with channel noise is a key problem to be solved in the practical implementation of quantum cryptographic protocols.

DOI 10.15302/J-SSCAE-2022.04.015

(2) New cryptographic tasks are required based on quantum cryptography characteristics. In quantum cryptography research, quantum protocols are frequently designed with the same functions as classical cryptographic protocols. However, quantum and classical cryptography have fundamentally different security bases and may be applicable to different cryptographic tasks. This may explain why a bottleneck has been encountered in designing quantum cryptographic protocols that follow the goals of classical cryptographic protocols. Therefore, according to the characteristics of quantum theory, a promising research concept exists in attempting to change the security goal of classical cryptographic protocols or explore new cryptographic tasks. A successful QPQ protocol is a typical example of this, as it modifies the security goal of classical 1-out-of-n OT to the "cheating sensitive" type, which not only caters to the characteristics of quantum protocols but also meets the requirements of practical applications with good practical potential.

(3) Quantum public-key cryptography models are required. From an application perspective, two important issues must be solved in quantum cryptographic protocol research as follows: digital signatures and two-party secure computation. The former is widely used and indispensable in daily communication networks, and the latter is the basic component of building other complex cryptographic protocols, both of which occupy an important position in cryptographic protocol systems. In classic cryptography, digital signatures and two-party secure computations are mostly achieved using public-key cryptographic algorithms. However, to date, a practical quantum public-key cryptographic algorithm/scheme has not been identified. In fact, the pursuit of information-theoretic security by quantum cryptography contradicts the properties of public-key cryptography, as it is not based on mathematical complexity assumptions. Quantum public-key cryptography is likely to be a new model that differs from classical public-key cryptography; however, it can implement the function of classical public-key cryptography. Therefore, the use of quantum mechanical properties to achieve a function similar to that of public-key cryptography has become the predominant task to appropriately solve these aforementioned problems.

As mentioned above, quantum cryptography may not be similar to classical cryptography, where public key cryptography can be designed, and digital signatures and two-party secure computation protocols can be obtained based on it. Therefore, it may be possible to design a quantum digital signature protocol with practical potential and a two-party secure computation protocol capable of crossing the no-go theorem.

(4) A new cryptosystem that combines quantum and classical cryptography is required. Currently, the development of some typical protocols in quantum cryptography has encountered a bottleneck, which complicates meeting the application requirements of comprehensively improving the security of information systems. Information systems that involve related functions can only be protected using classical cryptography. Therefore, the cryptosystem combines quantum and classical cryptography; for example, the key distribution is quantum and the digital signature (because no practical quantum protocol exists) is classical. If the (currently available) quantum cryptographic protocol is simply combined with the classical cryptographic protocol, quantum cryptography may be meaningless. From this perspective, focusing on currently available quantum cryptographic protocols (such as QKD and QPQ), it is feasible to design classical cryptographic protocols matching these quantum protocols to ensure that the use of quantum cryptographic protocols provides practical security advantages, even if only to a certain extent. Valuable research questions include: 1) Can the use of currently available quantum cryptography improve the security of some classical cryptography in essence? 2) If so, how can this new security feature be defined? 3) How did various cryptography functions develop before public-key cryptography emerged? This clearly has important reference value for quantum cryptography, which currently has no public-key cryptography. 4) Can the functions of trusted third parties be fully explored to assist in solving bottleneck-type problems in quantum cryptographic protocols, such as digital signatures and two-party secure computation? In summary, if quantum cryptography remains too complex for implementation in the foreseeable future, it continues to be an extremely meaningful topic to study in terms of what improvements could be made to classical cryptography.

9 Suggestions for relevant research in China

To achieve comprehensive improvement of information systems security, the aforementioned problems must be solved in quantum cryptographic protocols. However, unique quantum cryptography security is fascinating. Theoretically, this topic will likely generate new concepts, valuable inspiration, and substantial security improvements in the development of cryptographic algorithms and protocols. For applications, it can at least realize a new system with limited functions and significant advantages in some scenarios; for example, a private network with few functions ("multi-function" often means that non-information-theoretic security classical

cryptography must be used, the use of which will limit overall information systems security, making it unable to achieve “high security” pursued by quantum cryptography). As quantum cryptography resists quantum computing attacks, subsequent research in this field may benefit from the following suggestions.

9.1 Research on quantum and post-quantum cryptography should be conducted simultaneously

Public-key cryptography can be designed based on mathematical problems (such as lattice, multivariable, hash, and coding) that currently, cannot be effectively solved by quantum computing. Such cryptography is called post-quantum (or anti-quantum) cryptography. Although post-quantum cryptography cannot achieve information-theoretic security, its ability to resist quantum computing attacks has been widely recognized, and it consists of advantages including good compatibility and easy implementation. Because quantum and post-quantum cryptography have their own advantages, both are important options for resisting quantum-computing attacks. Considering the rapid development of quantum computers, it is necessary to prepare for these two aspects and ensure the simultaneous development of research.

It should be emphasized that, although to date, practical quantum cryptography is not perfect, it is of great significance to the development of cryptography. Research on quantum cryptographic systems is a lengthy process, which should not be abandoned because of the high technical cost or short-sighted behavior of the excessive pursuit of practicality. On one hand, with the development of technology, the cost of quantum cryptography equipment will decrease, and may also lead to theoretical breakthroughs (for example, protocol post-processing difficulty will be significantly reduced after the reduction of quantum channel noise). However, even if post-quantum cryptography is applied in a speedier manner, quantum cryptography may continue to be beneficial in the future because the latter has a stronger theoretical basis against quantum computing attacks.

9.2 Strengthen interdisciplinary research of “quantum science and technology” and “cryptography” and relevant talent training

In quantum cryptography, it is imperative to develop a new cryptographic system that combines quantum and classical cryptography. In post-quantum cryptography, the study of quantum computational algorithms that can be used for cryptanalysis is also crucial for evaluating “quantum security”. Both these key research directions require professionals to be familiar with both disciplines. However, owing to the independence and professionalism of the two disciplines, cross-research is difficult, the threshold is high, and a shortage of researchers who meet the above requirements remains. This makes our relevant research still lag behind foreign countries. Therefore, it can be considered good practice to provide policy support for corresponding cross-research and talent training.

9.3 Optimize related fundamental research evaluation

The cryptography field preventing quantum computing attacks is currently in its infancy as a theoretical concept. To advance further in the field, relevant researchers must dare to chew “hard bones”. In some current assessment and evaluation mechanisms, the eagerness for quick success and instant benefit (such as the pursuit of short-term results and big projects) is not conducive to long-term research. Therefore, continuing to optimize the assessment and evaluation mechanism of related research and creating a scientific research environment suitable for “long-term research surrounding a problem”, will play a positive role in effectively promoting future research in this tentative field.

10 Conclusion

This study investigates and analyzes the research status of quantum cryptographic protocols such as QKD, QSDC, QSS, QIA, QDS, and quantum two-party secure computation. It is confirmed that current quantum cryptographic protocols remain in an unbalanced state and that QKD is significantly ahead of other protocols which have difficulty achieving breakthroughs. Further significant research is required to establish a mature and practical protocol system. On this basis, the key problems to be solved in future quantum cryptography and related research suggestions are provided from the micro-, macro-, and application perspectives.

Quantum cryptography is a new field with high-security potential; therefore, it has important research value. From the application perspective, it is almost inevitable that it must be combined with classical cryptography. Improving overall information systems security must be considered. Few practical quantum cryptographic protocols exist; thus, specific networks with fewer functions can be prioritized in applications. In the future, with

DOI 10.15302/J-SSCAE-2022.04.015

practical quantum cryptographic protocol improvement and matched classical cryptography techniques, quantum cryptography will have a broad application space.

Acknowledgments

We would like to extend our gratitude to Li Yongmei, Guo Mingchao, Cai Xiaoqiu, Li Jing, Wei Chunyan, Wu Shengyao, Wei Dongmei, and other members of the research team for their assistance in preparing this study.

References

[1] Bennett C H, Brassard G. WITHDRAWN: Quantum cryptography: Public key distribution and coin tossing [C]. New York: Proceedings of the IEEE International Conference on Computers Systems and Signal Processing, 1984.

[2] Christandl M, Ferrara R, Horodecki K. Upper bounds on device independent quantum key distribution [J]. Physical Review Letters, 2021, 126(16): 160501.

[3] Schwonnek R, Goh K T, Primaatmaja I W, et al. Device-independent quantum key distribution with random key basis [J]. Nature Communications, 2021, 12(1): 2880.

[4] Woodward R I, Lo Y S, Pittaluga M, et al. Gigahertz measurement device-independent quantum key distribution using directly modulated lasers [J]. npj Quantum Information, 2021, 7: 58.

[5] Zeng P, Zhou H Y, Wu W J, et al. Quantum key distribution surpassing the repeaterless rate-transmittance bound without global phase locking [J]. arXiv: 2201.04300, 2022, accepted by Nature Communications.

[6] Chen Y A, Zhang Q, Chen T Y, et al. An integrated space-to-ground quantum communication network over 4600 kilometres [J]. Nature, 2021, 589: 214–219.

[7] Feng Z, Li S B, Xu Z Y. Experimental underwater quantum key distribution [J]. Optics Express, 2021, 29(6): 8725–8736.

[8] Wang S, Yin Z Q, He D Y, et al. Twin-field quantum key distribution over 830 km fiber [J]. Nature Photonics, 2022, 16: 154–161.

[9] Liu X, Hu J, Li Z F, et al. Heralded entanglement distribution between two absorptive quantum memories [J]. Nature, 2021, 594: 41–45.

[10] Long G L, Liu X S. Theoretically efficient high-capacity quantum key- distribution scheme [J]. Physical Review A, 2002, 65(3): 032302.

[11] Deng F G, Long G L. Secure direct communication with a quantum one-time pad [J]. Physical Review A, 2004, 69(5): 052319.

[12] Long G L, Deng F G, Wang C, et al. Quantum secure direct communication and deterministic secure quantum communication [J]. Frontiers of Physics in China, 2007, 2(3): 251–272.

[13] Hu J Y, Yu B, Jing M Y, et al. Experimental quantum secure direct communication with single photons [J]. Light-Science & Applications, 2016, 5: e16144.

[14] Qi Z T, Li Y H, Huang Y W, et al. A 15-user quantum secure direct communication network [J]. Light-Science & Applications, 2021, 10(1): 183.

[15] Hillery M, Bužek V, Berthiaume A. Quantum secret sharing [J]. Physical Review A, 1999, 59(3): 1829.

[16] Chou Y H, Zeng G J, Chen X Y, et al. Multiparty weighted threshold quantum secret sharing based on the Chinese remainder theorem to share quantum information [J]. Scientific Reports, 2021, 11: 1–10.

[17] Bell B, Markham D, Herrera-Martí D, et al. Experimental demonstration of graph-state quantum secret sharing [J]. Nature Communications, 2014, 5(1): 1–12.

[18] Zhou Y, Yu J, Yan Z, et al. Quantum secret sharing among four players using multipartite bound entanglement of an optical field [J]. Physical Review Letters, 2018, 121(15): 150502.

[19] Liao Q, Liu H, Zhu L, et al. Quantum secret sharing using discretely modulated coherent states [J]. Physical Review A, 2021, 103(3): 032410.

[20] Dušek M, Haderka O, Hendrych M, et al. Quantum identification system [J]. Physical Review A, 1999, 60(1): 149.

[21] Gottesman D, Chuang I L. Quantum digital signatures [C]. arXiv: quant-ph/0105032, 2001.

[22] Barnum H, Crépeau C, Gottesman D, et al. Authentication of quantum messages [C]. Vancouver: The 43th Annual IEEE Symposium on Foundations of Computer Science, 2002.

[23] Puthoor I V, Amiri R, Wallden P, et al. Measurement-device independent quantum digital signatures [J]. Physical Review A, 2016, 94(2): 022328.

[24] Thornton M, Scott H, Croal C, et al. Continuous-variable quantum digital signatures over insecure channels [J]. Physical Review A, 2019, 99(3): 032341.

[25] Zhao W, Shi R, Ruan X. High-efficiency continuous-variable quantum digital signature protocol for signing multi-bit messages [J]. Laser Physics Letters, 2021, 18(3): 035201.

[26] Qiu L, Cai F, Xu G. Quantum digital signature for the access control of sensitive data in the big data era [J]. Future Generation Computer Systems-The International Journal of eScience, 2018, 86: 372–379.

[27] Singh S, Rajput N K, Rathi V K, et al. Securing blockchain transactions using quantum teleportation and quantum digital signature [J]. Neural Processing Letters, 2020. DOI: 10.1007/S11063-020-10272-1.
[28] Lo H K, Chau H F. Is Quantum bit commitment really possible? [J]. Physical Review Letters, 1997, 78(17): 3410–3413.
[29] Mayers D. Unconditionally secure quantum bit commitment is impossible [J]. Physical Review Letters, 1997, 78(17): 3414–3417.
[30] Ng N, Joshi S, Ming C, et al. Experimental implementation of bit commitment in the noisy-storage model [J]. Nature Communications, 2012, 3: 1326.
[31] Lunghi T, Kaniewski J, Bussières F, et al. Experimental bit commitment based on quantum communication and special relativity [J]. Physical Review Letters, 2013, 111: 180504.
[32] Liu Y, Cao Y, Curty M, et al. Experimental unconditionally secure bit commitment [J]. Physical Review Letters, 2014, 112: 010504.
[33] Mochon C. Quantum weak coin flipping with arbitrarily small bias [J]. arXiv:0711.4114, 2007.
[34] Berlín G, Brassard G, Bussières F, et al. Fair loss-tolerant quantum coin flipping [J]. Physical Review A, 2009, 80(6): 062321.
[35] Chailloux A. Improved loss-tolerant quantum coin flipping [J]. arXiv:1009.0044, 2010.
[36] Chailloux A, Kerenidis I. Optimal quantum strong coin flipping [C]. Atlanta: 2009 50th Annual IEEE Symposium on Foundations of Computer Science, 2010.
[37] Bozzio M, Chabaud U, Kerenidis I, et al. Quantum weak coin flipping with a single photon [J]. Physical Review A, 2020, 102(2): 022414.
[38] Pappa A, Jouguet P, Lawson T, et al. Experimental plug and play quantum coin flipping [J]. Nature Communications, 2014, 5: 3717.
[39] Crépeau C, Kilian J. Achieving oblivious transfer using weakened security assumptions [R]. White Plains: 29th Annual Symposium on Foundations of Computer Science, 1988.
[40] Shimizu K, Imoto N. Communication channels analogous to one out of two oblivious transfers based on quantum uncertainty [J]. Physical Review A, 2002, 66(5): 052316.
[41] Damgard I B, Fehr S, Salvail L, et al. Cryptography in the bounded quantum-storage model [C]. Pittsburgh: 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS'05), 2005.
[42] Pitalúa-García D. Spacetime-constrained oblivious transfer [J]. Physical Review A, 2016, 93(6): 062346.
[43] Chailloux A, Gutoski G, Sikora J. Optimal bounds for semi-honest quantum oblivious transfer [J]. Chicago Journal of Theoretical Computer Science, 2016: 1–16.
[44] Amiri R, Stárek R, Reichmuth D, et al. Imperfect 1-out-of-2 quantum oblivious transfer: Bounds, a protocol, and its experimental implementation [J]. PRX Quantum, 2021, 2(1): 010335.
[45] Gao F, Qin S, Huang W, et al. Quantum private query: A new kind of practical quantum cryptographic protocol [J]. Science China Physics, Mechanics & Astronomy, 2019, 62(7): 70301.
[46] Giovannetti V, Lloyd S, Maccone L. Quantum private queries [J]. Physical Review Letters, 2008, 100(23): 230502.
[47] Scarani V, Acin A, Ribordy G, et al. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations [J]. Physical Review Letters, 2004, 92(5): 057901.
[48] Jakobi M, Simon C, Gisin N, et al. Practical private database queries based on a quantum-key-distribution protocol [J]. Physical Review A, 2011, 83(2): 022301.
[49] Liu B, Gao F, Huang W, et al. QKD-based quantum private query without a failure probability [J]. Science China-Physics Mechanics & Astronomy, 2015, 58(10): 100301.
[50] Wei C, Cai X, Liu B, et al. A generic construction of quantum oblivious-key-transfer-based private query with ideal database security and zero failure [J]. IEEE Transactions on Computers, 2018, 67(1): 2–8.
[51] Gao F, Liu B, Huang W, et al. Postprocessing of the oblivious key in quantum private query [J]. IEEE Journal of Selected Topics in Quantum Electronics, 2015, 21(3): 98–108.
[52] Chan P, Lucio-Martinez I, Mo X, et al. Performing private database queries in a real-world environment using a quantum protocol [J]. Scientific Reports, 2014, 4: 5233.
[53] Li N, Li J, Chen X B, et al. Quantum wireless network private query with multiple third parties [J]. IEEE Access, 2019, 7: 33964–33969.
[54] Wei C, Cai X, Wang T, et al. Error tolerance bound in QKD-based quantum private query [J]. IEEE Journal on Selected Areas in Communications, 2020, 38(3): 517–527.