Archives of Computational Methods in Engineering (2021) 28:3831–3868
https://doi.org/10.1007/s11831-021-09561-2

ORIGINAL PAPER

State-of-the-Art Survey of Quantum Cryptography

Ajay Kumar[1] · **Sunita Garhwal**[1]

Received: 20 April 2020 / Accepted: 28 January 2021 / Published online: 19 April 2021

Abstract
In today Internet era, confidential information transmitted over an insecure channel. With the significant development in the area of quantum computing, there is a need for unconditional security in confidential information. Quantum key distribution protocols are proven secure if all devices are perfect (in terms of technologies and proper protocol operations). The major challenges in quantum communication are secret key rate, distance, cost and size of QKD devices. The purpose of this survey article is to carry out a systematic review in the area of quantum cryptography by covering various aspects of non-deterministic quantum key distribution protocols, quantum secure direct communication, semi-quantum key distribution, secure multiparty communication protocol, post-quantum cryptography and device-independent cryptography techniques. In addition, we also discussed various experimental work carried out in the area of quantum cryptography, various attacks and challenges relative to the paradigm shift from classical cryptography to quantum cryptography. Quantum cryptography will become a future replacement of classical cryptography techniques after the development of the first physical quantum computer.

Abbreviations

PNS	Photon number splitting
CHSH	Clauser Horne Shimony Holt
QBER	Quantum bit error rate
RSA	Rivest Shamir Adleman
DES	Data encryption standard
QKD	Quantum key distribution
QSDC	Quantum secure direct communication
SQKD	Semi-quantum key distribution
SMPC	Secure multiparty communication
ASQKD	Authenticated semi-quantum key distribution
DIQKD	Device independent quantum key distribution
EPR	Einstein Podolsky Rosen

1 Introduction

In a conventional digital communication system, information can be passively monitored or copied; some eavesdropper can alter even information. Classical cryptosystem methods (Rivest–Shamir–Adleman (RSA), Data Encryption Standard (DES)) are based on number theory and guesswork. There is a need for more secure communication as the number of users using online transaction are increasing day by day. If two parties do not share secret initially, then it is impossible in the classical system to share secret key over an insecure channel between these parties. In the today Internet era, our personal information (Such as Financial and Health) and National security data are transmitted over the Internet. Security of these transmitted data is utmost importance in today world. Shor [1] designed an algorithm for finding prime factors of a large number. Once quantum computer will be available, Shor's algorithm will give security threats to all classical cryptographic protocol [2]. Research in quantum computing accelerated after the Shor's algorithm and Grover's search algorithm [3].

In a quantum system, information can not be copied (No-cloning Theorem) or read by an eavesdropper. Classical information can be copied like students prepare notes from a book or blackboard without any disturbance, whereas quantum information can not be copied. Any uncontrollable control in quantum information is likely to be detected by the legitimate user. The concept of quantum cryptography evolved with Wiesner's [4] idea almost fourth-nine years ago, and now commercial key distribution devices are available. Paper was written back in 1970 and remained unpublished till 1983 as no one showed interest in his work. He described quantum coding and its application in money-making and multiplexing of two or three messages (reading of one message can destroy other messages). He pointed out

✉ Ajay Kumar
ajayloura@gmail.com

[1] Computer Science and Engineering Department, Thapar Institute of Engineering and Technology, Patiala, India

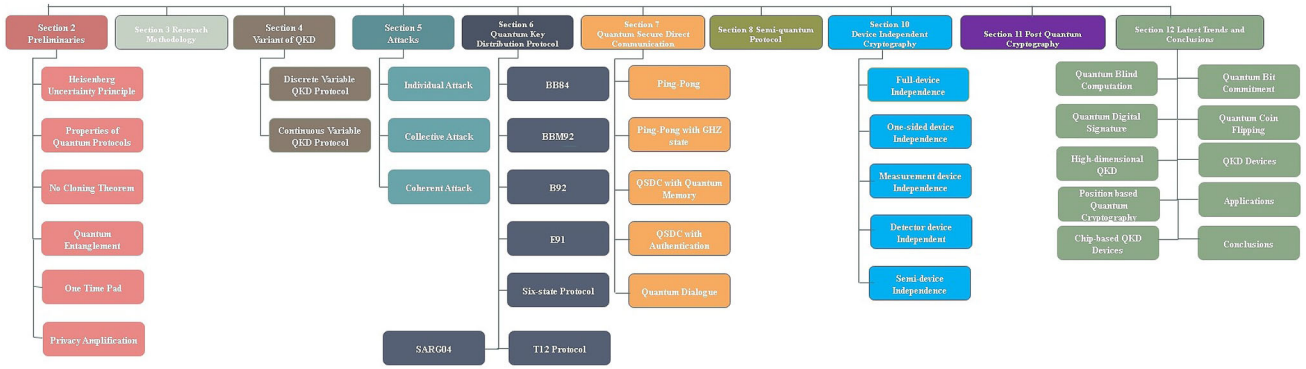


Fig. 1 Survey organization

that quantum money will have a serial number (similar as classical money) and 20 perfectly reflective boxes (each box contains a single photon in one of the four states, i.e. vertical, horizontal, right-circular or left-circular). Bank will maintain a record of each photon in each box with respect to the serial number of quantum money, and fake currency can be avoided using the concept of no-cloning theorem.

Gisin et al. [5] carried out an early review on quantum cryptography in 2002. Similar studies were carried out by Alleaume et al. [6], Giampouris [7] Diamanti et al. [8], Long [9] and Zhou et al. [10]. We believe that there is still a need to carry out an in-depth study of the various quantum cryptographic protocol. Compared with previous existing survey papers [5–10], our survey introduces the in-depth discussion of Quantum key distribution protocols, reviews the existing work published up to 2020, serving as a guide for other researchers to understand and apply the existing protocols, current research directions and discusses several open problems. Further, this survey also helps the reader to identify a few most impacting protocols and their sources.

For a better understanding of the state-of-the-art in quantum cryptography, we surveyed with the following goals:

- We review various concepts and terminologies used for understanding quantum protocols.
- A state-of-the-art of current trends in quantum cryptography. We further elaborate various quantum attacks on quantum protocols.
- An exhaustive survey on deterministic protocols for quantum secure communication without the shared secret key.
- To identify and discusses the current trends in quantum cryptography like satellite-based communication, device-independent cryptography and high-dimensional Quantum key distribution.
- Classification of discrete and continuous-variable quantum key distribution.
- We survey the existing literature on semi-quantum key distribution protocols.
- An in-depth overview of multiparty communication protocols.

Outline of the Paper The rest of the paper is organized as follows. Section 2 outlines the concepts of quantum cryptography. In Sect. 3, research methodology has been described. Section 4 deals Discrete and Continuous Variable Quantum Key Distribution and in Sect. 5, we classify various quantum attacks. In Sect. 6, we described various Quantum Key Distribution Protocols. Sections 7, 8 and 9 deals with Quantum Secure Direct Communication, Semi-quantum Key Distribution Protocol and Secure Multiparty Communication, respectively. In Sect. 10, Device-Independent Cryptography will be introduced and followed by Post Quantum Cryptography in Sect. 11. Section 12 describes the current trends, sources of quantum cryptography research, various papers in terms of citations (Google as well as Web of Science), few real-life applications of quantum cryptography, and concluding remarks. Figure 1 represents the organization of the paper.

2 Preliminaries

In this section, several fundamental aspects of quantum communication will be discussed.

The Heisenberg Uncertainty Principle: [11] It states that certain pairs of physical properties are related and complementary in the sense measuring one property, prevent simultaneously knowing of other property and destroying it. Two-photon polarization rectilinear (horizontal and vertical) and diagonal (at 45° and 135°) are complementary to each other.

Properties of Quantum Protocol: Quantum Protocol must be secure, correct and robust. In the classical protocol, correction and security are the primary concern. Quantum protocols

are based on either the Heisenberg uncertainty principle or quantum entanglement.

- *Correct:* Bob can able to decrypt the original message from Cipher-text using the decryption key.
- *Secure:* Eve has no gain of the information sent from Alice to Bob.
- *Robustness:* The legitimate user (Alice/Bob) will detect errors if Eve attempt to obtain or alter the information

No Cloning Theorem: [12] It states that an unknown quantum state cannot be cloned.

Quantum Entanglement: State of two or more quantum particles are entangled if many of the physical properties of the particles are strongly correlated. State of an individual particle cannot be specified individually. Einstein et al. [13] gave the initial thought that quantum mechanics is incomplete and described the concept of quantum entanglement by "Spooky action at a distance". Quantum entanglement is a crucial phenomenon for long-distance quantum key distribution. If two qubits are maximal entanglement, then no eavesdropper has any share of entanglement. The heart of quantum cryptography is entangled states. It means quantum entanglement particle A and B must satisfy the following inequality:

$$|\psi\rangle_{AB} \neq |\psi\rangle_A \otimes |\psi\rangle_B$$

Following are four maximally entangled states.

$$|\psi_1\rangle = 1/\sqrt{2}(|0\rangle|0\rangle + |1\rangle|1\rangle)$$
$$|\psi_2\rangle = 1/\sqrt{2}(|0\rangle|0\rangle - |1\rangle|1\rangle)$$
$$|\psi_3\rangle = 1/\sqrt{2}(|0\rangle|1\rangle + |1\rangle|0\rangle)$$
$$|\psi_4\rangle = 1/\sqrt{2}(|0\rangle|1\rangle - |1\rangle|0\rangle)$$

One Time Pad: Vernam [14] introduced the concept of one-time pad or Vernam Cipher in 1918. Message and Secret key are represented using a sequence of 0's and 1's using an encoding mechanism.

- Encryption Process: It is carried out by XOR (modulo 2) of the original message with secret key bit by bit.
  Plain text(m): 11001101
  Secret Key(k): 01100101
  Ciphertext(c): 10101000 $c = m \oplus k$ and $\oplus$ is XOR operation.
- Decryption Process: This is carried out by performing XOR of the cipher text and the secret key.
  Ciphertext(c): 10101000
  Secret Key(k): 01100101
  Plain text(m): 11001101 $m = c \oplus k$

The classical one-time pad allows Alice and Bob to share a secret message over the public classical channel. Quantum one-time pad allows Alice and bob to share the secret message (in the form of private quantum states) over a public quantum channel. Assume Alice, Bob and Eve share a quantum state ψ_{ABE}. Schumacher and Westmoreland [15] worked on classical private message sharing between Alice and Bob by considering that Eve state is unrelated with state of Alice and Bob, i.e. $\psi_{ABE} = \psi_{AB} \otimes \psi_E$. Brandao and Oppenheim [16] carried out the work on the quantum one-time pad for sharing quantum messages by considering that Alice and Bob's state is related with Eve state.
Quantum One-time Pad Encryption: $|e\rangle = X^k|m\rangle$ and $X|m\rangle = |m \oplus 1\rangle$
Quantum One-time Pad Decryption: $|m\rangle = X^k|e\rangle = X^k|X^k m\rangle$
Here X is a quantum operation for performing bit flip.
If $k = 0$ then $X^0 = I$
If $k = 1$ then $X^1 = X$

Quantum Bit Error Rate (QBER): In a classical system, the bit error rate is the error rate due to noise, interference or any other issues like imperfections in sending or receiving device. It indicates the quality of signal and success of packet delivery. In a quantum system, QBER is defined by the ratio of the error rate to the key rate. QBER provides useful information about Eavesdropper presence and how much information eavesdropper knows.

Privacy Amplification: In the quantum protocol, privacy amplification is performed to reduce the amount of information known to Eve by shrinking the key. Bennett et al. [17] introduced the concept of privacy amplification for amplifying the privacy between Alice and Bob.

3 Research Methodology

Table 1 represents the review process, search criterion, databases, inclusion and exclusion criterion. Figure 2 depicts the types of research papers considered in this survey paper. Paper selection consists of following two phases:

1. Title and Abstract Level Screening: Initially, We had selected papers from 1964 to 2020, and two essential papers of 1927 and 1935 are considered. In this screening, we used the inclusion/exclusion criterion to publication title and abstract. To minimize the research bias, both authors independently analyzed the search results and analyzed the results. Disagreements were resolved through discussion. Figure 3 depicts the number of research publications used from 1980 onward in this review paper.

Table 1 Review methodology, search criterion, databases, inclusion and exclusion criterion

Property	Category
Publication	Journal articles
	Conference, symposium and workshop Paper
	Web link of reputed companies (Toshiba, QuantumCTek, ID Quantique)
	Patents, reports
	PhD/master thesis of reputed institute
Year	1964–2020
Evaluation	Initial screening using title and abstract
Criterion	Followed by full-text
Search	Quantum cryptography
strings	Quantum protocol
	Quantum key distribution
Automated search in digital libraries	www.webofknowledge.com
	https://aps.org
	https://ArXiv.org/
	https://ieeexplore.ieee.org/Xplore/home.jsp
	https://www.springer.com/
	https://www.sciencedirect.com/
	https://google.com/
Classification of papers	Quantum key distribution,
	Quantum secure direct communication,
	Semi-quantum key distribution,
	Secure multiparty communication,
	Device independent cryptography,
	Post quantum cryptography
Inclusion	Focus on the quantum protocols
Exclusion Criterion	Similar paper in ArXiv and later published in journal
	Tutorials and short papers

2. Full-Text Screening: In this phase, we had analyzed the papers based on the full text. We applied the inclusion-exclusion criterion specified in Table 1. If two or more papers were contributed by the same authors and their significant contribution is same, we considered the most relevant paper with a significant contribution.

4 Discrete and Continuous Variable Quantum Key Distribution Protocol

Quantum key distribution protocols are classified into Discrete variable QKD and Continuous variable QKD protocol. Table 2 represents the major differences between discrete and continuous variable protocols.

- Discrete Variable QKD Protocol: In discrete variable QKD protocol, discrete refers to the spin of electron or polarization of single photon. BB84, E91, SARG04, B92 are few examples of discrete variable QKD protocol.
- Continuous Variable QKD Protocol: In continuous variable QKD protocol, Information is stored in the form of light. Protocol based on continuous variable offer advantage over discrete because coherent light with photon can easily producible using laser than single-photon [18]. Ralph [19] and Reid [20] independently introduced the concept of continuous-variable quantum key distribution. Ralph [19] examined two continuous variable scheme based on coherent light and 2-mode squeezed light. Table 3 represents the classification of continuous-variable quantum key distribution based on source state and detection mechanism. In Table 3, squeeze state refers to the state with very low variance in one quadrature and very high in other quadrature. Coherent state refers to a state with no quadrature having very low variance. Hillery [21] proposed a continuous analogue of BB84 using squeezed states of light and Homodyne detection mechanism. Garcia-Patron and Cerf [22] proposed a continuous-variable QKD protocol based on squeezed states and heterodyne detection for obtaining higher security key rate over the noisy line. Cerf and Grangier [23] surveyed various continuous-variable Quantum key distribution protocol.
  Leverrier and Grangier [29] proposed two continuous variable QKD protocols with discrete modulation using two and four coherent states. They established the security of these protocols against collective attacks. Recently, Papanastasiou and Pirandola [30] designed continuous-variable QKD protocol using discrete-alphabet encoding. They also studied the protocol against collective Gaussian attacks.
  Andersen et al. [31] discussed the integration of discrete and continuous variable QKD in the applications of quantum teleportation, entanglement distillation, error-correcting and testing Bell inequalities.

5 Quantum Attacks

Eve's attacks can be classified into individual, collective and coherent attacks. The coherent attack is considered as the most powerful among individual, collective and coherent attacks. Table 4 indicates a summary of individual, collective and coherent attacks. More details on these classes can be found in the PhD thesis of Snchez [32].

- Individual Attack: Eve prepares each ancilla qubit independently, interact with each qubit on quantum channel independently and measure independently. With the

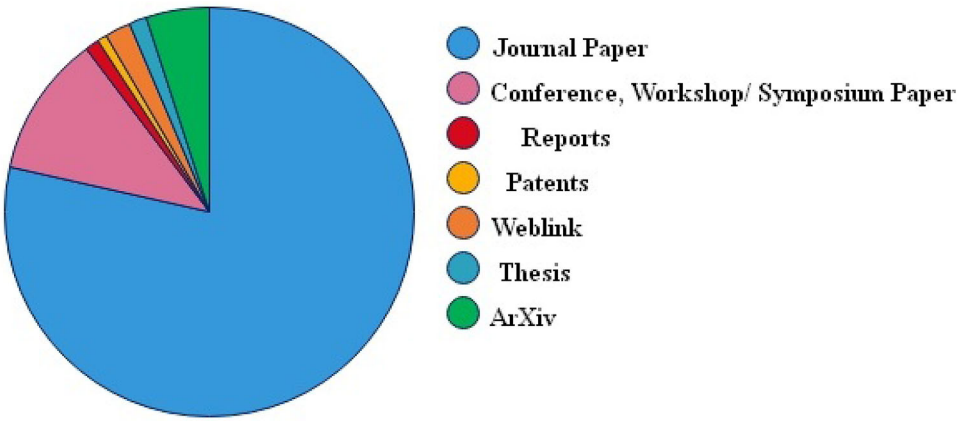


Fig. 2 Graphical representation for type of papers referred in the review process

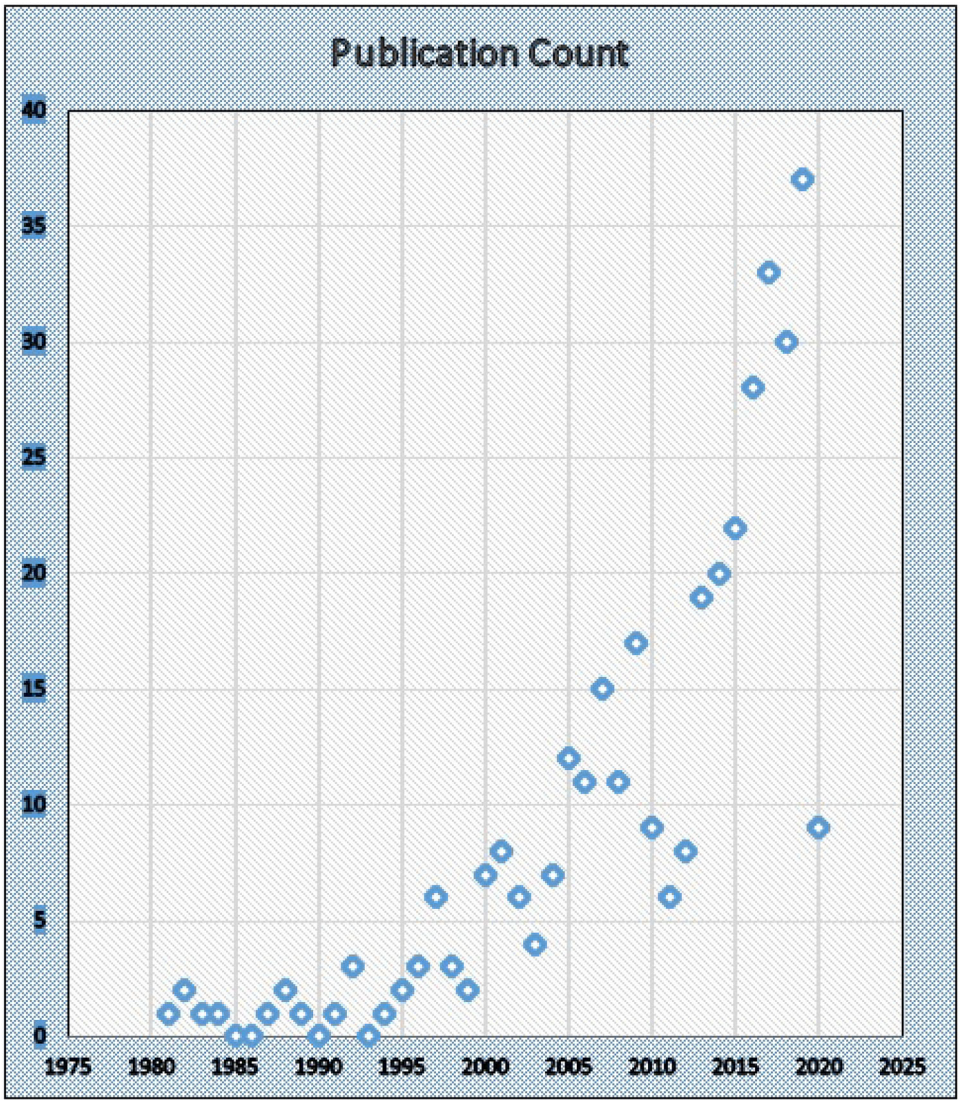


Fig. 3 Number of publications from 1980 onward in the area of quantum cryptography

Table 2 Discrete and continuous variable protocols

Type of protocol	Information prepared	Detection technique	Example
Discrete variable	Qubits (Polarization of single photon or single electron)	Single photon counter	BB84, SARG04
Continuous variable	Continuous spectrum quantum observable (quadrature of light)	Homodyne detection	Grosshans–Grangier protocol
		Heterodyne detection	Noise-tolerant protocol

Table 3 Classification of various continuous-variable protocol [23]

Author's names	Source state	Detection technique	Protocol
Cerf et al. [24]	Squeezed state	Homodyne detection	Cerf–Levy–VanAssche
Grosshans and Grangier [25]	Coherent state	Homodyne detection	Grosshans–Grangier
Grosshans et al. [26]			
Lodewyck et al. [27]	Coherent state	Heterodyne detection	No basis-switching
Weedbrook et al. [28]			
Garcia-Patron and Cerf [22]	Squeezed state	Heterodyne detection	Noise-tolerant

Table 4 Classes of attack in quantum cryptography

Type of attack	Ancilla qubit prepared individually	Interaction with qubits on channel	Measurement	Quantum memory	Powerful	Example
Individual	✓	✓	✓	✗	Least	Intercept-resend Faked-state [33]
Collective	✓	✓	✗	✓	Moderate	Symmetric collective attacks [34]
Coherent	✗	✗	✗	✓	Strongest	PNS attack [35–37]

technology available today, only Individual attacks are applicable.

- Collective Attack: Eve prepares each ancilla qubit independently, interact with each qubit on quantum channel independently and measure jointly all ancilla qubits. The collective attack is a subclass of Coherent attack.
- Coherent Attack (Joint Attack): Eve prepares entangled states of the ancilla qubits, interact with qubits on the channel and then measure all ancilla qubits collectively.

Makarov and Hjelme [33] discussed the concept of Faked states attack. Instead of creating the original state, Eve generates a light pulse, and the legitimate user (Alice or Bob) will not be able to notice the eavesdropper. Faked states is a kind of intercept and resend attack.

Pirandola [34] proposed the symmetric collective attacks by extending individual symmetric attacks of Gisin et al. [5] and Fuchs et al. [38] for BB84 and six-state protocols.

Photon Number Splitting Attack (PNS attack: Typically used laser sources are coherent, and they emit more than one photon in each signal. Alice usually encodes her qubits in one photon, two photons, three photons and so on with frequency $p_1, p_2, p_3, \ldots$ respectively. Eve (not limited by no-cloning theorem) keep few of the photons and store them in quantum memory whereas letting the other photons go to the Bob. Such an attack is known as photon-number splitting attack [35–37]. Eve waits till Alice reveals the bases publically to Bob using a classical channel. Thereafter, Eve reveals the state deterministically. In the PNS attack, Eve presence should not be noticed as the photon rate received by Bob remains unmodified.

Vakhitov et al. [39] introduced the concept of a large pulse attack. It is based on the conventional optical eavesdropping, and it eliminates the need for immediate interaction. Dehmani et al. [40] studied the effect of cloning attacks with several eavesdroppers on the quantum error and mutual infor-

mation between honest parties. Gisin et al. [41] analyzed the effect of Trojan horse attack on quantum key distribution. They found that all system must have counter-measure and auxiliary detector monitors the incoming light. Kronberg and Molotkov [42] analyzed the concept of an optimal attack on BB84 protocol based on linear fiber optical elements and controlled-NOT. Gisin et al. [41], Jain et al. [43] and Fei et al. [44] carried out their work on Trojan-horse and Man-in-the-middle attack, respectively.

Side Channel attacks refer to the imperfections caused by experimental set up rather than information gained by a protocol implementation. Lamas-Linares and Kurtsiefer [45] experimentally demonstrated the timing-side channel attack. In timing side-channel attack, timing information disclosed by Communicating parties (Alice and Bob) during the public discussion is used by Eve to access the significant part of the secret key. Qi et al. [46] introduced the time-shift attack in which Eve shift the arrival time of signal pulse or synchronization pulses or both between Alice and Bob.

Sun et al. [47] used a quantum hacking strategy by tampering the source without leaving the trace behind. Various quantum attacks can be classified into attack at source (Photon number splitting attack [35–37], Phase remapping attack [48,49], Laser Seeding (Sun et al. [47] etc.) and attack at detection (Timing-side channel attack [45], Faked state attack [33], Time-shift attack [46,50] and Polarization shift [51]).

In recent years, Various researchers studied the eavesdropper strategy in quantum cryptography [52,53]. Jain et al. [54] carried out a study on various attacks and their protection in quantum key distribution protocol.

6 Quantum Key Distribution Protocol

Quantum Key Distribution (QKD) utilize the concept of quantum mechanics for sharing the secret keys from one party (Alice) to another (Bob). It can not prevent eavesdropper while enabling the legitimate user to detect the eavesdropper and throw away the key if eavesdropper detected and new key generation takes place. QKD protocols are based on the concept of the no-cloning theorem, Heisenberg uncertainty principle and entanglement property. QKD usage, both classical and quantum channel. Figure 4 represents the significant developments in quantum cryptography and Fig. 5 represents the significant developments in Quantum Key Distribution Protocols.

6.1 BB84 Protocol

In 1984, Bennett and Brassard [55,56] developed a first quantum key distribution protocol named as BB84 based on the concept of quantum coding proposed by Wiesner's [4]. They presented a protocol for coin tossing by exchanging quantum messages. In BB84, information is encoded in orthogonal quantum states. BB84 protocol can be classified as prepare and measure protocol. In prepare and measure protocol, one party (say Alice) prepare a quantum state and send the prepared quantum state to another party (say Bob), who will measure it. Both party then compare measurement and preparation bases and after post-processing comes up with a shared secret key (Fig. 6).

In BB84, Alice prepare a random qubit for sending to Bob in Circular (C) basis $\{|+\rangle, |-\rangle\}$ with direction 45 and 135 degrees respectively or Rectilinear (R) $\{|0\rangle, |1\rangle\}$ with direction 0 and 90 degree respectively. It is a 4-state (vertical, horizontal, right-circular, left-circular) QKD protocol.

Rectilinear (R) Basis:

$$|\rightarrow\rangle = |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$|\uparrow\rangle = |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Circular (C) Basis:

$$|\nearrow\rangle = 1/\sqrt{2}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = 1/\sqrt{2}(|\rightarrow\rangle + |\uparrow\rangle)$$

$$|\nwarrow\rangle = 1/\sqrt{2}\begin{pmatrix} -1 \\ 1 \end{pmatrix} \quad = 1/\sqrt{2}(-|\rightarrow\rangle + |\uparrow\rangle)$$

BB84 is divided into quantum transmission phase (step 1 to step 4) and classical communication phase (step 5 and step 6).

Algorithm 1 BB84 protocol [55]

1: Alice chooses n-random bit by flipping coin.
2: Alice again flip coin n-times for determining the basis used for each corresponding random bit.
3: Alice prepares the random bits in their corresponding basis and sends to Bob.
4: Bob does not know the basis corresponding to each random bit. He tosses the coin n-times. He measures the received qubit in the obtained random basis after tossing the coin. Bob announces the receipt of states.
5: Alice and Bob publicly compare their bases using an authentic classical channel. Alice informs the Bob regarding bases agreement and disagreement. If they disagree on a particular basis, they drop the corresponding bit. Now Bob will get only $n/2$ random bits and $n/2$ random bits are scratch out.
6: Bob randomly choose half of the remaining $n/2$ random bits obtained from Step 5 and compare with Alice publicly. If both disagree above a permitted allowed errors (due to noise), then they drop the complete sequence of random bits and it indicate that Eve was listening. If these $n/4$ random bits are almost similar (i.e. within permitted allowed error due to noise) means Eve was not listening. In this case, remaining $n/4$ will be used as a random key between Alice and Bob.

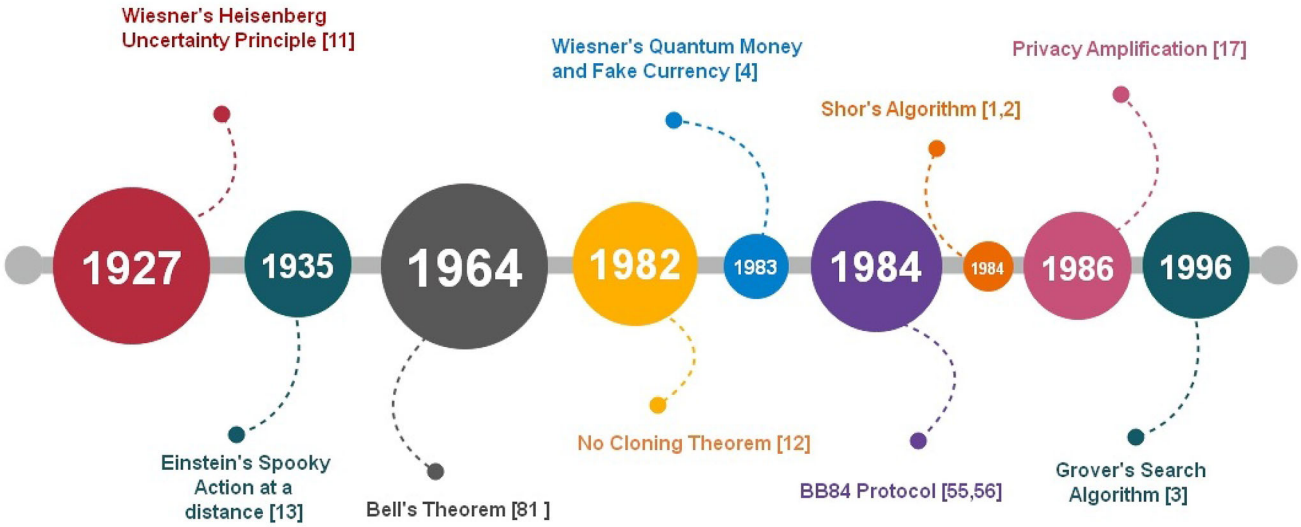
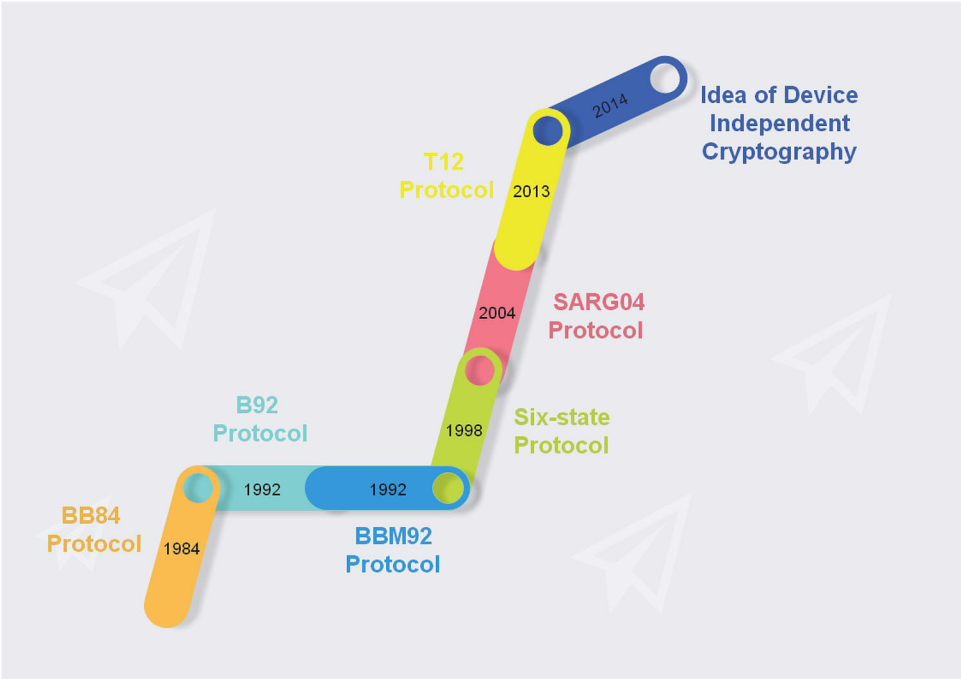


Fig. 4 Significant development in quantum cryptography

Fig. 5 Significant development in quantum key distribution protocols



For a particular bit, if Alice and Bob both measure on the same basis, they will get the same result for that particular bit. If Alice send a particular bit in a Circular Basis and Bob measure it in Rectilinear Basis, then there is 50-50% chance of getting $|\rightarrow>$ or $|\uparrow>$. Similarly, If Alice send a particular bit in Rectilinear Basis and Bob measure it in Circular Basis, then there is 50–50% chance of getting $\nearrow>$ or $\nwarrow>$.

In BB84, Alice communicate the basis in which she prepared her qubits on a classical authenticate channel to Bob. If the same basis used by Bob, then their result matches otherwise they discard the qubit. This process is called **basis reconciliation** or **Sifting**. If Alice and Bob want to share n bit key, then Alice needs to start with $4n$ quantum bits as $2n$ random bit available after step 4 and only n quantum bit key is generated after step 6. If the transmission has not disturbed, then the shared key obtained after step 6 is used in the same way as one-time pad used in a classical cryptosystem. Table 5 illustrates an example of a shared secret key generated using the BB84 protocol.

Step 6 of BB84 can be carried out by various techniques such as parity checking [57]. In step 6.1, Alice selects some random bits with odd parity, and Bob at the other end, picks the same set of random bits and their parity are compared. In step 6.2, Alice select some random bits will even parity, and

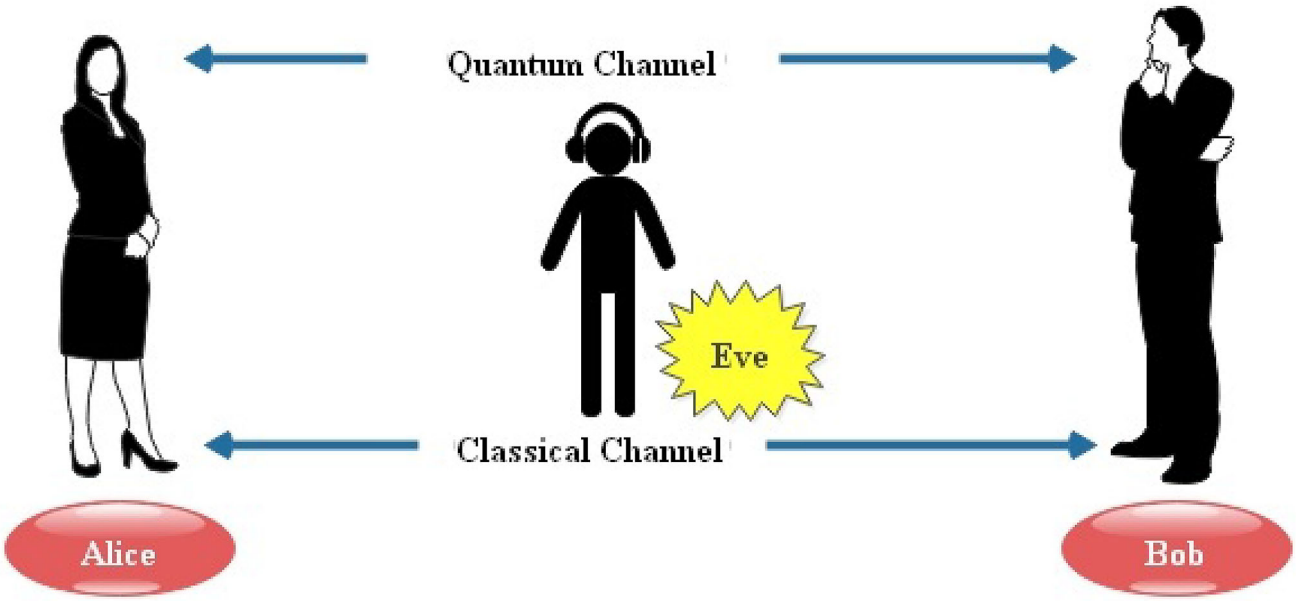


Fig. 6 Communication between Alice and Bob using classical and quantum channel

Table 5 Example of quantum secret key sharing in BB84 protocol [56]

Bit no.	1	2	3	4	5	6	7	8	...
Alice's random bit	1	1	0	0	0	1	0	1	...
Alice's random Basis	R	C	R	C	R	R	R	C	...
Alice's qubit	| ↑>	| ↖>	|→>	|↗>	|→>	|↑>	|→>	| ↖>	...
Bob's random basis	R	R	R	C	R	R	C	C	...
Bob's observed qubit	| ↑>	| ↑>	| →>	| ↗>	| →>	| ↑>	| ↖>	| ↖>	...
Basis matching	OK		OK	OK	OK	OK		OK	...
Presumably shared key	1		0	0	0	1		1	...
Alice–Bob security test			0		0			1	...
Final secret key	1			0		1			...

Bob check the same at the other end. If Alice and Bob agree for odd and even parity, there is very less chance of having eavesdropper.

Unconditional security (Secure irrespective of the computational power used by Eve) of BB84 protocol has been proved by various researchers [58–60]. Scarani and Kurtsiefer [61] pointed out the real implementation problems of QKD on 25th anniversary of BB84 protocol and suggested two options (device-independent security and reasonable security of a device). Their idea later give rise to the concept of device-independent cryptography. BB84 is completely robust if Alice and Bob both usage qubit. If one party (say Alice) unknowingly transmit two or more copies of the qubit, then BB84 is partially robust.

Goldenberg and Vaidman [62] proposed GV protocol based on the orthogonal states. They claimed that their approach ensures the detection of eavesdroppers. Peres [63] commented on Goldenberg and Vaidman protocol that Goldenberg and Vaidman protocol support similar features as BB84 protocol. Further, Goldenberg and Vaidman [64] reclaimed the novelty of their protocol and pointed out that they had used carrier of information in a quantum state and the quantum state belongs to a definite set of orthonormal states.

Dan et al. [65] proposed an intercept/resend attack on BB84 based on Breidbart basis. Using their proposed attacking strategy, the probability of Eve detection will decrease. Although Eve can not be able to obtain the exact information. Wang et al. [66] analyzed the man-in-the-middle attack on the BB84 protocol and suggested the defence mechanism against it. An et al. [67] suggested solution for Beam Splitter attack in BB84 protocol. Garcia-Patron et al. [68] proposed single-photon two-qubit quantum logic for simulating the optimal individual attack on BB84 protocol without quantum memory.

Boyer et al. [69] proposed a protocol BB84-INFO-z (Identical to BB84, except information bits are in z-basis) and

found that the modification in BB84 does not harm its security against collective attacks. Fung et al. [48] introduced the phase-remapping attack in QKD protocol. Eve introduces phase-remapping by time-shift on the signal pulses. They showed that if Alice and Bob are unaware of the attack, then the final secret key will be compromised in some situations. Jiang et al. [70] introduced the frequency shift attack using the imperfection used in phase-remapping attack [48]. Using frequency shift attack, Eve gets more information as compared to phase-remapping attack. Fuchs et al. [38] presented optimal eavesdropping strategy for four state BB84 protocol.

6.2 BBM92 Protocol

Bennett, Brassard and Mermin [71] proposed entanglement version of BB84 named BBM92 without the usage of Bell's theorem. In BBM92, Alice and Bob both take photons generated from a central source, and Alice is not supposed to generate a photon. If Alice and Bob usage the same measurement basis, then their results are perfectly correlated. If Alice and Bob choose a different basis (Alice choose C-basis and Bob choose R-basis or vice-versa), then their results will not be correlated.
BBM92 is again divided into quantum transmission phase (Step 1- Step 3) and classical communication phase (Step 4-Step 5). Classical communication phase of BBM92 and BB84 protocols are the same.

Algorithm 2 BBM92 protocol [71]

1: Alice and Bob receive their entangled photon from a central source.
2: Alice chooses n-random bases (either R or C basis) corresponding to each random bit.
3: Bob also chooses n-random bases (either R or C basis) corresponding to each random bit.
4: Alice and Bob publicly compare their bases using an authentic classical channel. Alice and Bob carry out basis reconciliation. They keep the same basis qubit and discard the mismatch basis qubit.
5: Alice and Bob compare a random subset of qubits (nearly half of the qubits) to check the performance of the quantum channel. If they agree to a large extent, then a remaining subset of agreed keys are used as the final secret key. If the error rate is less than a permitted errors (let say 10%), then classical post-processing is done for correcting the remaining bits. If the error rate is higher, then they drop the corresponding qubits and procedure is repeated.

Table 6 illustrates example of shared secret key generated using BBM92 protocol with two bases and maximally entangled state $|\psi_1\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$.
Waks et al. [72] presented the security proof for BBM92 protocol using realistic and un-trustable source against individual attacks. They found that average collision probability of BBM92 and BB84 is same, whereas, BBM92 perform better in terms of communication rate (a function of distance) as compared to BB84. Adenier et al. [73] proposed the double-blinding attack (On each side) on entangled protocols. The double-blinding attack is not a kind of intercept and resend attack. Eve is blocking entangled source completely and replacing it with pairs of bright pulses. In BBM92, Eve gets full information of the key and remain undetected.
Major advantage of BBM92 protocol is that Alice and Bob will detect any malicious control by Eavesdropper to the source. In BBM92, we do not require a trusted central source for generating entangled photon.

6.3 B92 Protocol

Usage of two different bases in BB84 protocol is redundant. In 1992, Bennett proposed a new protocol named B92 using one non-orthogonal basis($\rightarrow$, $\nearrow$). In B92, Alice used only one non-orthogonal basis. In B92 protocol [74], Alice only sends information using the following two non-orthogonal states.

$$|\rightarrow\rangle = |0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$$

$$|\nearrow\rangle = 1/\sqrt{2}(|\uparrow\rangle + |\rightarrow\rangle) = \quad 1/\sqrt{2}\begin{pmatrix}1\\1\end{pmatrix}$$

Alice represents random bit 0 and 1 by $\rightarrow$ and $\nearrow$ respectively.

Algorithm 3 B92 protocol [74]

1: Alice chooses n-random bit by flipping coin. She sends $|\rightarrow>$ for random bit 0 and $|\nearrow>$ for random bit 1.
2: Bob measure received qubit in Rectilinear (R) or Circular (C) basis. Bob certain cases occur when he observes $|\uparrow>$ and $|\nwarrow>$. Bob uncertain cases occur when he observes $\rightarrow$ and $\nearrow$.Table 7 and 8 show the certain and uncertain cases in B92 protocol. If Bob observes $|\uparrow>$ in Rectilinear basis, then the bit is 1. If Bob observes $\nwarrow$ in Circular basis, then the bit is 0.
3: Bob publicly informs Alice regarding uncertain bits and share half of the certain bits to ensure security. The remaining half of the certain bit can be used as a secret key.

Table 9 illustrates one example of a shared secret key generated using the B92 protocol.
Tamaki et al. [76,77] proved the security of B92 using a single-photon source. Koashi [78] proposed the implementation of B92 using strong phase-reference coherent light. Kuppam [79] analysed and compared the performance of BB84 and B92 protocol in PRISM. He observed that the B92 protocol performs better in term of eavesdropper detection as compared to BB84. The number of accurate measurement by eavesdropper is less in B92 as compared to BB84. Phoenix et al. [80] proposed a three mutually non-orthogonal state protocol to overcome suppression attack in B92 protocol. Senekane et al. [81] demonstrated an optical implementation of the six-state QKD protocol using three non-orthogonal states. They added the additional features of

Table 6 Example of secret key sharing using BBM92 protocol [57]

Bit no.	1	2	3	4	5	6	7	8	9	10	11	12	...
Alice's bases	C	R	C	C	R	C	C	R	C	R	R	R	...
Bob's bases	C	R	C	R	C	R	C	R	R	R	R	R	...
Alice's observation	1	0	1	0	1	1	0	0	0	1	0	1	...
Bob's observation	1	0	1	1	0	0	0	0	1	1	0	1	...
Bases comparison	OK	OK	OK				OK	OK		OK	OK	OK	...
Agreed key	1	0	1				0	0		1	0	1	...
Security test	1						0	0				1	...
Final secret key		0	1							1	0		...

Table 7 Certain cases for B92 protocol [75]

Bob basis	Bob observe	Alice sent	Bit	Certainty reason
R	$\mid\uparrow>$	$\mid\nearrow>$	1	If Alice sent $\mid\rightarrow>$ then Bob receive $\mid\rightarrow>$ in R basis
C	$\mid\nwarrow>$	$\mid\rightarrow>$	0	If Alice sent $\mid\nearrow>$ then Bob receive $\nearrow$ in C basis

Table 8 Uncertain cases for B92 protocol [75]

Bob basis	Bob observe	Uncertainty reason	Bit
R	$\mid\rightarrow>$	Alice may sent $\mid\rightarrow>$ or $\mid\nearrow>$ collapse into $\mid\rightarrow>$	0|1
C	$\mid\nearrow>$	Alice may sent $\mid\nearrow>$ or $\mid\rightarrow>$ collapse into $\mid\nearrow>$	0|1

another detection set in [80] to improve security and eavesdropper detection probability.

6.4 E91 Protocol

Ekert [82] proposed an entanglement based protocol E91. He used the generalized Bell's theorem for testing of eavesdropping. His approach used Bohm's version of the Einstein–Podolsky–Rosen (EPR) for generating identical random numbers at remote places. A sequence of entangled pairs of qubits from central sources and each one of our communicators (Alice and Bob) received one of the pairs. In entangled pair, it does not matter whether Alice or Bob measure it first. If Alice/Bob measures the first pair, then Bob/Alice will collapse respectively.
Consider Alice and Bob are in maximally entangled using $|\psi_1\rangle$.

$$|\psi_1\rangle = |EPR\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$$

Using $|\psi_1|$ as entangled pair, Alice's and Bob's results are perfectly correlated when measured in the same basis (i.e. they receive exactly same bits).
Consider Alice and Bob are in maximally entangled using $|\psi_3\rangle$.

$$|\psi_3\rangle = |EPR\rangle = 1/\sqrt{2}(|10\rangle + |01\rangle)$$

Using $|\psi_3|$ as entangled pair, Alice's and Bob's results are perfectly anti-correlated when measured in the same basis(i.e. they receive inverted bits). Using $|\psi_3|$ following compatible cases can occur:

1. If Alice/Bob measure spin up, then Bob/Alice collapse into a spin down.
2. If Alice/Bob measure spin down, then Bob/Alice collapse into spin up.

Using $|\psi_3\rangle$ as entangled pair, following Incompatible cases can occur:

1. If Alice/Bob measure spin up, then Bob/Alice collapse into spin down or spin up.
2. If Alice/Bob measure spin down, then Bob/Alice collapse into spin up or spin down.

In E91 protocol, Alice's and Bob's results are perfectly correlated or anti-correlated, which help in identifying the Eavesdropper. Entangled pair become disentangled due to noise in the environment. Therefore we need to compare the matching of bases as in BB84 protocol.
In original E91 protocol [82], Ekert had considered three bases for Alice (0°, 45° and 90°) and Bob (45°, 90° and 135°). There are 1/3 chances that Alice and Bob measure in compatible bases (E91 original protocol consider three bases). Alice and Bob publicly announce their bases and discard

Table 9 Example of secret key in B92 protocol

Bit no.	1	2	3	4	5	6	7	8	...
Alice's bit	1	1	0	1	1	0	1	0	...
Alice's qubit	$\|\nearrow>$	$\|\nearrow>$	$\|\rightarrow>$	$\|\nearrow>$	$\|\nearrow>$	$\|\rightarrow>$	$\|\nearrow>$	$\|\rightarrow>$	...
Bob's random basis	R	C	C	C	R	C	C	R	...
Bob's bit's	1	0|1	0	0| 1	1	0	0| 1	0| 1	...
Certain bit	1		0		1	0			...
Security test	1					0			...
Final secret key			0		1				...

incompatible bases. In original E91 protocol, to produce a key size of N, we need to $6N$ original key size as there is 33% chances that bases are compatible and half of the key is used to check the eavesdropper.

Algorithm 4 E91 protocol

1: Alice and Bob receive their entangled photon from a central source using any one of four maximal entangled states($|\psi_1\rangle$ to $|\psi_4\rangle$). Consider source generate EPR pair $|\psi_3\rangle = |EPR\rangle = 1/\sqrt{2}(|10\rangle + |01\rangle)$
2: Alice chooses one of the bases from 0, 45 and 90 degree to measure her received particle from entangled pair [57].
3: Bob chooses one of the bases from 45, 90 or 135 degree to measure his received particle from entangled pair [57].
4: Alice and Bob publicly compare their basis using an authentic classical channel. For the same bases measurement, Alice and Bob's results are perfectly anti-correlated for $|\psi_3\rangle$ entangled state. Inversion or 1's complement of Bob's string is equal to Alice's string. Alice and Bob carry out the post-processing, which involves any error detection and correction phase.
5: For different Bases, Alice and Bob announce their result publicly for checking the performance of the channel using the Bell test. This test is used to ensure whether there is a potential eavesdropper present or not.

In 1964, John Stewart Bell [83] presented an analogy to Einstein Podolsky Rosen (EPR) paradox based on the spin measurement on pair of entangled photons. He presented a model of reality with hidden variables that allow entanglement. For classical particle, Bell's inequality will be satisfied with the measurement of particles. For entangled photons, the measurement will violate Bell's inequality, and it represents the quantum behaviour of a system. Hensen et al. [84] carried out an experiment and analyzed Loophole-free Bell test using electron spins in diamond at the Delft University of Technology. Ilic [85] described various concepts of error correction, privacy amplification and violation of Bell's theorem in E91 protocol. Li et al. [86] analysed the security of E91 protocol and proposed a model for noise analysis. Their result shows that Eavesdropper can maximally get 50% of the key if the noise level is approximately 0.5.
Inamori et al. [87] proposed a symmetric incoherent eavesdropping strategy in E91 protocol. If Eve controls the preparation of entangled photon, the effectiveness of E91 protocol reduces to BB84 protocol. Ling et al. [88] reported the implementation of E91 protocol by violating the Bell inequality to derive a secure key. Acin et al. [89] simplified the E91 protocol by taking three bases on one side and two bases on the other side. Honjo et al. [90] carried out an entanglement based QKD experiment over 100 KM of optical fiber using superconducting single-photon detectors.
Fujiwara et al. [91] demonstrated the experimental realisation of Acin et al. protocol [89] through 20 KM fiber using hybrid entanglement photon pair source. Li et al. [92] proposed a model of noise analysis in E91 protocol. They observed that Eve could get 50% of the secret key if the noise level reaches 0.5. Sharma and Lenka [93] applied the concept of E91 protocol in an online banking system for user authentications.

6.5 Six-State Protocol

Bruß [94] generalized the BB84 protocol and designed six-state protocol using three conjugate bases. These six states are pointing towards positive and negative of x-axis, y-axis and z-axis of the Bloch sphere. Bruß [94] further proved that six-state protocol are more secure than BB84 protocol. Implementation of the six-state protocol can be carried out using only optical technologies, without a quantum computer.
Three bases in six-state protocol are:
Along z-axis of Bloch Sphere: $|0\rangle, |1\rangle$
Along x-axis of Bloch Sphere: $1/\sqrt{2}(|0\rangle + |1\rangle), 1/\sqrt{2}(|0\rangle - |1\rangle)$
Along y-axis of Bloch Sphere: $1/\sqrt{2}(|0\rangle + i|1\rangle), 1/\sqrt{2}(|0\rangle - i|1\rangle)$
Alice selects the basis with equal probability of 1/3 and sends qubits to Bob. Increase in the number of inputs by Alice, make it difficult to learn the message to eavesdropper Eve. After Bob receives all qubits, Alice announces the basis used using a classical channel. Bob measure Alice's basis and their value are used as the key. Eavesdropper Eve can measure the qubit sent by Alice by choosing random basis (1/3 for correct bases and 2/3 for incorrect bases) and resend new qubits to Bob. Eve guesses the right bases with 1/3 probability and incorrect basis with 2/3 probability. Therefore, Bob receives the right qubits with probability 2/3 and incorrect qubits with

Table 10 Example of secret key in E91 protocol [57]

Bit no.	1	2	3	4	5	6	7	8	9	...
Alice's base	45	45	0	90	45	0	90	90	90	...
Bob's bases	90	45	135	90	45	135	45	90	135	...
Alice's observation	0	0	0	1	1	1	1	0	1	...
Bob's observation	1	1	0	0	0	0	0	1	1	...
Bases comparison		OK		OK	OK			OK		...
Same bases result		0|1		1|0	1|0					...
Agreed key		0		1	1			0		...
Different bases result	0|1		0|0			1|0	1|0		1|1	...

1/3 probability [94]. practical implementation and security proof of six-state protocol is difficult as compared to BB84.

Disadvantage of Six-State Protocol: In the six-state protocol, Bob has a quantum memory, and he performs all its measurement after Alice reveals the Basis. In contrast, in BB84 Bob initial measure his qubit in a random basis and then Alice send him the basis in which she prepared the qubits and mismatch basis are discarded.

Lo [95] proved the unconditional security of the six-state protocol. Lo demonstrated the bit error rate of 12.7%, which is an improvement over BB84 (11%) by allowing one-way classical communication. Kato and Tamaki [96] established the security proof of six-state protocol by using a photon number resolving detector. They found that the bit error rate threshold for six-state protocol is higher than the BB84 protocol. Garapo et al. [97] investigated the effect of collective-rotation noise on the six-state protocol. They observed that the six-state protocol is robust against intercept-resend attacks on collective noise while keeping the rotation angle within certain bounds. Bechmann-Pasquinucci and Gisin [98] found that coherent eavesdropping will not increase Eve's Shannon information but increase the probability of guessing all correct bits.

Recently, Azuma and Ban [99] investigated the six-state protocol against intercept/resend and collective attacks. They showed that intercept/resend attack can be described by hidden variable models, whereas, the hidden-variable model can not describe collective attacks if the disturbance is smaller than 1/3.

6.6 SARG04 Protocol

Scarani et al. [100] designed SARG04 protocol, which is robust against PNS attack with weak pulses. SARG04 uses two non-orthogonal quantum states similar to B92 protocol. BB84 and SARG04 protocols have the same transmission phase and the measurement phase. SARG04 usages a different post-processing phase as compared to BB84 protocol. SARG04 is more secure even Alice emits two photons.

In SARG04 protocol, Alice never announces her basis to Bob. In classical sifting procedure, Alice does not reveal her basis. For binary values of a_i and b_i gives us four different qubit states ($|\psi_{00}\rangle$, $|\psi_{10}\rangle$, $|\psi_{01}\rangle$, $|\psi_{11}\rangle$) as shown in Table 12. It is evident from the 4^{th} and 5^{th} column of Table 11 that a_i is encoded in Computational or Hadamard basis is decided by b_i. As Bob announces the receipt of qubits, Alice will not share the basis in which these qubits are prepared. Corresponding to each qubit, Alice prepare two states (one in computational basis and other in Hadamard basis) and announces both to Bob. For example, Alice transmit $|\psi_{11}\rangle$ and she announces $|\psi_{11}\rangle$ and $|\psi_{10}\rangle$ in Hadamard and computational basis respectively. Bob Hadamard measurement will result in $|\psi_{11}\rangle$, whereas computational measurement will result in $|\psi_{00}\rangle$ and and $|\psi_{10}\rangle$ with equal probability 1/2. If Bob observes $|\psi_{00}\rangle$ state, he can determine the state $|\psi_{11}\rangle$ sent by Alice. Further, Scarani et al. [100] proved that the SARG04 is more robust than BB84 against PNS attack. Table 11 represent various combinations of Alice announces and detection of a qubit by Bob (other cases like Alice transmit $|\psi_{00}\rangle$ and $|\psi_{11}\rangle$ for Alice qubit $|\psi_{00}\rangle$ will occur in the same way).

Branciard et al. [102] designed the entangled version of SARG04 and proved that for a wider class of Eve's attacks, SARG04 perform better than BB84 in terms of secret key rate and maximal achievable distance. Further, they also showed that the quantum bit error rate (QBER) of SARG04 is twice the QBER of BB84 if a channel of given visibility is available. Koashi [103] generalized the SARG04 protocol to n quantum state protocol. Fung et al. [104] compared the performance of SARG04 with decoy-state and SARG04 with two-way classical communication with BB84. They showed that SARG04 with two-way communications could tolerate a higher bit error rate than SARG04 with one-way communications.

6.7 T12 Protocol

Lucamarini et al. [105] introduced the concept of T12 protocol with the same features as BB84 except that decay qubits

Table 11 SARG04 Alice transmission states in computational and Hadamard basis [101]

State	a_i	b_i	a_i is encode in computational basis	a_i is encode in Hadamard basis
$\|\psi_{00}\rangle$	0	0	✓	
$\|\psi_{10}\rangle$	1	0	✓	
$\|\psi_{01}\rangle$	0	1		✓
$\|\psi_{11}\rangle$	1	1		✓

Table 12 Different combination of revealing the exact state by Bob in the SARG04 protocol [101,102]

Alice transmit	Alice announces	Bob observation 1 $p = 1$	Bob observation 2 $p = 1/2$	Bob observation 3 $p = 1/2$	Bob final decision
$\|\psi_{00}>$	$\|\psi_{00}>$	$\|\psi_{00}>$			$\|\psi_{00}>$
	$\|\psi_{01}>$		$\|\psi_{01}>$		
				$\|\psi_{11}>$	
$\|\psi_{01}>$	$\|\psi_{01}>$	$\|\psi_{01}>$			$\|\psi_{01}>$
	$\|\psi_{10}>$		$\|\psi_{10}>$		
				$\|\psi_{00}>$	
$\|\psi_{10}>$	$\|\psi_{10}>$	$\|\psi_{10}>$			$\|\psi_{10}>$
	$\|\psi_{01}>$		$\|\psi_{01}>$		
				$\|\psi_{11}>$	
$\|\psi_{11}>$	$\|\psi_{11}>$	$\|\psi_{11}>$			$\|\psi_{11}>$
	$\|\psi_{10}>$		$\|\psi_{10}>$		
				$\|\psi_{00}>$	

are used, and different probabilities are assigned to C and R basis. Decoy state protocol uses imperfect single-photon sources such as weak coherent state source. They observed increased efficiency with a higher key rate in a gigahertz clocked QKD system. Bases are selected using asymmetric probability using $P_Z \geq 1/2$ and $P_X = 1 - P_Z$.
Lucamarini et al. [105] found that the optimal probability value ($P_X \leq 1/16$) should be used to achieve higher possible key rate. Toshiba's QKD [106] (TQKD) system delivered digital keys over fiber optic using the concept of T12 protocol. TQKD provide the digital key over a distance of 50 KM with a bit rate one megabit per sec; otherwise, it also facilitates more than 100 Kms.

6.8 Other QKD Protocols

Table 13 represents a comparative summary of few QKD protocols. Bennett and Wiesner [107] found that Bob performs one of the four unitary operations on the EPR pairs prepared by Alice. By measuring two particles jointly, Alice can find the operation performed by Bob. Bechmann-Pasquinucci and Peres [108] proposed a QKD protocol using a 3-state system for carrying the information. They showed that the 3-state system provides better security than 2-state carriers. Inoue et al. [109] proposed differential phase shift QKD where a single photon is prepared in a superposition state of three basis kets. The phase difference between two pulses out of three pulses of photons is used to carry bit information from Alice to Bob. Deng and Long [110] proposed a two-way QKD protocol using faint laser pulses and without the involvement of basis reconciliation. In Deng and Long protocol, first Bob sends laser pulses to Alice, and Alice encodes it using unitary operations and returns laser pulses to Bob.
Stucki et al. [111] designed a Coherent one-way (COW) quantum key distribution protocol to work with weak coherent pulses and high bit rate. In COW protocol, emitter Alice encodes information in time. Alice information contains 0-pulses, no-light or $\mu-$pulses in time slot separated by T. Pan et al. [112] QKD protocol using twelve nonorthogonal states in a four-state system. Khan et al. [113] proposed KMB protocol that allows more noise without adding intermediate nodes by using two mutually unbiased bases. Any attempt by eavesdropper significantly increases the higher-dimensional photon state. In QKD protocols like BB84, a single particle is transmitted over the quantum channel to share the secret key. Noh [114] had introduced the concept of counterfactual quantum cryptography. Noh's protocol is more secure without the transmission of a particle on the quantum channel. Gao et al. [115], Wei et al. [116] and Gao et al. [117] carried out work on the quantum private queries.

Table 13 Comparative summary of few QKD protocols. Here O, N and C denote orthogonal, non-orthogonal and conjugate bases

Protocol name	Reference	Year	Prepare and measure	Basis	No. of basis/no. of bases states	Discrete/ continuous	Entanglement	Basis reconciliation
BB84	[55,56]	1984	✓	O	2, 4	D	✗	✓
BBM92	[71]	1992	✗	O	2, 4	D	✓	✓
B92	[74]	1992	✓	N	1, 2	D	✗	✗
E91	[82]	1991	✗	N	3, 5	D	✓	✓
Six-state	[94]	1998	✓	C	3, 6	D	✗	✓
SARG04	[100]	2004	✓	O	2, 4	D	✗	✗

7 Quantum Secure Direct Communication (QSDC)

Cryptographic protocols like BB84 are non-deterministic and used to establish a shared secret key. Alice encodes a bit in a quantum state and sends it to Bob, but Alice can not able to determine the value decoded by Bob. Beige et al. [118] introduced the concept of direct secure communication. There is no need for establishing a shared secret key in the direct secure communication. In direct secure communication, each photon transmits one bit of Alice's message without revealing any information to an eavesdropper. The protocol proposed by Beige et al. [118] is deterministic.
Alice represent $+$ and $-$ by $|n_+\rangle$ and $|n_-\rangle$ respectively, where n represent next cipher of Alice key. Alice announces her key publicly after verifying that no eavesdropper was listening. Hong-Mei [119] proposed a QSDC protocol based on cluster entangled state. Figure 7 depicts significant development in Quantum Secure Direct Communication.

7.1 Bostrom and Felbinger's Ping-Pong Protocol

Bostrom and Felbinger [120] proposed the concept of direct communication using the concept of entanglement. They proposed a deterministic ping-pong protocol. In ping-pong protocol, the transmission is instantaneous (no additional information is needed to decode the message), and no qubits are discarded. It can be used for plain-text or secret key transmission. For secret key transmission protocol is asymptotically secure, whereas in plain-text transmission it is quasi-secure.
Following steps are used in Bostrom and Felbinger ping-pong protocol [120]:

- Bob prepare two photons in an entangled state $|\psi_3\rangle = 1/\sqrt{2}(|0\rangle|1\rangle + |1\rangle|0\rangle)$.
- Bob keeps one photon (Home qubit) and send other photon (travel qubit) to Alice through quantum channel.
- Alice choose control or message mode.
- Alice choose message mode:

  In message mode, if Alice wants to send 0, she performs an identity operation $I = |0\rangle\langle 0| + |1\rangle\langle 1|$ on travel photon.
  If Alice wants to send 1, she performs $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$ on travel qubit which result into $|\psi_4\rangle = 1/\sqrt{2}(|0\rangle|1\rangle - |1\rangle|0\rangle)$.
  Alice send the travel qubit back to Bob.
  Bob perform Bell measurement which results in $|\psi_3\rangle$ or $|\psi_4\rangle$. Based on the result he can infer the encoded qubit is 0 or 1.

- Alice choose control mode:

  Alice perform measurement in z-basis.
  Alice inform her result to Bob using Public channel.
  Bob switches to control mode and perform measurement in the same basis.
  Presence of Eavesdropper is detected if their result coincide. If their result are anti-correlated then no eavesdropper is presented.

This protocol is called ping-pong as the travelling photon travels from Bob to Alice and back to Bob. In Ping-Pong protocol, no bit is discarded. Incase Eve has complete access of the information in each attack; the detection probability is higher in Ping-Pong Protocol (1/2) as compared to BB84 Protocol (1/4).
Various researchers [121–124] challenged the security of Ping-Pong protocol by channel loss. Deng et al. [125] identified an attack in the Ping-Pong protocol proposed by [120] in a noise channel. Eavesdropper intercepts the photon and replaces it by a multi-photon signal in the same state for generating the fake signal for one photon. They also proposed an improvement in the Ping-Pong protocol. Lucamarini and Mancini [126] proposed a secure direct communication protocol LM05, which combines the advantages of BB84 and Ping-Pong protocol.
Han et al. [127] proposed a simple and experimental feasible modification to the original Ping-Pong protocol and proved its security in the noisy and lossy channel. In their proposed protocol, Alice prepares n-pairs of maximally entangled state and send half of the qubits to Bob. In message mode, Bob per-

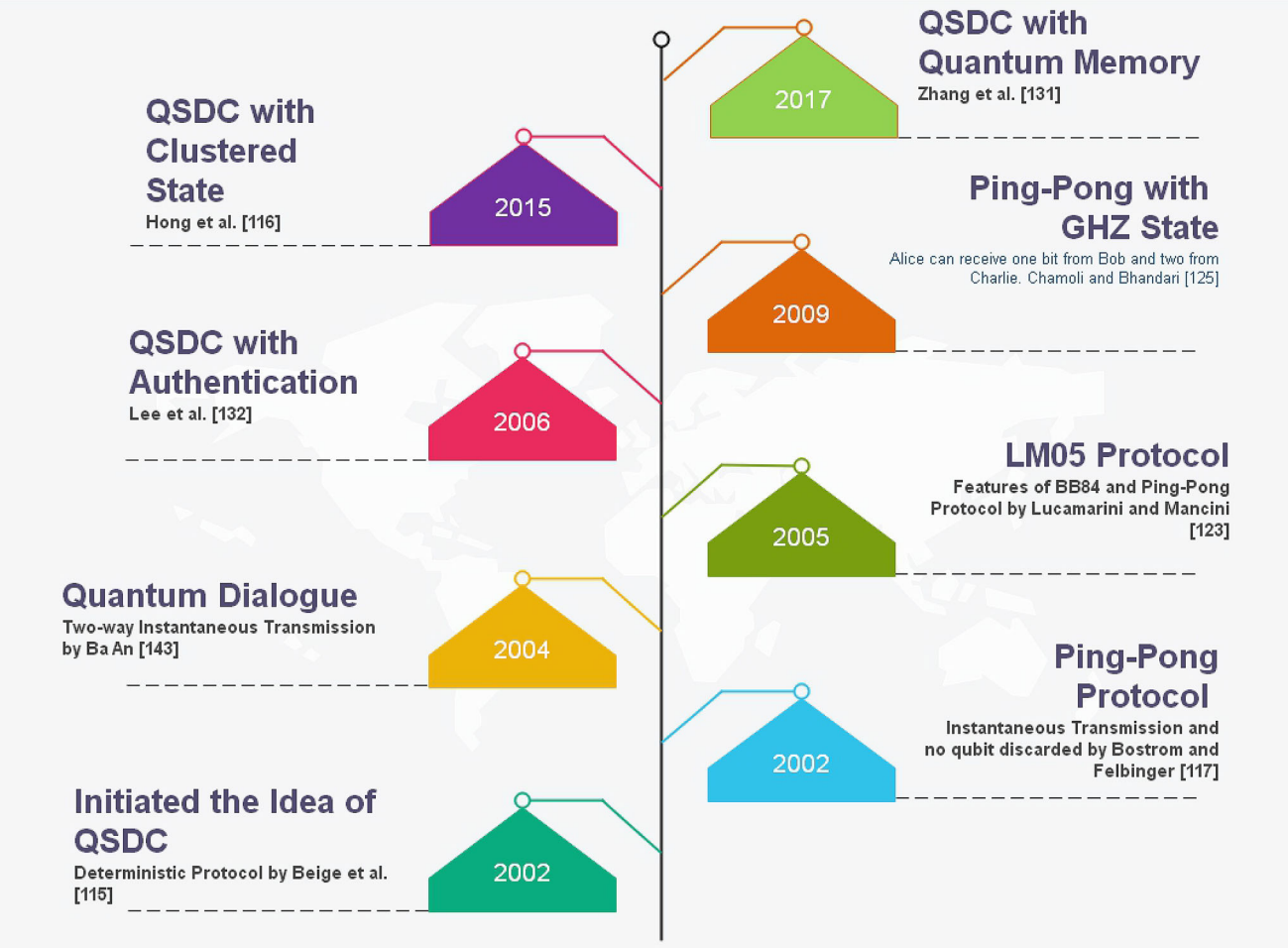


Fig. 7 Significant development in quantum secure direct communication

form one of following four unitary operations (I_0, I_1, Y_0, Y_1) to incoming states [127]:

$$I_0\{|v\rangle, |0\rangle, |1\rangle\} = \{|v\rangle, |0\rangle, |1\rangle\},$$
$$I_1\{|v\rangle, |0\rangle, |1\rangle\} = \{|v\rangle, -|0\rangle, -|1\rangle\},$$
$$Y_0\{|v\rangle, |0\rangle, |1\rangle\} = \{|v\rangle, |0\rangle, -|1\rangle\},$$
$$Y_1\{|v\rangle, |0\rangle, |1\rangle\} = \{|v\rangle, -|0\rangle, |1\rangle\},$$

The existence of vacuum state make (I_0, I_1, Y_0, Y_1) non-unitary. All four operations are having equal probability $(1/4)$. Bob uses I_0, I_1 to encode 0 and Y_0, Y_1 to encode 1 for sending to Alice. The introduction of vacuum states introduces phase randomization in Eve system.

7.2 Ping-Pong Protocol with GHZ state

Chamoli and Bhandari [128] modified the Bostrom and Felbinger [120]'s Ping-pong protocol using three-particle GHZ states and the receiver can simultaneously receive information from the other two parties. Using their protocol Bob and Charlie can communicate to Alice. She receives one bit of information from Bob and two bits of information from Charlie simultaneously through a different quantum channel. Following steps are used in Chamoli and Bhandari's ping-pong protocol [128]:

- Alice prepares initial state of three photons in one of the eight GHZ states.

$$|\Phi_1\rangle = 1/\sqrt{2}(|000\rangle_{ABC} \pm |111\rangle_{ABC})$$
$$|\Phi_2\rangle = 1/\sqrt{2}(|100\rangle_{ABC} \pm |011\rangle_{ABC})$$
$$|\Phi_3\rangle = 1/\sqrt{2}(|010\rangle_{ABC} \pm |101\rangle_{ABC})$$
$$|\Phi_4\rangle = 1/\sqrt{2}(|110\rangle_{ABC} \pm |001\rangle_{ABC})$$

  Lets us consider initial GHZ state with three photons is $|\Phi_5\rangle = 1/\sqrt{2}(|010\rangle_{ABC} + |101\rangle_{ABC})$
- Alice keeps one photon and sends one photon to Bob and another one to Charlie through different quantum

Table 14 Encoded information of Bob and Charlie in Ping-Pong using GHZ state [128]

Communicator name	Encoded information	Operation on qubit
Bob	0	$I = \|0\rangle\langle 0\| + \|1\rangle\langle 1\|$
Bob	1	$i\sigma_y = \|0\rangle\langle 1\| - \|1\rangle\langle 0\|$
Charlie	00	$I = \|0\rangle\langle 0\| + \|1\rangle\langle 1\|$
Charlie	01	$\sigma_x = \|0\rangle\langle 1\| + \|1\rangle\langle 0\|$
Charlie	10	$i\sigma_y = \|0\rangle\langle 1\| - \|1\rangle\langle 0\|$
Charlie	11	$\sigma_z = \|0\rangle\langle 0\| - \|1\rangle\langle 1\|$

channel without declaring the order of photons to Bob and Charlie.

- Bob and Charlie mutually decide whether they will proceed in control or message mode, and inform the same to Alice.
- In control mode (Similar as in the original ping-pong protocol), Bob and Charlie perform measurement in z-basis and inform their results to Alice through a public channel.
  Alice performs a measurement in z-basis, and if she obtains result as expected, it means no eavesdropper is presented.
- Bob and Charlie can encode the information by performing operation, as shown in Table 14. Both Bob and Charlie send their qubit to Alice.
- Alice measures the GHZ state and receives one of the eight GHZ states. By observing the measured GHZ state, Alice can able to determine the Bob and Charlie encoded information deterministically.

The main advantage of Chamoli and Bhandari protocol [128] over Bostrom and Felbinger's Ping-Pong Protocol [120] is that Alice can receive one bit from Bob and two-bit from Charlie.

Naseri [129] analyzed the Chamoli and Bhandari [128] protocol and pointed out that Eavesdropper can find out the secret message by introducing the concept of fake entangled particles. Using fake entangled particle, any dishonest party can able to obtain the secret of others without any risk of detection. Furthermore, he proposed the improvement in the protocol using decoy photon technique [130,131] so that secure communications can be avoided against fake entangled particles. In decoy photon technique, Alice prepares some photons in one of the four non-orthogonal states $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ and insert it into the transmitted sequence to Bob and Charlie. She keeps the record of insertion positions for the detection of the dishonest sender. Li et al. [132] proposed a QSDC protocol based on the hyper-entangled state with improved efficiency for the detection of an eavesdropper. In hyper-entangled state [133], photons are entangled in multiple degrees of freedom.

7.3 QSDC with Quantum Memory

To transmit a message effectively, QSDC needs to be combined with quantum memory. Zhang et al. [134] introduced the concept of quantum memory in Quantum Secure Direct Communication and demonstrated its application in long-distance quantum communication. They used the polarization degree of freedom of photons as an information carrier and obtained 90% fidelity in the entanglement decoding.

7.4 QSDC with Authentication

QSDC provides direct transmission of a message without establishing a key, which leads to higher security. Thus there is a need to certify the user's identity to prevent Eavesdropper. Lee et al. [135] proposed the first QSDC protocol for authentication. Min-Jie and Wei [136] proposed two protocols by combining the idea of user authentication and direct communication with dense coding.

Dan et al. [137] proposed a protocol for realizing identity authentication based on polarized photons and EPR pairs (Four Bell states). They used EPR pairs for transmitting information, whereas polarized photons are used for detecting the Eavesdropper and transmitting the identity authentication information. Security is guaranteed by shared identity number, which is encoded in the form of polarized photons. They proposed the following steps for comparing the identity numbers [137]:

- Alice and Bob have an identity number A_{ID} and B_{ID} respectively.
- Bob prepares a sequence of entangled photons randomly in Bell states. Bob prepare polarized photons in Rectilinear or Circular basis (Similar as in BB84). He further inserts the polarized photons in the sequence of entangled states and transmits the new sequence to Alice.
- Alice receives the sequence, store in quantum memory, measure polarized photons and publishes the measurement bases and result.
- Alice will revise the wrong bases and determine whether Bob is legal or not.

Various researchers [86,138–144] proposed a number of QSDC protocols with authentication. Sarvaghad-Moghaddam [145] proposed an efficient and secure protocol using the concept of entanglement swapping for bidirectional quantum secure direct communication under the controller permission.

7.5 Quantum Dialogue

Ping-Pong Protocol supports only one-way communication. Ba An [146] pointed out denial-of-service or disturbance

attack in the Ping-Pong Protocol. Eve can wait in the Pong-route and see that a qubit is coming from Alice in the message mode. Eve can apply operation and destroy the entanglement or changes the EPR pair randomly. Bob will not receive useful information from Alice, and Eve also remains undetected. To overcome the limitation of a denial-of-service attack, Ba An [146] proposed the concept of quantum dialogue in which Alice and Bob can simultaneously exchange their messages. Bennett and Wiesner [107] proposed that Alice will always pong the qubit to Bob in both control and message mode. In addition, he used the concept of super-dense coding for doubling the quantum channel capacity.

Hong and Yang [147] showed that the quantum dialogue is not secure against intercept and resend attack. Further, Zhong-Xiao et al. [148] proposed the modified quantum dialogue, which is secure against the intercept-and-resend attack.

YuGuang and QiaoYan [149] proposed quasi-secure quantum dialogue protocol using batches of single photons. Alice and Bob obtain classical information from running of single-photon back and forth. Their protocol is free from the concept of entanglement. Tan and Cai [150] pointed out that in quantum dialogue protocols, half of the message between Alice and Bob is leaked through classical public communication. Xia et al. [151] and Yan et al. [152] proposed their quantum dialogue protocols using the GHZ state.

Cao and Jiang [153] proposed a multi-party quantum dialogue protocol by introducing a semi-honest third party. Their protocol usage the concept of multi-particle entangled GHZ state and result in communication among multi-party without leaking any information. Recently Gong et al. [154] proposed a quantum network dialogue protocol for communication among multiple legitimate parties using continuous-variable GHZ state. Using their protocol, the sender can send information to multiple users. The continuous-variable quantum protocol offers a significant improvement in channel capacity.

Chou et al. [155] proposed a dynamic group multi-party quantum key agreement protocol using multicast transmission method. It has the feature to deal with complex situations such as joining and revoking of a member, dividing one group into two and combining two groups into one group.

8 Semi-Quantum Key Distribution Protocol

Secure key distribution is possible when both Alice and Bob are quantum in nature. Semi-quantum Key Distribution (SQKD) protocol operate over a two-way communication channel. In SQKD protocol, one/some of the two users/multi-user are classical in nature. A classical user with no quantum memory can able to measure the qubits only in the computational basis. In contrast, a quantum user can prepare the qubits and measure them in any computational basis (states of the basis must be non-orthogonal). Boyer et al. [156] introduced the concept of SQKD based on entanglement in 2007. In SQKD, Alice and Bob share the secret key as in QKD except Bob is usually classic in nature. They had not proved that their protocol is robust against an eavesdropper. They [157] extended their work and proposed two robust protocol against eavesdropper. Figure 8 depicts the significant development in semi-quantum key distribution protocol.

First, Alice sends a qubit to Bob, then Bob sends back to Alice after measuring and resend or reflect (send back the same qubit to Alice). SQKD protocols also require an authentic classical public channel. The main advantage of SQKD is that it will reduce hardware cost and computational burden. In SQKD, Alice the powerful quantum communicant, can perform the following operations:

- Prepare quantum state (such as single photons and Bell state)
- Bell measurement and multi-qubit joint measurement.
- Storing qubit in quantum memory.

In SQKD, Bob the classical-quantum communicant, can perform the following operations:

- Qubit preparation and measurement in computational Z-basis $|0\rangle$, $|1\rangle$
- Reflect the qubit (Sending back to Alice without distributing the qubit.
- Reorder the qubits via different delay lines.

Krawec [158] designed a single state semi-quantum key distribution protocols which permit reflections to carry information. He considered a restricted attack by Eve and showed the robustness of the protocol. Further, Krawec [159] designed the Mediated semi-quantum key distribution protocol (multi-user quantum key distribution protocol) using Bell basis for allowing two classical or limited semi-quantum users (Alice and Bob) to establish a secret key using the untrusted full quantum server/center. In this quantum server/center will prepare the quantum states and forward it to Alice and Bob. Alice and Bob can only reflect or measure in computational Z-basis and need to rely on the quantum server/center for performing measurement in alternate bases and ensuring the security of quantum channel. He showed that semi-quantum protocol has similar security as full quantum protocol.

Boyer et al. [156] proposed a four states in the quantum protocol. Zou et al. [160] proposed five different SQKD protocols using less than four states and proved their robustness. In two of their protocol, Alice only sends one quantum state. They observed that the protocol with single quantum state have double information bit proportion as compared to Boyer et al. protocol [156].

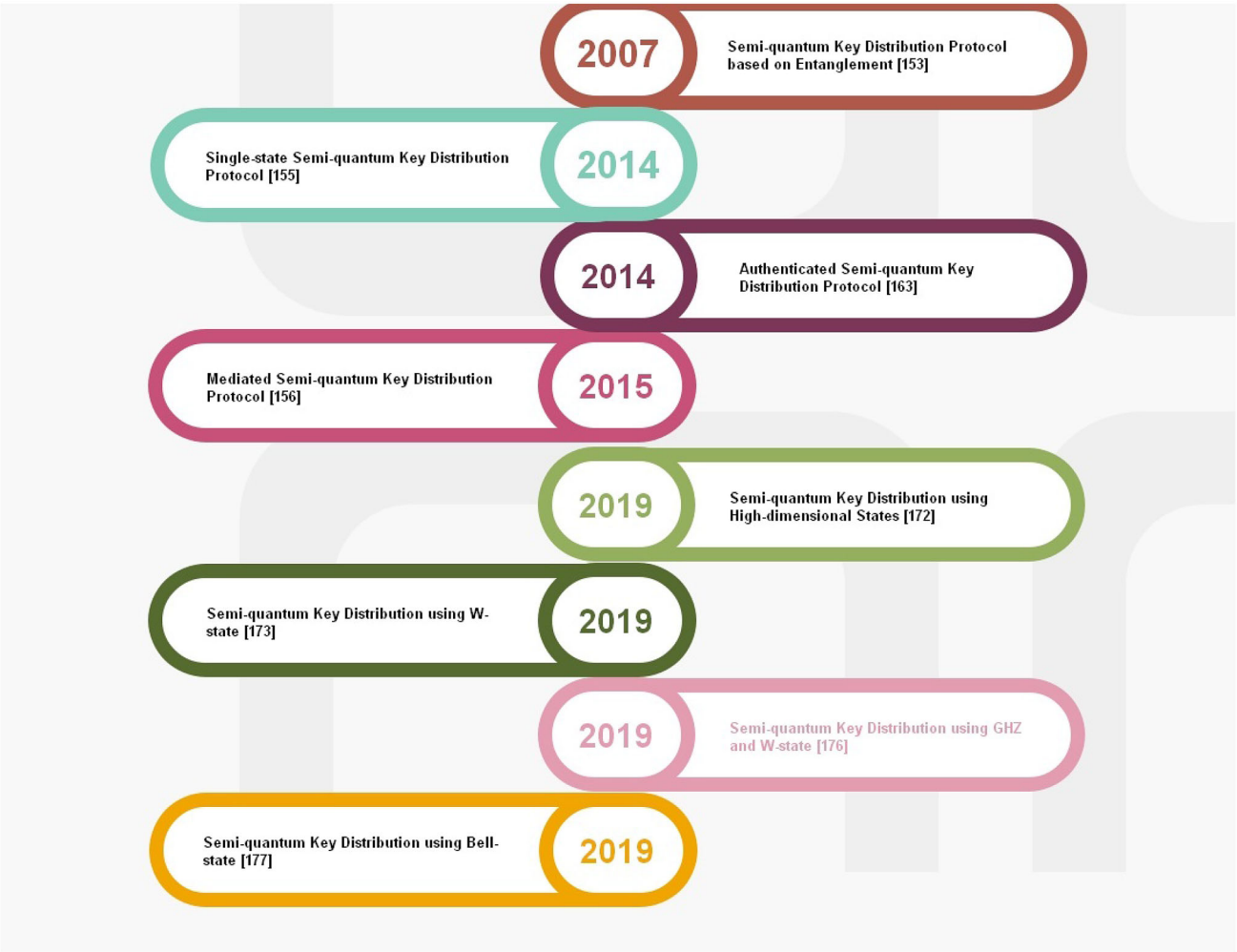


Fig. 8 Significant development in semi-quantum key distribution protocol

Lu and Cai [161] proposed a quantum protocol with classical Alice and Eve is aware about Alice classic nature. They extended and devised a protocol when both Alice and Bob are classical in nature. Zhang et al. [162] proved the unconditional security of the single state semi-quantum key distribution protocol proposed by Zou et al. [160].

Xian-Zhou et al. [163] developed and proved the robustness of a protocol to distribute key bits among one quantum party and m classical parties (No quantum capacity). Their protocol is secure against symmetrically individual attacks, and any attack should be detected with non-zero probability.

Jian et al. [164] proposed an improved and secured protocol using entangled states. Alice prepares two-particle entangled state and measured particle in Bell state. Alice prepare N bell states and choose one particle from each states to form N particle $B_1, B_2, .., B_N$ to Bob. Bob either measure it in a computational basis (Called SIFT) or reflecting the particles (Send the qubit back to Alice without disturbing it or reordering of particles). Their proposed protocol can be modified to measure-resend protocol. Li et al. [165] proposed a semi-quantum secret sharing protocol by utilizing the concept of product states ($|+\rangle|+\rangle$). Alice prepares the product state and sends one qubit to classical Bob and other to classical Charlie. They tested the protocol by introducing some errors which will further be noticed by the legitimate users.

Yu et al. [166] designed the first SQKD protocol free from all attack and without using authentic classical channels known as Authenticated semi-quantum key distribution (ASQKD). Alice and Bob require pre-sharing of the master secret key, which can be generated by using QKD or SQKD protocol. After generating the master secret key, many session keys can be generated using ASQKD protocol. They proposed randomization based ASQKD and measure-resend ASQKD protocols. Luo and Hwang [167] proposed two authenticated semi-quantum direct communication protocols based on randomization and measure-resend. Sender (Say Alice) equipped with quantum devices transmit a message to the classical receiver. They analyzed that their protocols

are robust against Trojan horse attack, intercept and resend attack, modification and impersonation attacks. Zou et al. [168] proposed a semi-quantum protocol without involving the classical Alice's measurement capability. Their proposed protocol requires less number of quantum states sent by both parties and it is secure against joint attacks.

Chou et al. [169] proposed a semi-quantum private comparison protocol with the presence of a dishonest third party. Lu et al. [170] proposed a no-key semi-quantum direct communication protocol using only constant entanglement preservation time and a fixed number of quantum bit registers.

Boyer et al. [171] in 2017 proposed a semi-quantum key distribution using classical Alice, with a controllable mirror and four-level available systems. In Quantum Private Comparison's, two users can compare equality of their private secrets using a third semi-honest third party. Thapliyal et al. [172] proposed two semi-quantum protocol for quantum private compassion's using orthogonal states and evaluated the performance under noisy environment.

Krawec [173,174] proved the unconditional security of Boyer et al. [156] semi-quantum protocol. Iqbal and Krawec [175] designed a semi-quantum key distribution protocol using high-dimensional quantum states and carried out the security analysis for the same. Recently, Tsai et al. [176] proposed a semi-quantum secret sharing protocol using W-state for three parties and found that the protocol is free from the well-known attacks. Iqbal and Krawec [177] carried a survey of various semi-quantum key protocol and pointed out several open problems. Lin et al. [178] proposed a semi-quantum protocol to share a secret key between two classical users with the help of third untrusted party. The untrusted third party will require single-photon and Bell measurement capability. Wen et al. [179] proposed a semi-quantum authentic protocol based on the correlation between GHZ and W state for determining the identities of two participants. They pointed out that the proposed protocol is more secure and effective than traditional quantum authentication protocols. Tao et al. [180] proposed two-semi direct communication protocols based on Bell states and two pre-shared secret keys. To overcome the problem of double CNOT attack and information leakage problem in the Sun et al. protocol [181], Yang [182] proposed an efficient and secure semi-quantum protocol. Zhou et al. [183] presented two semi-quantum identification protocols using a single photon. In their proposed protocols, quantum Alice and classical Bob can identify each other to resist against a man-in-the-middle attack. Yan et al. [184] proposed a semi-quantum protocol to transmit a secret message between classical Bob and quantum Alice using Bell states.

In addition to the above mentioned protocol, semi-quantum key distribution protocol has attracted the attention by various researchers and carried out work in [185–214].

9 Secure Multiparty Communication (SMPC)

Secure Multiparty Communication (SMPC) is also known as Secure function computation. It was introduced originally by Yao [215] in the form of Millionaire problem for secure multiparty computation. Millionaire problem is a comparison problem in which two millionaires want to discover which one is richest without revealing the precise amount of their personal fortune. SMPC has several applications in the field of online bidding, secure voting and market clearing price scenario. In general, SMPC refers to n parties, and they compute a publicly available function using a set of private variables without revealing their personal fortune. Figure 9 depicts the significant development of Secure Multiparty Communication.

Zhang et al. [216] proposed a quantum protocol using Bell states for comparing the values of two distrustful parties with the help of the third semi-dishonest party. Mayers [217], and Lo and Chau [218] independently pointed out in 1997 that the previously developed multiparty communication is insecure due to unreliable quantum bit commitment scheme.

Dong et al. [219] proposed a generalized multi-party deterministic quantum protocol using entanglement swapping. Shi and Zhong [220] proposed two protocols for quantum multiparty communication using entanglement swapping and EPR pairs. Liu et al. [221] found that multiparty protocol proposed by Shi and Zhong [220] is not secure as a dishonest participant can able to determine the secret key independently by illegal means. Further, Liu et al. [221] proposed a secure multiparty quantum protocol which is secure against participant attacks as well as an outside attack using a single particle. Sun et al. [222] improved the Liu et al. [221] protocol efficiency from $\frac{1}{(k+1)(N)(N-1)}$ to $\frac{1}{(k+1)(N)}$ using two additional unitary operations, where N denotes the number of parties. Xun-Ru et al. [223] proposed a three-party QKD based on EPR pairs. Yin et al. [224] proposed a three-party QKD protocol using two-qubit entangled state and each party equally contribute to the establishment of a shared secret key. Zhu et al. [225] found that Yin et al. [224] protocol is not secure if two dishonest parties offset the role of the third party in the generation of the shared secret key by launching a special kind of attack. They also proposed an improved protocol to overcome the participant attack.

Shukla et al. [226] proposed two protocols (Two-party and multi-party) using multi-partite entangled states and found that such quantum systems are useful in the implementation of quantum dialogue. Zhu et al. [227] showed that the Shukla et al. [226] protocol is not secure, and any participant can directly obtain the secret key of the other two participants. They found that in Shukla et al. [226] protocol, an eavesdropper can flip any bit in the final secret key without introducing any error. Finally, they proposed a protocol to overcome the limitation of Shukla et al. protocol [226].

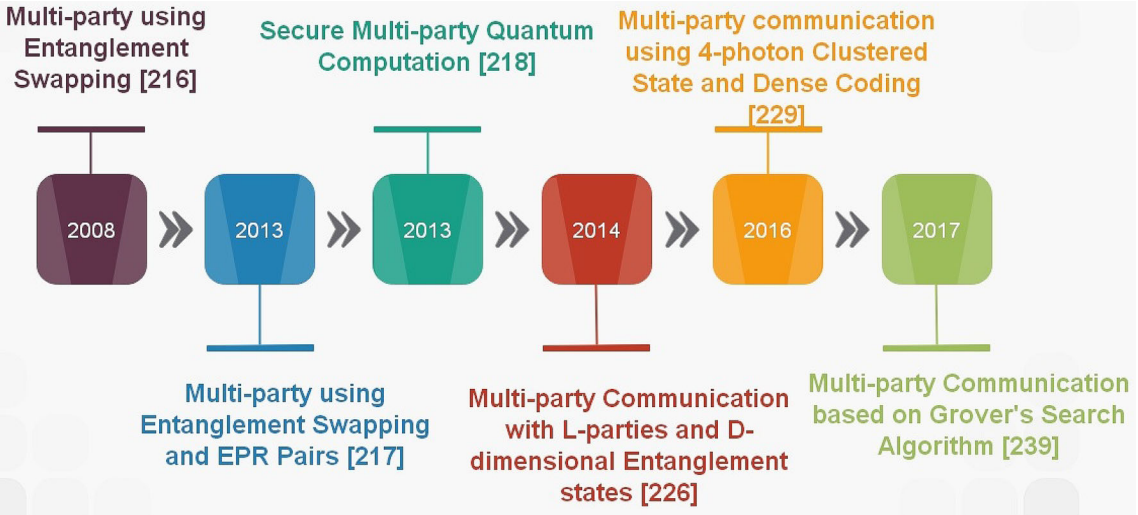


Fig. 9 Significant development in secure multiparty communication

Further, Gu and Hwang [228] found that Zhu et al. protocol [227] suffers from Collusive attack (Any two dishonest parties collaborate and perform manipulation in the final secret key without getting detected). Luo et al. [229] proposed a quantum private comparisons protocol using $l-$parties and $d-$dimensional entangled state.

Huang et al. [230] pointed out that Sun et al. [222] protocol cannot achieve privacy and fairness. They also proposed a fair and secured protocol for secret key amongst n-parties with a high qubit efficiency. Smania et al. [231] performed experimental realisation of a three-party quantum protocol using qutrit communication using a three-level system includes Secret Sharing, Detectable Byzantine agreement and communication complexity reduction.

Sun et al. [232] proposed a multi-party quantum key protocol by utilizing the four-photon cluster state, block transmission technique, dense coding method and decoy-state. Sun et al. [233] proposed fairness (No one alone cannot be able to determine the key) multiparty quantum key protocol using maximally entangled six-qubit states. Sun et al. [234] proposed a single qubit state protocol for multiparty quantum key agreement by performing an exclusive-OR operation on all the parties without the explicit need of entanglement states, joint measurement and unitary operations. Li et al. [235] found that circle-type multi-party quantum key agreement protocols are not fair, and any two dishonest parties at a special position can able to determine the shared secret key. In multiparty quantum key agreement travelling and distributed mode is used to transmit the quantum information. Huang [236] proposed two protocols for travelling mode using EPR pairs and single photons. Huang et al. [237] proposed an efficient, fair and secure multiparty quantum key agreement protocol using single photons in travelling mode.

Liu et al. [238] proposed a multiparty protocol by taking Bell state as a quantum resource and considering the client-server model. Participants will able to access quantum channel and prepare single photons, whereas the delegate computation such as Bell measurement and unitary operations will be performed at remote quantum centers. Wang et al. [239] proposed a general circle-type multi-party key agreement, which is secure against $t < N$ dishonest parties cooperation.

Zhou et al. [240] proposed a semi-quantum protocol based on four-particle cluster states. Using Zhou et al. 's protocol, the key can be distributed among one quantum and two classical parties. Further, they pointed out that the concepts can be extended for more than 3-user for communication. Sun et al. [241] proposed a fair multi-party protocol that resists against Liu's et al. [235] collusion attack. Participants prepare the initial states only and server to prepare the quantum states. The main advantage of this protocol is that any eavesdropper including server is not able to find the final shared secret key. Cao and Ma [242] proposed the first multiparty quantum key agreement based on Grover's search algorithm. They showed that their protocol work on a five-party system and further compared the proposed protocols with the existing protocols. A travelling mode in multiparty quantum key agreement protocol achieves higher efficiency than the distributed mode. Cao et al. [243] proposed a multi-party quantum key agreement protocol for travelling mode based on non-orthogonal quantum pairs, Bell states and their dualities by mixed dense encoding.

Sun et al. [244] proposed an efficient multiparty quantum key agreement protocol using sequential communication of a single d-level quantum system. Each participant only performs a unitary operator and measurement complexity is independent on the number of participants. The main advantage of Sun et al. protocol is that the efficiency rate is $\frac{1}{2N}$. Huang

et al. [245] investigated existing multi-party quantum key agreement in a travelling mode. They found that dishonest participants with favourable geographical location collaborating with other participants can able to determine the secret key. Further, they proposed a multi-party quantum key agreement in travelling mode using non-orthogonal Bell states. He et al. [246] proposed a high-efficiency three-party quantum key agreement protocol by utilizing two-photon polarization entangled Bell states and a few single-photon polarization states. They used quantum dense coding to improve the efficiency and each participant need to perform one unitary operation to encode the sub-secret key. Jo et al. [247] carried out a security analysis which provides an asymptotic secret key rate for multiparty quantum key distribution under the restriction that the successive trials are independent. Mohajer and Eslami [248] pointed out that the participant attack on Sun et al. protocol [234] and proposed an improvement to avoid the participant attack.

10 Device Independent Cryptography

Actual device used in quantum key distribution suffer from unavoidable imperfections and behave differently than the theoretical assumptions. Zhao et al. [50] experimentally demonstrated time-shift attack (first quantum hacking attack) against a commercially available QKD system. Lydersen et al. [249] introduced the concept of detector blinding attack to acquire the whole secret key. QKD system suffers from the loophole that allows the side-channel attack. Full-device independent QKD was proposed to avoid the side-channel attack. Figure 10 depicts the significant development in Device Independent Cryptography.

In full device-independent cryptography, Alice and Bob can buy a device from anyone (reliable or unreliable one). It means the security does not rely on the truthfulness of the quantum apparatus. In full-device Independent Quantum Key Distribution (DIQKD), quantum apparatuses are considered as a black box, which takes classical input and produces classical output. Entanglement based devices are more difficult to implement over long distances. Security of quantum key distribution protocol lies with the credibility of the quantum devices. In device-independent cryptography, there is no guarantee that the quantum device performs as per the specifications.

Bell inequality test is performed to ensure that the devices are adequately entangled and ensure the testing of quantumness [82,250–252]. Bell inequality can be considered as the Clauser–Horne–Shimony–Holt (CHSH) game [253] played between honest parties (Alice and Bob) using their shared device.

In CHSH game, Honest Alice (input x and output y) and Honest Bob (input y and output b) such that $x, y \in 0, 1$.

Wining condition of game $a \oplus b = x.y$

Classical Case Optimal wining probability 75%

Quantum Case for Maximally Entangled State Winning Probability 86%.

Bell [83] experimented and showed that there exist no hidden variable in nature. The Locality loophole refers that particles and detectors are communicating during the Bell test. Researchers are carrying out the work to close the loopholes one by one for excluding Einstein's Hidden variable. Mayers and Yao [250] introduced the concept of self-testing quantum source by considering the non-local correlations.

Colbeck [254] applied the Bell test to check the honesty of quantum apparatus. Pironio et al. [255] provided the security proof of Acin et al. [256] device-independent quantum key distribution protocol. Hensen et al. [84] carried out an experiment Loophole-free Bell test using electron spins in artificial diamond at Delft University of Technology, Netherland. They separated the electron and detector 1.3 Km apart so that they can not be able to communicate. They performed 245 trials to test CHSH-Bell inequality [253] and found that Einstein's hidden variables are wrong. Lucamarini et al. [257] designed a device-independent entanglement based B92 protocol.

Full Device-independent quantum key distribution shows that security of the cryptographic protocol is based on the assumption of trusted random number generator, Authenticated classical public channel, the correctness of quantum physics and Both parties (Alice and Bob) physical locations are secure. The major limitation of full-device independent QKD is that it requires a loophole-free Bell test with distant parties, which is practically impossible with currently available technologies.

One-Sided Device-Independent QKD: In standard QKD, Alice and Bob both trusts their measurement apparatus. Branciard et al. [258] introduced the concept of one-sided device-independent QKD, a less restricted device-independent QKD, where one of the party trust his/her measurement apparatus. Cao et al. [243] proposed one-sided measurement-device-independent QKD to overcome the limitations of measurement-device-independent QKD and to enjoy the detection of loophole-free. They considered Bob encoding system is trusted and carried out an experiment using a coherent light source. Tomamichel et al. [259] showed that the standard BB84 QKD scheme is one-sided device-independent QKD by considering Bob's quantum apparatus as malicious, and Alice apparatus is a trusted one. Walk et al. [260] carried out an experimental demonstration of Gaussian protocol for one-sided device-independent QKD.

Measurement Device-Independent Quantum Cryptography: Measurement device-independent QKD is one of the feasible solutions with currently available technology to quantum hacking and bridging the gap between theoretical and practical implementation of QKD. Lo et al. [261] introduced

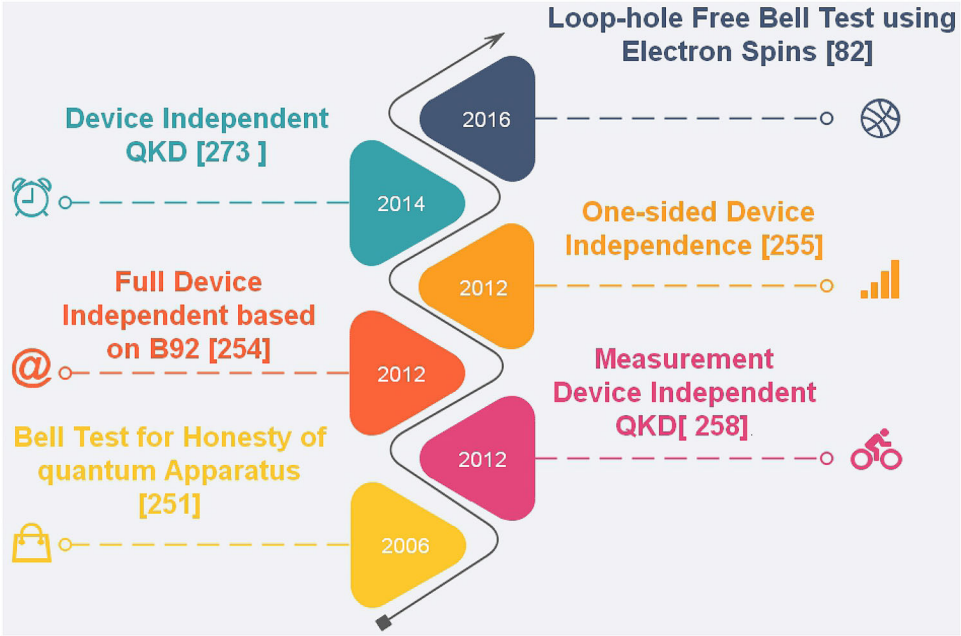


Fig. 10 Significant development in device independent cryptography

the concept of measurement device-independent QKD for removing all detector side channels attacks. In their approach, Alice and Bob prepare phase randomized weak coherent pulse in different BB84 polarization state. These polarization states are selected randomly and independently for each signal. Further, they showed that the system remains secure over 200 KMs in the existence of seriously flawed detectors. Measurement device-independent QKD [262] provide high key rate and long-distance with the currently available technologies.

Tang et al. [263] performed the first experimental realization of measurement device-independent QKD by considering the state preparation flaws and distributed secure keys up to 40 KM. Experimental realization of measurement device-independent QKD has been carried out by various researchers (For details, the reader can see [221,264–267]). Qiao et al. [268] proposed a scheme for monitoring light source using single-photon detectors for measurement-device-independent QKD. This new scheme significantly improves the secure key rate and transmission distance. Cui et al. [269] proposed a high-dimensional measurement device QKD protocol with qudits hyper-encoding in spatial mode and polarization degrees of freedom. They demonstrated that their scheme is unconditional secure for weak coherent pulses with decoy states. Dellantonio et al. [270] also proposed a high-dimensional measurement-device-independent QKD protocol and carried out an analysis for phase error and imperfect sources.

Measurement-device independent QKD requires an interface of two photons from two different light source, which makes the experiment more demanding. Secure key rates achieved in measurement-device independent QKD is lower than prepare and measure the QKD system.

Semi-Device Independence Fully device-independent QKD is based on non-locality and applicable only for entanglement based protocols. Semi-device-independent QKD provides secure key distribution for one way prepare and measure protocols [271]. The measurement apparatus's dimension is of fixed Hilbert space. Yang et al. [272] demonstrated the security of semi-device-independent QKD against collective attacks. Dall'Arno et al. [273] discussed security concerns in semi-device-independent QKD and suggested ways to prevent the malicious attack. Chaturvedi et al. [274] studied the security of semi-device-independent QKD protocol under the random access code, cryptography primitive.

Woodhead et al. [275] proposed a semi-device-independent QKD based on modified BB84 protocol and Bob carried-out CHSH-type estimation on the qubit send by Alice.

Detector Device-Independent Quantum Cryptography: To overcome the limitations of measurement-device independent QKD (Security key rate and Interface of two photons), Lim et al. [276] and Gonzalez [277] proposed the concept of detector device-independent quantum cryptography the combine the security of measurement-device independent quantum cryptography with the efficiency of conventional QKD. The main advantage of detector-based-independent QKD is that two-qubit single photon is used instead of an interface between two widely separated independent single-photon source.

Wei et al. [278] proposed detector blinding attack with intrinsic attack and Eve can obtain the security key without getting detected. They also explicitly discussed the attack

Table 15 Few examples of symmetric and asymmetric cryptosystem with quantum attacks [287]

Type of cryptosystem	Algorithm name	Attack
Symmetric	AES128	Grover's algorithm
Symmetric	AES256	Grover's algorithm
Symmetric	Salsa20	Grover's algorithm
Asymmetric	RSA2048	Shor's algorithm
Asymmetric	RSA3072	Shor's algorithm
Asymmetric	ECC521	Shor's algorithm

proposed by Qi and Siopsis [279], which combines the blinding attack and detector wavelength dependency of a beam splitter. Sajeed et al. [280] demonstrated that detector-device-independent QKD is not secure against side-channel attacks.

11 Post Quantum Cryptography

Security of existing classical cryptosystems relies on the Integer factorization problem, discrete logarithm problem or elliptic-curve discrete logarithm problem. Shor algorithm can able to solve all these three problems using a quantum computer. Grover algorithm [3] showed that the Security of the symmetric encryption algorithm is at risk. Table 15 represents a few symmetric and asymmetric cryptosystem with quantum attacks.

Once a scalable quantum computer is developed, the existing classical security algorithms such as Diffie–Hellman key-exchange [281], RSA public key encryption [282], Algebraically Homomorphic [283], Elliptic curve cryptography [284] and Buchmann–Williams key-exchange [285] will become insecure. There is a growing interest in post-quantum algorithm to make the system secure. Post-quantum algorithms deal with cryptosystem that runs on a conventional computer but secure against attacks by quantum computer [286]. Bernstein and Lange [287] listed various existing cryptographic system and the quantum attacks against the cryptographic system.

Post-quantum cryptography schemes are classified into code-based cryptography, Lattice-based Cryptography, Hash-based Cryptography, Multivariate-quadratic equations cryptography. Table 16 represents a few public cryptosystems with their examples.

Table 16 Public cryptosystems and their examples

Scheme name	Classical example
Code-based cryptography	McEliece's Hidden Goppa-code 1978 [288]
Lattice-based cryptography	NTRU public cryptosystem [290]
Hash-based cryptography	Lamport-Diffie one-time signature scheme [296]
	Winternitz one-time signature scheme [297]
Multivariate-quadratic equations cryptography	Patarin's and vinegar signature scheme [300]

- Code-Based Cryptography: McEliece [288] introduced the concept of code-based cryptography in 1978. Code-based cryptosystem uses error-correcting code. There is a trade-off between efficiency and security in the code-based cryptosystem. By reducing key size, efficiency can be improved but at the cost of security. By increasing the key size, security can be improved but at the cost of efficiency [289]. The main issue of a code-based cryptosystem is the key size (megabyte) for higher security. Although Researchers had proposed few code-based cryptography schemes; attacks have been proposed corresponding to these schemes. Still, the initially proposed scheme by McEliece remain unbreakable, but it suffers from a key size. In future, there is a possibility of new code-based cryptography approach to be proposed that remain secure with the quantum attack.
- Lattice-Based Cryptography: Hoffstein et al. [290] introduced NTRU public cryptosystem with a smaller key size than McEliece cryptosystem. Several quantum attacks have been proposed by exploiting the polynomial structure [291,292] and without exploiting the polynomial structure [293–295]. To gain confidence against quantum attack, more research is needed to be carried out on lattice-based cryptography.
- Hash-Based Cryptography: Hash-based cryptography relies on the hash function and requires minimal security requirements. Lamport-Diffie one-time signature scheme [296] and Winternitz one-time signature scheme [297] are hash-based cryptography schemes. Dods et al. [298] and Hulsing [299] proposed the improved hash-based cryptography schemes using better one-time signatures to decrease the signature size.
- Multivariate-Quadratic Equations Cryptography: It is based on the computational difficulty involved to solve non-linear equations over finite fields. This cryptography scheme is also known as trapdoor multivariate quadratic as it involves higher-order quadratic polynomial equation. Patarin's and vinegar signature scheme [300], Ding and Schmidt's Rainbow signature scheme [301] and Patarin's et al. Quartz signature scheme [302] are few well known multivariate public-key cryptography schemes.

National Institute of Standards and Technology (NIST) has initiated the process to evaluate and standardize the quantum-

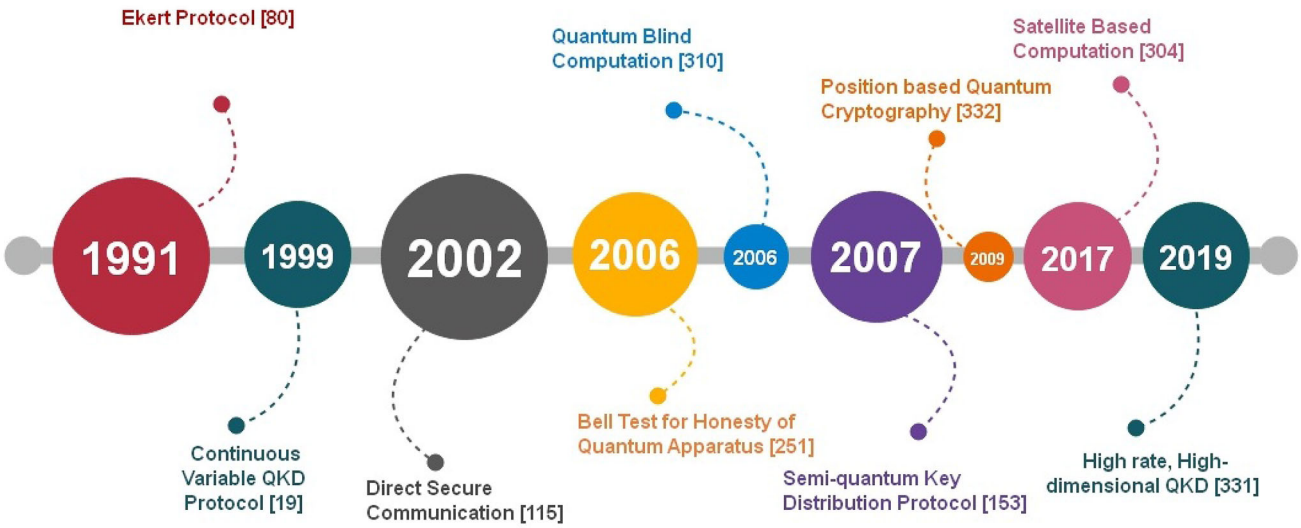


Fig. 11 Significant development in quantum cryptography after BB84 protocol

resistant algorithms for post-quantum cryptography. NIST had shortlisted 26 quantum algorithms (17 Public key encryption and key-establishment algorithms and 9 for digital signatures) for the post-quantum algorithms. Researchers are considering these 26 algorithms as the strongest candidate for post-quantum algorithms [303]. There is an upward trend of research in the area of post-quantum computing. Reader can go through [286,287,304] for a detailed study on post-quantum cryptography.

12 Latest Trends and Concluding Remarks

Latif et al. [305] proposed a framework for secure communication in the cloud and internet of things environment. They also proposed a quantum steganography protocol using a hash function and entanglement states. Amer et al. [306] proposed a semi-quantum key distribution protocol for tolerating high-level of noise by considering the advantage of a two-way quantum channel. Figure 11 represents the significant development in quantum cryptography after the design of the BB84 Protocol. Figure 12 represents the major experimental work carried out in the area of quantum cryptography. Table 17 depicts a summary of various attacks on the quantum protocol.

To overcome the limited distance communication over fiber cables, free space-based QKD give rise to the concept of satellite-based communication for sharing secret information. Yin et al. [312] explored the satellite-based communication between two entangled photons separated by 1203 KM on earth. Liao et al. [313] reported the development and launch of a low-earth satellite for achieving the kilohertz key rate for a distance up to 1200 KM by implementing decoy-state QKD. Further, Liao et al. [314] performed decoy-state quantum key distribution between multiple locations on the ground (Xinglong, Nanshan and Graz) and low-earth orbit satellite. They communicated the secret message over 7600 KM between locations in Europe and China. Sharma and Banerjee [315] carried out the analysis of the atmospheric effect on satellite-based communication against Photon number splitting and intercept resend with unambiguous discrimination attacks. In 2017, Bedington et al. [316] summarized the research on QKD with satellite. Chunli Bai (President of Chinese Academy of Science) and Anton Zeilinger (President of Austrian Academy of Sciences) successfully conducted the first Inter-Continental video conference call using Chinese quantum satellite Micius [317]. Quantum key is transmitted using the satellite Micius. Chinese Academy of Science and Jian-Wei Pan research group from University of Science and Technology, China collaboratively working on quantum communication between low earth orbit satellite and receiving stations on earth to achieve secure communications between optical ground stations in China and Europe. Many Indo-Pacific nations also joined the race for Quantum satellite. The National University of Singapore developed a nano-satellite carrying quantum node, which was launched by Indian vehicle in 2015. National Institute of information and Communications technology, Japan also demonstrated quantum communication using a micro-satellite in 2017. Quantum cryptography can be applied in substantial numbers of applications. Table 18 represents a few real-life applications of quantum cryptography.

12.1 Quantum Blind Computation

It is likely possible that the quantum computer after its development will be available in centers across the world. Blind

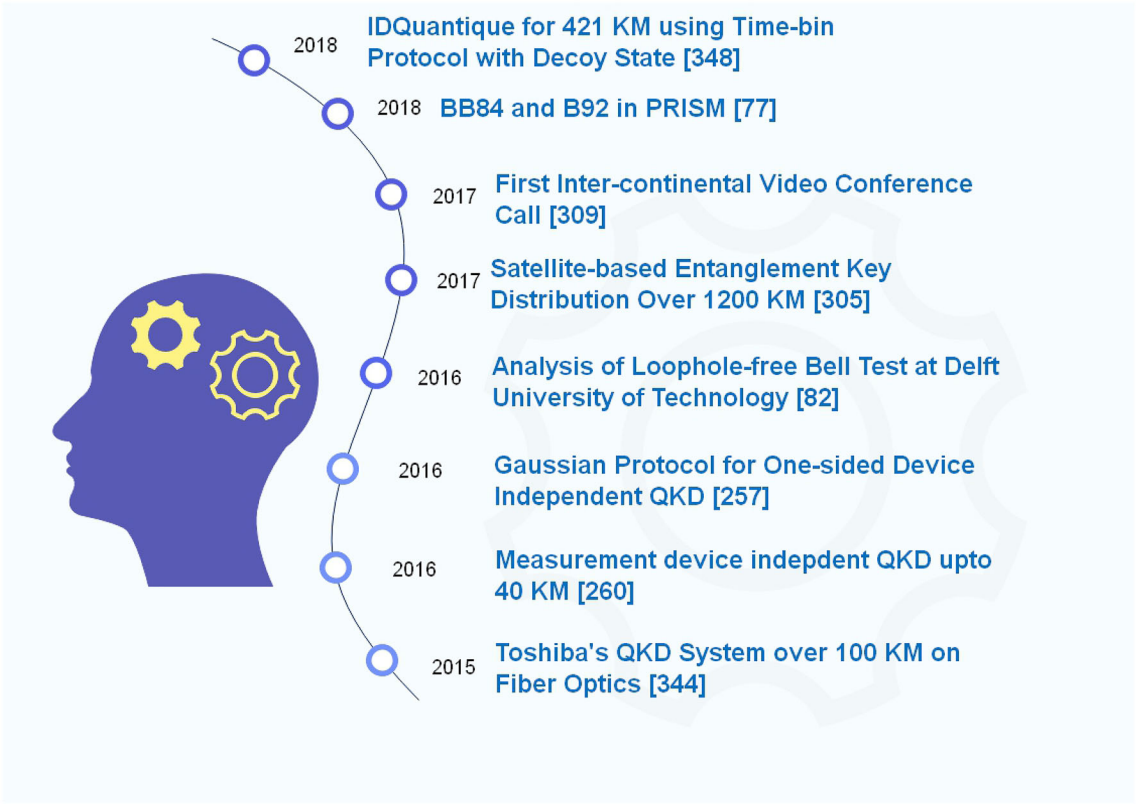


Fig. 12 Major experimental work in the area of quantum cryptography

Table 17 Summary of various attack on quantum protocol

Attack name	References	Year(s)
Beam splitter attack	[67]	2014
Detector blinding attack	[249,278]	2010, 2017
Double blinding attack	[73]	2012
Double CNOT attack	[180]	2019
Einstein–Podolsky–Rosen Attack	[218]	1997
Faked state	[33]	2005
Frequency shift attack	[70]	2014
Gaussian attacks	[30]	2019
Intercept/resend attack	[65,147]	2009, 2006
Large pulse attack	[39]	2001
Laser seeding	[47]	2015
Man-in-middle attack	[41,43,44,66]	2006, 2014, 2018, 2009
Optimal attack	[42]	2010
Phase remapping attack	[48,49]	2007, 2010
PNS attack	[35–37]	1995, 2000, 2011
Polarization shift	[51]	2019
Symmetric collective attack	[34]	2008
Time-shift attack	[46,50]	2007, 2008
Timing-side channel attack	[45]	2007
Trojan horse attack	[41,43,44]	2006, 2014, 2018

Table 18 Applications of quantum cryptography

Application	Country/collaborating institutes	Year
Secure online voting	Switzerland	Since 2007
FIFA World Cup secure link between Moses Mabhida Stadium and main hub	South Africa	2010
POS system for transmitting quantum keys [307]	Nokia, Bay Photonics, Oxford University	2017
QkarD quantum smart card [308,309]	Los Alamos National Security	2010
Data protection of 6000 banks and 6000 hospitals [310]	United states	
Quantum encrypted video call [307]	Chinese Academy of Sciences	2017
	Austrian Academy of Sciences in Vienna	
Quantum voting [311]	Southeast University, Nanjing, China	2017
	East China Normal University, Shanghai, China	

Table 19 Major sources titles with papers > 3 used in the review process

Journal name	Number of paper used	Publisher name
Physical Review A	45	American Physical Society
Physical Review Letters	37	American Physical Society
Quantum Information Processing	33	Springer
International Journal of Theoretical Physics	17	Springer
Scientific Reports	15	Nature Publishing Group
New Journal of Physics	9	IOP Publishing
International Journal of Quantum Information	7	World Scientific
Optics Express	6	OSA, The Optical Society
NPJ Quantum Information	5	Nature Publishing Group
Nature	5	Nature Publishing Group
Chinese Physics Letters	5	Chinese Physical Society
Theoretical Computer Science	4	Elsevier
Physics Letters A	4	Elsevier
Journal of Modern Optics	4	Taylor and Francis
Modern Physics Letters A	4	World Scientific
SIAM Journal of Computing	3	Society for Industrial and Applied Mathematics
International Journal of Quantum Information	3	World Scientific
Chinese Physics B	3	IOP Publishing
IEEE Access	3	IEEE
Nature Photonics	3	Nature Publishing Group

quantum computation is emerged for performing secure computation rather than secure communication. Consider Alice (does not have a quantum computer) and Bob have a quantum computer. Alice wants to utilize Bob quantum resources without revealing about the computation. In Blind quantum computation, Bob will remain unaware of the usage of his quantum computer by Alice. Alice will perform her computation on Bob quantum computer, and Bob will not be aware of her input, output and computation. Arrighi and Salvail [318] introduced the concept of quantum blind computation and proposed a protocol for carrying out the blind quantum computation.

Broadbent et al. [319] proposed a protocol for blind quantum computation. In their protocol, Alice, a purely classical client, communicate with two non-communicating entangled servers for performing the computation. Fitzsimons [320]

reviewed the blind quantum computation. Li et al. [86] proposed two protocols for blind quantum computation with identity authentication. Barz et al. [321], Greganti et al. [322] and Huang et al. [323] experimentally demonstrated the concept of blind quantum computing.

12.2 Quantum Digital Signature

With the significant development in the area of a quantum network, Quantum digital signature and Quantum Key distribution are needed for signing and information distribution in the quantum network. Gottesman and Chuang [324] introduced the concept of quantum digital signature in 2001. Quantum digital Signature is an approach used to sign a document by quantum means and transfer to the user with information-theoretically study [325,326]. Roberts et al. [266] carried out an experimental demonstration of quantum digital signature by realising quantum network architecture mediated by measurement-device-independent quantum key distribution. Cai et al. [327] carried out cryptanalysis on multiparty digital signatures. Shi et al. [328] carried out an analysis of quantum signature scheme based on asymmetric quantum cryptography against forgery attack and suggested the addition of random integer shared between the signer and verifier. Collins et al. [329] reviewed the development in experimental quantum digital signatures. Collins et al. [330], Donaldson et al. [331] carried out experimental demonstration of quantum digital signature.

12.3 High-Dimensional Quantum Key Distribution

Encoding by the polarization of light in quantum key distribution limits the information to be sent per photon. It puts tight bounds on the error rates the system can tolerate. High-dimensional Quantum Key Distribution is an efficient and robust way to encode information with higher key rate. High-dimensional QKD systems are more resistant to noise in the channel and overcome the limitation of QKD by encoding more bits per transmitted photon.

In high-dimensional QKD protocol, information can be encoded using spatial modes [332–334], time-phased [335–337]. Ding et al. [334] proposed a high-dimensional QKD protocol based on space-division multiplexing in multi-core fiber using silicon photonic integrated lightwave circuits. Jo et al. [247] proposed an efficient high-dimensional QKD protocol using hybrid encoding by two-degree-of freedom of a single photon, multi-path modes and orbital angular momentum modes. Islam et al. [338,339] proposed and demonstrated a high-dimensional quantum key distribution using two-photon interference technique.

12.4 Position-Based Quantum Cryptography

Chandran et al. [340] devised the concept of classical position-based cryptography. Further, Chandran et al. [341] introduced the concept of position-based quantum cryptography by considering the geographical position of a party as the credential. Using position-based quantum cryptography, two military bases can be communicated without pre-shared keys over an insecure channel. Bilski and Winiecki [342] analyzed the position-based quantum cryptography in a distributed system. Qi and Siopsis [279] studied the performance of position-based quantum cryptography protocols over a noisy channel by assuming that no entanglement is pre-shared between adversaries. Buhrman et al. [343] studied quantum setting in position-based quantum cryptography. Chakraborty and Leverrier [344] proposed interleaved product protocol for position verification.

12.5 Chip-Based QKD Devices

The main limitation of the existing QKD equipment is cost, space and power consumption. To miniaturise and mass-produce of QKD system, Sibson et al. [345] introduced the concept of chip-based quantum communications. IMEC (World-leading research and Innovation hub in Nanoelectronics) and National University of Singapore (NUS) joined their hands to develop robust, scalable and efficient technologies for QKD and quantum random number generation. Roger et al. [346] demonstrated on-chip quantum random generator using laser pulses. Zhang et al. [347] designed a 3 mm silicon photonic chip operating at 1550 nm for continuous-variable QKD system by integrating the all-optical component except for laser source.

12.6 Quantum Bit Commitment

Bit commitment involves Alice and Bob, two mistrustful parties. In Bit commit protocol, Bob is interested that Alice will bind to her commitment and Alice conceal the commitment. Alice commits an encoded bit of information to Bob. Alice cannot be able to change the information after submit, and Bob cannot identify the information until Alice decodes it.

In 1997, Lo and Chau [218] showed that Alice could cheat using the Einstein-Podolsky-Rosen (EPR) attack successfully, causing Quantum Bit commitment to insecure.

12.7 Quantum Coin Flipping Protocol

Blum [348] introduced the concept of coin tossing. Coin tossing can be classified as weak or strong. The strong coin-tossing protocol is used if the preference of other party is unknown. In the weak coin-tossing protocol, the preference of other party is known. For instance, a divorced couple (Say

Table 20 Papers with citation> 1000 in the area of quantum cryptography

Reference	Google citation	Web of science	Publication year	Quantum/ classical
[279]	21,388	NA	1978	C
[278]	18,797	NA	1976	C
[81]	13,969	NA	1964	Q
[80]	10,303	5960	1991	Q
[2]	9083	2723	1997	Q
[55,56]	7859	NA	1984	Q
[5]	7781	4595	2002	Q
[281]	6498	NA	1987	C
[1]	6192	NA	1994	Q
[3]	5373	NA	1996	Q
[12]	5265	NA	1982	Q
[212]	4509	NA	1982	Q
[73]	3379	1810	1992	Q
[57]	2528	1405	2000	Q
[70]	2226	1368	1992	Q
[280]	2046	NA	1978	C
[285]	2035	NA	1978	C
[294]	1858	NA	1989	C
[287]	1707	NA	1998	C
[4]	1647	NA	1996	Q
[253]	1190	744	2007	Q
[117]	1190	772	2002	Q
[29]	1165	751	2003	Q
[250]	1145	NA	1969	Q
[59]	1106	512	2001	Q
[258]	1043	654	2012	Q
[17]	1014	NA	1988	Q

Table 21 Papers with google citation> 30 per year in the area of quantum cryptography

Reference	Google citation	Google citation/m $m = 2020-$ Year of Publication	Web of science	Publication year
[287]	494	164.66	233	2017
[305]	435	145	241	2017
[53]	598	99.6	365	2014
[306]	191	95.5	92	2018
[246]	853	85.3	483	2010
[283]	918	83.45	NA	2009
[131]	235	78.33	160	2017
[324]	363	72.6	221	2015
[348]	134	67	61	2018
[301]	243	60.75	NA	2016
[8]	208	52	120	2016
[248]	769	51	458	2005
[28]	917	50.94	567	2002
[255]	403	50.375	309	2012
[142]	185	46.25	143	2016
[98]	736	46	366	2004
[218]	322	46	208	2013
[337]	127	42.33	57	2017
[292]	169	42.25	NA	2016
[92]	905	41	439	1998
[36]	804	40.2	454	2000
[284]	117	39	23	2017
[313]	304	38	168	2012
[50]	454	37.8	272	2008
[26]	180	36	107	2015
[214]	800	34.78	373	1997
[311]	338	30.72	NA	2009
[252]	341	31	200	2009
[41]	429	30.64	280	2006

Alice and Bob) both want to stay with their single kid and Alice is staying in North India and Bob is staying in South India. A weak coin-tossing protocol will be useful in such a situation where both want to take the responsibility of their kid.

Molina-Terriza et al. [349] designed the first quantum coin flipping protocol using qutrits rather than qubit for higher securities. Here, both communicator Alice and Bob distrust each other. They showed the possibility of a cheater and ways to detect the cheater. Using the concept of photons entangled, Alice and Bob succeeded to toss a row coin remotely.

Colbeck [350] designed a protocol for strong coin-tossing using the power of entanglement and achieve a bias of 1/4. The major advantage of colbeck's protocol is that it requires only qubits for achieving the bias, whereas bit-commitment require higher-dimensional system [351].

12.8 QKD Devices

Toshiba's QKD system [352] delivers secure key over 100 KM on fiber optic-based network with a bit rate of 1 Megabit per second. This QKD system is based on T12 protocol (A decoy-state protocol with appropriate modification in BB84) [105]. Toshiba reported that cryogenic detectors operating at room temperature would enhance the performance of high bit rate [106].

To meet the requirement of Metropolitan Area Network, QuantumCTek [353] developed QKD-POL40 series QKD systems based on BB84 protocol with decoy-state and polarization coding. QKD-POL40 is further classified in transmitting mode (QKD-POL40A) and receiving mode (QKD-POL40B). QuantumCTek's QKD system is secure

against attacks (photon beam separation, light blinding and double counting) and provide the feature of quantum channel automatic correction. It provides 15 KBPS@10 dB under typical key rate @25 °C.

IDquantique IDQ's Cerberis QKD system [354] provides secure key exchange at temperature 10° to 30° with secret key rate of 1.4 kb/s (12 dB). Details of parameters and feature of Cerberis QKD system can be found in [355].

The Quantum Technologies Group of the University of Geneva, ID Quantique and Corning Incorporated performed a successful Quantum key distribution at a distance of 421 KM using a three-state time-bin protocol with decoy approach and 2.5 GHZ repetition rate [356]. Travagnin and Lewis [357] carried out a detailed survey of quantum key distribution deployment worldwide. Yuan et al. [358] reported the first QKD complete system which delivers real-time secure keys at the rate of exceeding 10 Mb/s.

12.9 Concluding Remarks

Classical Cryptography is still safe as classical computers can not crack the cryptography algorithms. Concept of quantum cryptography has been commercialized rapidly after the design of the BB84 protocol. Table 19 depicts the significant sources of quantum cryptography. Table 20 shows the most influential quantum cryptography research papers with $citation > 1000$. Table 21 represents a few additional influencing research papers with $citations > 30$ per year.

Computational speed will improve dramatically after the development of the quantum computer. Various research organization and companies are working extensively towards the development of post-quantum algorithms. With NIST competitions, more attacks, algorithms design and implementations are also emerging. Unconditional security of quantum cryptography will make it a long term security solution.

Determining the power of quantum hardware is also a challenging issue. Significant work on verifying quantum computation devices can be found in [359–361]. Significant efforts have been made to develop QKD devices. However, low-cost, robust and higher secure key rate and distance remain a challenges question. Satellite-based QKD also emerges rapidly because QKD based on ground approaches has a limited distance (due to fiber attenuation and atmospheric losses).

To overcome challenges in quantum cryptography (quantum attacks, imperfections in quantum communications, cost, distance, secret key rate) and achieve the goal of the quantum internet, research in the area of quantum cryptography will take a rapid pace in the years to come.

Acknowledgements All figures in this manuscript has been drawn using Edraw Software.

References

1. Shor PW (1994) Algorithms for quantum computation: discrete logarithms and factoring. In: Proceeding of 35^{th} annual symposium on the foundations of computer science, 20–22 Nov. NM, USA, Santa Fe, pp 124–134
2. Shor PW (1997) Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J Comput 26:1484–1509
3. Grover LK (1996) A fast quantum mechanical algorithm for database search. In: Proceedings of the 28^{th} annual symposium on theory of computation, Philadelphia, Pennsylvania, USA, May 22–24, pp 212–219
4. Wiesner S (1983) Conjugate coding. ACM SIGACT News 15:78–88
5. Gisin N, Ribordy G, Tittel W, Zbinden H (2002) Quantum cryptography. Rev Mod Phys 74:145–195
6. Alleaume R, Branciard C, Bouda J, Debuisschert T, Dianati M, Gisin N, Godfrey M, Grangier P, Langer T, Lutkenhaus N, Monyk C, Painchault P, Peev M, Poppe A, Pornin T, Rarity J, Renner R, Ribordy G, Riguidel M, Salvail L, Shields A, Weinfurter H, Zeilinger A (2014) Using quantum key distribution for cryptographic purposes: a survey. Theor Comput Sci 560:62–81
7. Giampouris D (2016) Short review on quantum key distribution protocols. In: Vlamos P (ed) GeNeDis computational biology and bioinformatics, advances in experimental medicine and biology, vol 988. Springer, Cham, pp 149–157
8. Diamanti E, Lo HK, Qi B, Yuan Z (2016) Practical challenges in quantum key distribution. npj Quantum Inf 2:16025
9. Long GL (2017) Quantum secure direct communication: principles, current status, perspectives. In: 2017 IEEE 85th vehicular technology conference (VTC 2017 Spring) 4–7 June 2017 Sydney, Australia, pp 1–5
10. Zhou T, Shen J, Li X, Wang C, Shen J (2018) Quantum cryptography for the future internet and the security analysis. Security and Communications Networks Article id 8214619, pp 1–7
11. Heisenberg W (1927) Uber Den Anschaulichen Inhalt Der Quantentheoretischen Kinematik Und Mechanik. Zeitschrift Fur Physik (in German) 43(3–4):172–198
12. Wootters WK, Zurek WH (1982) A single quantum cannot be cloned. Nature 299:802–803
13. Einstein A, Podolsky B, Rosen N (1935) Can quantum-mechanical description of physical reality be considered complete? Phys Rev 47:777–780
14. Vernam GS (2019) Secret signaling system, US Patent 1310719A, July 22, 1919. https://patentimages.storage.googleapis.com/5d/ae/f5/1256151a84830e/US1310719.pdf
15. Schumacher B, Westmoreland MD (2006) Quantum mutual information and the one-time pad. Phys Rev A 74:042305
16. Brandao FGSL, Oppenheim J (2012) The quantum one-time pad in the presence of an eavesdropper. Phys Rev Lett 108(4):040504
17. Bennett CH, Brassard G, Robert JM (1988) Privacy amplification by public discussion. SIAM J Comput 17(2):210–229
18. Griffet C (2019) From discrete-to continuous-variable protocols for quantum key distribution, Master Thesis, Universite Libre De Bruxelles
19. Ralph TC (1999) Continuous variable quantum cryptography. Phys Rev A 61:010303
20. Reid MD (2000) Quantum cryptography with a predetermined key, using continuous variable Einstein–Podolsky–Rosen correlations. Phys Rev A 62(6):062308-1–062308-6
21. Hillery M (2000) Quantum cryptography with squeezed states. Phys Rev A 61:022309

22. Garcia-Patron R, Cerf NJ (2009) Continuous-variable quantum key distribution protocols over noisy channels. Phys Rev Lett 102:130501-1–130501-4
23. Cerf NJ, Grangier P (2007) From quantum cloning to quantum key distribution with continuous variables: a review (Invited). J Opt Soc Am 24(2):324–334
24. Cerf NJ, Levy M, Assche GV (2001) Quantum distribution of gaussian keys using squeezed states. Phys Rev A 63:052311
25. Grosshans F, Grangier P (2002) Continuous variable quantum cryptography using coherent states. Phys Rev Lett 88:057902
26. Grosshans F, Assche GV, Wenger J, Brouri R, Cerf NJ, Grangier P (2003) Quantum key distribution using gaussian-modulated coherent states. Nature 421:238–241
27. Lodewyck J, Debuisschert T, Tualle-Brouri R, Grangier P (2005) Controlling excess noise in fiber optics continuous variables quantum key distribution. Phys Rev A 72:050303
28. Weedbrook C, Lance AM, Bowen WP, Symul T, Ralph TC, Lam PK (2004) Quantum cryptography without switching. Phys Rev Lett 93(17):170504-1–170504-4
29. Leverrier A, Grangier P (2011) Continuous-variable quantum key distribution protocols with a discrete modulation. arXiv:1002.4083
30. Papanastasiou P, Pirandola S (2020) Continuous-variable quantum cryptography with discrete alphabets: composable security under collective gaussian attacks, pp 1–6. arXiv:1912.11418
31. Andersen UL, Neergaard-Nielsen JS, Loock P, Furusawa A (2015) Hybrid discrete-and continuous-variable quantum information. Nat Phys 11:713–719
32. Sanchez RG (2007) Quantum information with optical continuous variables: from Bell tests to key distribution, PhD Thesis, The Center for Quantum Information and Communication (QuIC) of the University of Bruxelles (ULB)
33. Makarov V, Hjelme DR (2005) Faked states attack on quantum cryptosystems. J Mod Opt 52:691–705
34. Pirandola S (2008) Symmetric collective attacks for the eavesdropping of symmetric quantum key distribution. Int J Quantum Inf 6:765–771
35. Huttner B, Imoto N, Gisin N, Mor T (1995) Quantum cryptography with coherent states. Phys Rev A 51(3):1863–1869
36. Lutkenhaus N (2000) Security against individual attacks for realistic quantum key distribution. Phys Rev A 61:052304-1–052304-10
37. Liu WT, Sun SH, Liang LM, Yuan JM (2011) Proof-of-principle experiment of a modifed photon-number-splitting attack against quantum key distribution. Phys Rev A 83:042326-1–042326-5
38. Fuchs CA, Gisin N, Griffiths RB, Niu CS, Peres A (1997) Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy. Phys Rev A 56(2):1163–1172
39. Vakhitov A, Makarov V, Hjelme DR (2001) Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography. J Mod Phys 48(13):2023–2038
40. Dehmani M, Ez-Zahraouy H, Benyoussef A (2010) Quantum cryptography with several cloning attacks. J Comput Sci 6(7):684–688
41. Gisin N, Fasel S, Kraus B, Zbinden H, Ribordy G (2006) Trojan-horse attacks on quantum-key-distribution-systems. Phys Rev A 73:022320-1–022320-6
42. Kronberg DA, Molotkov SN (2010) Quantum scheme for an optimal attack on quantum key distribution protocol BB84. Bull Russ Acad Sci Phys 74(7):912–918
43. Jain N, Anisimova E, Khan I, Makarov V, Marquardt C, Leuchs G (2014) Trojan-horse attacks threaten the security of practical quantum cryptography. New J Phys 16:123030
44. Fei YY, Meng XD, Gao M, Wang H, Ma Z (2018) Quantum man-in-the-middle attack on the calibration process of quantum key distribution. Sci Rep 8:1–10
45. Lamas-Linares A, Kurtsiefer C (2007) Breaking a quantum key distribution system through a timing side channel. Opt Express 15(15):9388–9393
46. Qi B, Fung CHF, Lo HK, Ma X (2007) Time-shift attack in practical quantum cryptosystems. Quantum Inf Comput 7(1):73–82
47. Sun SH, Xu F, Jiang MS, Ma XC, Lo HK, Liang LM (2015) Effect of source tampering in the security of quantum cryptography. Phys Rev A 92(2):022304
48. Fung CHF, Qi B, Tamaki K, Lo HK (2007) Phase-remapping attack in practical quantum-key-distribution systems. Phys Rev A 75(3):032314-1–032314-12
49. Xu F, Qi B, Lo HK (2010) Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. New J Phys 12:113026
50. Zhao Y, Fung CHF, Qi B, Chen C, Lo HK (2008) Quantum hacking: experimental demonstration of time-shift attack against practical quantum-key-distribution systems. Phys Rev A 78:042333-1–042333-5
51. Wei K, Zhang W, Tang YL, You L, Xu F (2019) Implementation security of quantum key distribution due to polarization-dependent efficiency mismatch. Phys Rev A 100(2):022325
52. Boyer M, Liss R, Mor T (2020) Composable security against collective attacks of a modified BB4 QKD protocol with information only in one basis. Theor Comput Sci 801:96–109
53. Lo HK, Curty M, Tamaki K (2014) Secure quantum key distribution. Nat Photonics 8:595–604
54. Jain N, Stiller B, Khan I, Elser D, Marquardt C, Leuchs G (2016) Attacks on practical quantum key distribution systems (and how to prevent them). Contemp Phys 57(3):366–387
55. Bennett CH, Brassard G (1984) Quantum cryptography: public key distribution and coin tossing. In: International conference on computers, systems and signal processing Bangalore, India, Dec 10–12 1984, pp 175–179
56. Bennett CH, Brassard G (2014) Quantum cryptography: public key distribution and coin tossing. Theor Comput Sci 560:7–11
57. Chuang I, Oliver W, Shor P (2019) Introduction to quantum computing online course. https://learn-xpro.mit.edu/quantum-computing. Accessed 24 May 2020
58. Shor PW, Preskill J (2000) Simple proof of security of the BB84 quantum key distribution protocol. Phys Rev Lett 85(2):441–444
59. Biham E, Boyer M, Boykin PO, Mor T, Roychowdhury V (2006) A proof of the security of quantum key distribution. J Cryptol 19(4):381–439
60. Mayers D (2001) Unconditional security in quantum cryptography. J ACM 48:351–406
61. Scarani V, Kurtsiefer C (2014) The black paper of quantum cryptography: real implementation problems. Theor Comput Sci 560:27–32
62. Goldenberg L, Vaidman L (1995) Quantum cryptography based on orthogonal states. Phys Rev Lett 75:1239–1243
63. Peres A (1996) Quantum cryptography with orthogonal states? Phys Rev Lett 77:3264
64. Goldenberg L, Vaidman L (1996) Reply to comment: Quantum cryptography with orthogonal states, pp 1–3. arXiv:quant-ph/9604029.pdf
65. Dan L, Chang-xing P, Dong-xiao Q, Bao-bin H, Nan Z (2009) A new attack strategy for BB84 protocol based on Breidbart basis, ChinaCom2009-network and information security symposium, 26th–27th Aug 2009, Xian, China, vol 4, pp 1–3
66. Yong W, Huadeng W, Zhaohong L, Jinxiang H (2009) Man-in-the-middle attack on BB84 protocol and its defence. In: 2^{nd} IEEE international conference on computer science and information technology (CSIT) Aug 8–11, Beijing, China, vol 2, pp 438–439
67. An H, Liu D, Yu T (2014) A solution for beam splitter attack on BB84 protocol. In: Proceedings of the 2014 international confer-

ence on computer, communications and information technology, advances in intelligent systems research. Atlantis Press
68. Garcia-Patron R, Wong FNC, Shapiro JH (2010) Optimal individual attack on BB84 quantum key distribution using single-photon two-qubit quantum logic. Proc SPIE Int Soc Opt Eng 7702:77020C-1–77020C-10
69. Boyer B, Liss R, Mor T (2017) Security against collective attacks of a modified BB84 QKD protocol with information only in one basis. In: Proceedings of the 2^{nd} international conference on complexity, future information systems and risk (COMPLEXIS 2017), vol 2, pp 23–29
70. Jiang MS, Sun SH, Li CY, Liang LM (2014) Frequency shift attack on plug-and-play quantum key distribution systems. J Mod Opt 61(2):147–153
71. Bennett CH, Brassard G, Mermin ND (1992) Quantum cryptography without Bell's theorem. Phys Rev Lett 68:557–559
72. Waks E, Zeevi A, Yamamoto Y (2002) Security of quantum key distribution with entangled photons against individual attacks. Phys Rev A 65:052310-1–052310-16
73. Adenier G, Ohya M, Watanabe N, Basieva I, Khrennikov AY (2012) Double blinding-attack on entanglement-based quantum key distribution protocols. AIP Conf Proc 1424:9–16
74. Bennett CH (1992) Quantum cryptography using any two nonorthogonal states. Phys Rev Lett 68:3121–3124
75. Yonofsky NS, Mannucci MA (2008) Quantum computing for computer scientists. Cambridge University Press, Cambridge
76. Tamaki K, Koashi M, Imoto N (2003) Unconditionally secure key distribution based on two nonorthogonal states. Phys Rev Lett 90:167904
77. Tamaki K, Lukenhaus N (2004) Unconditional security of the Bennett 1992 quantum key-distribution protocol over a lossy and noisy channel. Phys Rev A 69:032316
78. Koashi M (2004) Unconditional security of coherent-state quantum key distribution with a strong phase-reference pulse. Phys Rev Lett 93:120501
79. Kuppam S (2018) Modelling and analysis of quantum key distribution protocols, BB84 and B92. In: Communicating quantum processes (CQP) language and analysing in PRISM, pp 1–12. arxiv.org/pdf/1612.03706.pdf
80. Phoenix SJD, Barnett SM, Chefles A (2000) Three-state quantum cryptography. J Mod Opt 47(2–3):507–516
81. Senekane M, Mafu M, Petruccione F (2015) Six-state symmetric quantum key distribution protocol. J Quantum Inf Sci 5:33–40
82. Ekert AK (1991) Quantum cryptography based on Bell's theorem. Phys Rev Lett 67:661–663
83. Bell JS (1964) On the Einstein Podolsky Rosen paradox. Physics 1(3):195–200
84. Hensen B, Kalb N, Blok MS, Dreau AE, Reiserer A, Vermeulen RFL, Schouten RN, Markham M, Twitchen DJ, Goodenough K, Elkouss D, Wehner S, Taminiau TH, Hanson R (2016) Loophole-free Bell test using electron spins in diamond: second experiment and additional analysis. Sci Rep 6(30289):1–11
85. Ilic N (2007) The Ekert protocol. J Phys 334:1–4
86. Li Q, Li Z, Chan WH, Zhang S, Liu C (2018) Blind quantum computation with identity authentication. Phys Lett A 382(14):938–941
87. Inamori H, Rallan L, Vedral V (2001) Security of EPR-based quantum cryptography against incoherent symmetric attacks. J Phys A: Math Gen 34(35):6913
88. Ling A, Peloso M, Marcikic I, Lamas-Linares A, Kurtsiefer C (2008) Experimental E91 quantum key distribution. In: Proceedings of advanced optical concepts in quantum computing, memory, and communication. Integrated Optoelectronic Devices, San Jose, California, USA, p 6903
89. Acin A, Massar S, Pironio S (2006) Efficient quantum key distribution secure against no-signalling eavesdroppers. New J Phys 8(126):1–11
90. Honjo T, Nam SW, Takesue H, Zhang Q, Kamada H, Nishida Y, Tadanaga O, Asobe M, Baek B, Hadfield R, Miki S, Fujiwara M, Sasaki M, Wang Z, Inoue K, Yamamoto Y (2008) Long-distance entanglement-based quantum key distribution over optical fiber. Opt Express 16(23):19118–19126
91. Fujiwara M, Yoshino KI, Nambu Y, Yamashita T, Miki S, Terai H, Wang Z, Toyoshima M, Tomita A, Sasaki M (2014) Modified E91 protocol demonstration with hybrid entanglement photon source. Opt Express 22(11):13616–13624
92. Li L, Li H, Li C, Chen X, Chang Y, Yang Y, Li J (2018) The security analysis of E91 protocol in collective-rotation noise channel. Int J Distrib Sens Netw 14(5):1–7
93. Sharma A, Lenka SK (2016) E91 QKD protocol for authentication in online banking systems. Int J Bus Inf Syst 22(1):116–122
94. Brub D (1998) Optimal eavesdropping in quantum cryptography with six states. Phys Rev Lett 81:3018
95. Lo HK (2001) Proof of unconditional security of six-state quantum key distribution scheme. Quantum Inf Comput 1(2):81–94
96. Kato G, Tamaki K (2016) Security of six-state quantum key distribution protocol with threshold detectors. Sci Rep 6:1–5
97. Garapo K, Mafu M, Petruccione F (2016) Intercept-resend attack on six-state quantum key distribution over collective-rotation noise channels. Chin Phys B 25(7):070303-1–070303-7
98. Bechmann-Pasquinucci H, Gisin N (1999) Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. Phys Rev A 59:4238
99. Azuma H, Ban M (2019) The intercept/resend attack and the collective attack on the six-state protocol of the quantum key distribution, pp 1–24. arXiv:1912.00196
100. Scarani V, Acin A, Ribordy G, Gisin N (2004) Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. Phys Rev Lett 92:057901
101. Chuang I, Oliver W, Shor W (2019) Sarg04. https://en.wikipedia.org/wiki/SARG04. Accessed 24 May 2019
102. Branciard C, Gisin N, Kraus B, Scarani V (2005) Security of two quantum cryptography protocols using the same four qubit states. Phys Rev A 72(3):032301
103. Koashi M (2005) Security of quantum key distribution with discrete rotational symmetry. arXiv:quant-ph/0507154
104. Fung CF, Tamaki K, Lo HK (2005) On the performance of two protocols: SARG04 and BB84. arXiv:quant-ph/0510025
105. Lucamarini M, Patel KA, Dynes JF, Frohlich B, Sharpe AW, Dixon AR, Yuan ZL, Penty RV, Shields AJ (2013) Efficient decoy-state quantum key distribution with quantified security. Opt Express 21(21):24550–24565
106. Comandar LC, Frohlich B, Lucamarini M, Patel KA, Sharpe AW, Dynes JF, Yuan ZL, Penty RV, Shields AJ (2014) Room temperature single-photon detectors for high bit rate quantum key distribution. Appl Phys Lett 104:021101
107. Bennett CH, Wiesner SJ (1992) Communication via one- and two-particle operators on Einstein–Podolsky–Rosen states. Phys Rev Lett 69:2881
108. Bechmann-Pasquinucci H, Peres A (2000) Quantum cryptography with 3-state systems. Phys Rev Lett 85(15):3313–3316
109. Inoue K, Waks E, Yamamoto Y (2002) Differential phase shift quantum key distribution. Phys Rev Lett 89(3):037902
110. Deng FG, Long GL (2004) Bidirectional quantum key distribution protocol with practical faint laser pulses. Phys Rev A 70(1):012311
111. Stucki D, Fasel S, Gisin N, Thoma Y, Zbinden H (2007) Coherent one-way quantum key distribution. International Congress on optics and optoelectronics, Prague, Czech. In: Proceedings photon

counting applications, quantum optics, and quantum cryptography, p 6583
112. Pan C, Yan-Song L, Fu-Guo D, Gui-Lu L (2007) Measuring-basis encrypted quantum key distribution with four-state systems. Commun Theor Phys 47:49–52
113. Khan MM, Murphy M, Beige A (2009) High error-rate quantum key distribution for long-distance communication. New J Phys 11:063043
114. Noh TG (2009) Counterfactual quantum cryptography. Phys Rev Lett 103:230501
115. Gao F, Liu B, Wen QY, Chen H (2012) Flexible quantum private queries based on quantum key distribution. Opt Express 20(16):17411–17420
116. Wei CY, Gao F, Wen QY, Wang TY (2014) Practical quantum private query of blocks based on unbalanced-state Bennett–Brassard-1984 quantum-key-distribution protocol. Sci Rep 4:7537-1–7537-7
117. Gao F, Liu B, Huang W, Wen QY (2015) Post processing of the oblivious key in quantum private query. IEEE J Sel Top Quantum Electron 21(3):6600111
118. Beige A, Englert BG, Kurtsiefer C, Weinfurter H (2002) Secure communication with a publicly known key. Acta Phys Pol A 101:357–368
119. Hong-Mei H (2015) Quantum secure direct communication protocol based on cluster entangled state. In: 10^{th} international conference on P2P, parallel, grid, cloud and internet computing (3PGCIC). Krakow, Poland, pp 440–443
120. Bostrom K, Felbinger T (2002) Deterministic secure direct communication using entanglement. Phys Rev Lett 89:187902
121. Wojcik A (2003) Eavesdropping on the "Ping-pong" quantum communication protocol. Phys Rev Lett 90:157901
122. Cai QY (2003) The "ping-pong" protocol can be attacked without eavesdropping. Phys Rev Lett 91:109801
123. Zhang Z, Man Z, Li Y (2004) Improving Wojcik's eavesdropping attack on ping-pong protocol. Phys Lett A 333:46–50
124. Bostroem K, Felbinger T (2008) On the security of the ping-pong protocol. Phys Lett A 372:3953–3956
125. Fu-Guo D, Xi-Han L, Chun-Yan L, Ping Z, Hong-Yu Z (2007) Eavesdropping on the "Ping-Pong" quantum communication protocol freely in a noise channel. Chin Phys 16:277–281
126. Lucamarini M, Mancini S (2005) Secure deterministic communication without entanglement. Phys Rev Lett 94:140501-1–140501-4
127. Han YG, Yin ZQ, Li HW, Chen W, Wang S, Guo GC, Han ZF (2014) Security of modified ping-pong protocol in noisy and lossy channel. Sci Rep 4:4936
128. Chamoli A, Bhandari CM (2009) Secure direct communication based on ping-pong protocol. Quantum Inf Process 8:347–356
129. Naseri M (2010) Comment on: Secure direct communication based on ping-pong protocol. Quantum Inf Process 9:693–698
130. Chun-Yan L, Hong-Yu Z, Yan W, Fu-Guo D (2005) Secure quantum key distribution network with Bell states and local unitary operations. Chin Phys Lett 22:1049–1052
131. Li XH, Deng FG, Li CY, Liang YJ, Zhou P, Zhou H (2006) Deterministic secure quantum communication without maximally entangled states. J Korean Phys Soc 49(4):1354–1359
132. Li J, Zhou Z, Wang N, Tian Y, Yang YG, Zheng Y (2019) Deterministic quantum secure direct communication protocol based on hyper-entangled state. IEEE Access 7:43948–43955
133. Kwiat PG (1997) Hyper-entangled states. J Mod Opt 44(11–12):2173–2184
134. Zhang W, Ding DS, Sheng YB, Zhou L, Shi BS, Guo GC (2017) Quantum secure direct communication with quantum memory. Phys Rev Lett 118:2205011–2205016
135. Lee H, Lim J, Yang HJ (2006) Quantum direct communication with authentication. Phys Rev A 73:042305
136. Min-Jie W, Wei P (2008) Quantum secure direct communication based on authentication. Chin Phys Lett 25(11):3860–3863
137. Dan L, Chang-Xing P, Dong-Xiao Q, Nan Z (2010) A new quantum secure direct communication scheme with authentication. Chin Phys Lett 27:0503061–0503063
138. Huang D, Chen Z, Guo Y, Lee MH (2007) Quantum secure direct communication based on chaos with authentication. J Phys Soc Jpn 76:124001-1–124001-4
139. Chen XB, Wen QY, Guo FZ, Sun Y, Xu G, Zhu FC (2008) Controlled quantum secure direct communication with W state. Int J Quantum Inf 6:899–906
140. Chen ZN, Qin Z, Lu L (2009) A quantum secure direct communication with authentication. Inf Technol J 8(7):1027–1032
141. Yang XY, Ma Z, Lu X, Li HX (2009) Quantum secure direct communication based on partially entangled states. In: Fifth international conference on information assurance and security, 18–20 Aug, vol 2, pp 11–14
142. Yu CH, Guo GD, Lin S (2013) Quantum secure direct communication with authentication using two nonorthogonal states. Int J Theor Phys 52:1937–1945
143. Yang CW, Hwang T, Lin TH (2013) Modification attack on QSDC with authentication and the improvement. Int J Theor Phys 52:2230–2234
144. Hu JY, Yu B, Jing MY, Xiao LT, Jia ST, Qin GQ, Long GL (2016) Experimental quantum secure direct communication with single photons. Light Sci Appl 5:e16144
145. Sarvaghad-Moghaddam M (2019) Efficient controlled bidirectional quantum secure direct communication using entanglement swapping in a network. arXiv:1902.11188 1–15
146. Nguyen BA (2004) Quantum dialogue. Phys Lett A 328:6–10
147. Hong C, Yang H (2006) Comment on "Quantum dialogue protocol", pp 1–4. arXiv:quant-ph/0606174
148. Zhong-Xiao M, Zhan-Jun Z, Yong L (2005) Quantum dialogue revisited. Chin Phys Lett 22(1):22–24
149. YuGuang Y, QiaoYan W (2007) Quasi-secure quantum dialogue using single photons. Sci China Press G Phys Mech Astron 50(5):558–562
150. Tan YG, Cai QY (2008) Classical correlation in quantum dialogue. Int J Quantum Inf 6(2):325–329
151. Xia Y, Fu CB, ZHANG S, Hong SK, Yeon KH, Um CI (2006) Quantum dialogue by using the GHZ state. J Korean Phys Soc 48:24–27
152. Yan X, Jie S, Jing N, He-Shan S (2007) Controlled secure quantum dialogue using a pure entangled GHZ states. Commun Theor Phys 48(5):841–846
153. Cao G, Jiang M (2017) Multi-party quantum dialogue protocol based on multi-particle GHZ states, 2017 Chinese Automation Congress (CAC), 20–22 Oct 2017, Jinan, China, pp 1614–1618
154. Gong L, Tian C, Li J, Zou X (2018) Quantum network dialogue protocol based on continuous-variable GHZ states. Quantum Inf Process 17(331):1–12
155. Chou YH, Zeng GJ, Chang ZH, Kuo SY (2018) Dynamic group multi-party quantum key agreement. Sci Rep 8:4633
156. Boyer M, Kenigsberg D, Mor T (2007) Quantum key distribution with classical Bob. Phys Rev Lett 99(14):140501
157. Boyer M, Gelles R, Kenigsberg D, Mor T (2009) Semiquantum key distribution. Phys Rev A 79:032341
158. Krawec WO (2014) Restricted attacks on semi-quantum key distribution protocols. Quantum Inf Process 13:2417–2436
159. Krawec WO (2015) Mediated semi-quantum key distribution. Phys Rev A 91:032323
160. Zou X, Qiu D, Li L, Wu L, Li L (2009) Semiquantum-key distribution using less than four quantum states. Phys Rev A 79:0522312
161. Lu H, Cai QY (2008) Quantum key distribution with classical alice. Int J Quantum Inf 6(6):1195–1202

162. Zhang W, Qiu D, Mateus P (2008) Security of a single-state semi-quantum key distribution protocol. Quantum Inf Process 17(6):1–21
163. Xian-Zhou Z, Wei-Gui G, Yong-Gang T, Zhen-Zhong R, Xiao-Tian G (2009) Quantum key distribution series network protocol with M-classical Bobs. Chin Phys B 18:2143
164. Jian W, Sheng Z, Quan Z, Chao-Jing T (2011) Semiquantum key distribution using entangled states. Chin Phys Lett 28:100301
165. Li L, Qiu D, Mateus P (2013) Quantum secret sharing with classical bobs. J Phys A: Math Theor 46:045304-1–045304-11
166. Yu KF, Yang CW, Liao CH, Hwang T (2014) Authenticated semi-quantum key distribution protocol using Bell states. Quantum Inf Process 13:1457–1465
167. Luo YP, Hwang T (2015) Authenticated semi-quantum direct communication protocols using Bell states. Quantum Inf Process 15:947–958
168. Zou X, Qiu D, Zhang S, Mateus P (2015) Semiquantum key distribution without invoking the classical party's measurement capability. Quantum Inf Process 14:2981–2996
169. Chou WH, Hwang T, Gu J (2016) Semi-quantum private comparison protocol under an almost-dishonest third party, pp 1–18. arXiv:1607.07961
170. Lu H, Barbeau M, Nayak A (2017) Economic no-key semi-quantum direct communication protocol. IEEE Globecom Workshops, Singapore, 4–8 Dec 2017, pp 1–7
171. Boyer M, Katz M, Liss R, Mor T (2017) Experimentally feasible protocol for semiquantum key distribution. Phys Rev A 96(6):062335-1–062335-6
172. Thapliyal K, Sharma RD, Pathak A (2018) Orthogonal-state-based and semi-quantum protocols for quantum private comparison in noisy environment. Int J Quantum Inf 16(5):1850047-1–1850047-27
173. Krawec WO (2015) Security proof of a semi-quantum key distribution protocol. In: IEEE international symposium on information theory (ISIT), Hong Kong, China 14–19 June 2015, pp 686–690
174. Krawec WO (2016) Security of a semi-quantum protocol where reflections contribute to the secret key. Quantum Inf Process 15(5):2067–2090
175. Iqbal H, Krawec WO (2019) High-dimensional semi-quantum cryptography, pp 1–29. arXiv:1907.11340.pdf
176. Tsai CW, Yang CW, Lee NY (2019) Semi-quantum secret sharing protocol using W-state. Mod Physi Lett A 34(27):1950213-1–1950213-12
177. Iqbal H, Krawec WO (2019) Semi-quantum cryptography, pp 1–60. arXiv:1910.05368.pdf
178. Lin PH, Tsai CW, Hwang T (2019) Mediated semi-quantum key distribution using single photons. Annalen Der Physik 531(8):1800347-1–1800347-7
179. Wen XJ, Zhao XQ, Gong LH, Zhou NR (2019) A semi-quantum authentication protocol for message and identity. Laser Phys Lett 16:075206-1–075206-10
180. Tao Z, Chang Y, Zhang S, Dai J, Li X (2019) Two semi-quantum direct communication protocols with mutual authentication based on Bell states. Int J Theor Phys 58:2986–2993
181. Sun Y, Yan L, Chang Y, Zhang S, Shao T, Zhang Y (2019) Two semi-quantum secure direct communication protocols based on Bell states. Mod Phys Lett A 34(1):1950004-1–1950004-10
182. Yang CW (2020) Efficient and secure semi-quantum secure direct communication protocol against double Cnot attack. Quantum Inf Process 19:1–15
183. Zhou NR, Zhu KN, Bi W, Gong LH (2019) Semi-quantum identifcation. Quantum Inf Process 18:197-1–197-17
184. Yan L, Sun YH, Chang Y, Zhang SB, Wan GG, Sheng ZW (2018) Semi-quantum protocol for deterministic secure quantum communication using Bell states. Quantum Inf Process 17:315-1–315-12
185. Bechmann-Pasquinucci H, Tittel W (2000) Quantum cryptography using larger alphabets. Phys Rev A 61(6):0623081–06230812
186. Tan YG, Lu H, Cai QY (2009) Comment on "Quantum key distribution with classical Bob". Phys Rev Lett 102(9):098901–1
187. Boyer M, Mor R (2011) Comment on Semiquantum-key distribution using less than four quantum states. Phys Rev A 83:046301-1–046301-2
188. Zou X, Qiu D (2011) Reply to "comment on 'semiquantum-key distribution using less than four quantum states"'. Phys Rev A 83:046302-1–046302-2
189. Gurevich P (2013) Experimental quantum key distribution with classical Alice. The Technion-Israel Institute of Technology, Thesis Master of Science in Computer Science
190. Nie YY, Li YH, Wang ZS (2013) Semi-quantum information splitting using GHZ-type states. Quantum Inf Process 12(1):437–448
191. Maitra A, Paul G (2013) Eavesdropping in semiquantum key distribution protocol. Inf Process Lett 113(12):418–422
192. Boyer M, Mor T (2015) On the robustness of quantum key distribution with classical Alice (Photons-based protocol). In: Proceedings of the ninth international conference on quantum, nano/bio, and micro technologies, ICQNM2015, Venice, Italy, vol 9, pp 29–34
193. Xie C, Li L, Qiu D (2015) A novel semi-quantum secret sharing scheme of specific bits. Int J Theor Phys 54(10):3819–3824
194. Krawec WO (2015) Semi-quantum key distribution: Protocols, security analysis, and new models, PhD thesis, Stevens Institute of Technology
195. Yin A, Fu F (2016) Eavesdropping on semi-quantum secret sharing scheme of specific bits. Int J Theor Phys 55(9):4027–4035
196. Meslouhi A, Hassouni Y (2017) Cryptanalysis on authenticated semi-quantum key distribution protocol using Bell states. Quantum Inf Process 16(18):1–17
197. Zhang W, Qiu D (2017) A single-state semi-quantum key distribution protocol and its security proof, pp 1-12. arXiv:1612.03087
198. Shukla C, Thapliyal K, Pathak A (2017) Semi-quantum communication: protocols for key agreement, controlled secure direct communication and dialogue. Quantum Inf Process 16(12):2951–29519
199. Gao X, Zhang S, Chang Y (2017) Cryptanalysis and improvement of the semi-quantum secret sharing protocol. Int J Theor Phys 56(8):2512–2520
200. Zhang MH, Li HF, Xia ZQ, Feng XY, Peng JY (2017) Semiquantum secure direct communication using EPR pairs. Quantum Inf Process 16(5):117-1–117-14
201. Yin A, Wang Z, Fu F (2017) A novel semi-quantum secret sharing scheme based on Bell states. Mod Phys Lett B 31(13):1750150-1–1750150-6
202. Zhu KN, Zhou NR, Wang YQ, Wen XJ (2018) Semi-quantum key distribution protocols with GHZ states. Int J Theor Phys 57(12):3621–3631
203. He J, Li Q, Wu C, Chan WH, Zhang S (2018) Measurement-device-independent semiquantum key distribution. Int J Quantum Inf 16(2):1850012-1–1850012-10
204. Krawec WO (2018) Practical security of semi-quantum key distribution. In: Proceeding of quantum information science, sensing, and computation X, International Society for Optics and Photonics, vol 10660, p 1066009
205. Xie C, Li L, Situ H, He J (2018) Semi-quantum secure direct communication scheme based on Bell states. Int J Theor Phys 57(6):1881–1887
206. Liu L, Xiao M, Song X (2018) Authenticated semiquantum dialogue with secure delegated quantum computation over a collective noise channel. Quantum Inf Process 17(12):342-1–342-17
207. Zhang W, Qiu D, Mateus P (2018) Security of a single-state semi-quantum key distribution protocol. Quantum Inf Process 17:135-1–135-21

208. Yan-Feng L (2018) Semi-quantum private comparison using single photons. Int J Theor Phys 57(10):3048–3055
209. Ye TY, Ye CQ (2018) Measure-resend semi-quantum private comparison without entanglement. Int J Theor Phys 57(12):3819–3834
210. Zhao XQ, Chen HY, Wang YQ, Zhou NR (2019) Semi-quantum Bi-signature scheme based on W states. Int J Theor Phys 58(10):3239–3251
211. Yan LL, Zhang SB, Chang Y, Sheng ZW, Yang F (2019) Mutual semiquantum key agreement protocol using Bell states. Mod Phys Lett A 34(35):1950294
212. Yan L, Zhang S, Chang Y, Sheng Z, Sun Y (2019) Semi-quantum key agreement and private comparison protocols using Bell states. Int J Theor Phys 58:3852–3862
213. Lu H, Barbeau M, Nayak A (2019) Keyless semi-quantum point-to-point communication protocol with low resource requirements. Sci Rep 9(1):64-1–64-15
214. Tsai CW, Yang CW, Lee NY (2019) Lightweight mediated semi-quantum key distribution protocol. Mod Phys Lett A 34:1950281-1–1950281-13
215. Yao AC (1982) Protocols for secure computations. In: Proceedings of the 23^{rd} annual IEEE symposium on foundations of computer science (SCFS1982). IEEE Computer Society, Washington, DC, USA, pp 160–164
216. Zhang WW, Li D, Zhang KJ, Zuo HJ (2013) A quantum protocol for millionaire problem with Bell states. Quantum Inf Process 12:2241–2249
217. Mayers D (1997) Unconditionally secure quantum bit commitment is impossible. Phys Rev Lett 78:3414
218. Lo HK, Chau HF (1997) Is quantum bit commitment really possible? Phys Rev Lett 78:3410
219. Dong L, Xiu XM, Gao YJ, Chi F (2008) Multiparty controlled deterministic secure quantum communication through entanglement swapping. Int J Mod Phys C 19(11):1673–1681
220. Shi RH, Zhong H (2013) Multi-party quantum key agreement with Bell states and bell measurements. Quantum Inf Process 12:921–932
221. Liu Y, Chen TY, Wang LJ, Liang H, Shentu GL, Wang J, Cui K, Yin HL, Liu NL, Li L, Ma X, Pelc JS, Fejer MM, Peng CZ, Zhang Q, Pan JW (2013) Experimental measurement-device-independent quantum key distribution. Phys Rev Lett 111(13):130502
222. Sun Z, Zhang C, Wang B, Li Q, Long D (2013) Improvements on "multiparty quantum key agreement with single particles.". Quantum Inf Process 12:3411–3420
223. Yin XR, Ma WP, Shen DS, Wang LL (2013) Three-party quantum key agreement with bell states. Acta Phys Sin 62(17):170304-1–170304-6
224. Yin XR, Ma WP, Liu WY (2013) Three-party quantum key agreement with two-photon entanglement. Int J Theor Phys 52:3915–3921
225. Zhu ZC, Hu AQ, Fu AM (2016) Participant attack on three-party quantum key agreement with two-photon entanglement. Int J Theor Phys 55(1):55–61
226. Shukla C, Alam N, Pathak A (2014) Protocols of quantum key agreement solely using bell states and Bell measurement. Quantum Inf Process 13:2391–2405
227. Zhu ZC, Hu AQ, Fu AM (2015) Improving the security of protocols of quantum key agreement solely using Bell states and Bell measurement. Quantum Inf Process 14(11):4245–4254
228. Gu J, Hwang T (2017) Comment on improving the security of protocols of quantum key agreement solely using Bell states and Bell measurement. In: IEEE conference on dependable and secure computing, 7–10 Aug 2017. Taiwan, Taipei, pp 520–521
229. Luo QB, Yang GW, She K, Niu WN, Wang YQ (2014) Multi-party quantum private comparison protocol based on d-dimensional entangled states. Quantum Inf Process 13(10):2343–2352
230. Huang W, Wen QY, Liu B, Su Q, Gao F (2014) Cryptanalysis of a multi-party quantum key agreement protocol with single particles. Quantum Inf Process 13:1651–1657
231. Smania M, Elhassan AM, Tavakoli A, Bourennane M (2016) Experimental quantum multiparty communication protocols. NPJ Quantum Inf 2:16010-1–16010-4
232. Sun Z, Yu J, Wang P (2016) Efficient multi-party quantum key agreement by cluster states. Quantum Inf Process 15:373–384
233. Sun Z, Zhang C, Wang P, Yu J, Zhang Y, Long D (2016) Multi-party quantum key agreement by an entangled six-qubit state. Int J Theor Phys 55(3):1920–1929
234. Sun Z, Huang J, Wang P (2016c) Efficient multiparty quantum key agreement protocol based on commutative encryption. Quantum Inf Process 15:2101–2111
235. Liu B, Xiao D, Jia HY (2016) Collusive attacks to "circle-type" multi-party quantum key agreement protocols. Quantum Inf Process 15:2113–2124
236. Huang W, Su Q, Xu B, Liu B, Fan F, Jia HY, Yang YH (2016) Improved multiparty quantum key agreement in travelling mode. Sci China Phys Mech Astron 59(12):120311-1–120311-10
237. Huang W, Su Q, Liu B, He YH, Fan F, Xu BJ (2017) Efficient multiparty quantum key agreement with collective detection. Sci Rep 7:15264-1–15264-9
238. Liu WJ, Chen ZY, Ji S, Wang HB, Zhang J (2017) Multi-party semi-quantum key agreement with delegating quantum computation. Int J Theor Phys 56(10):3164–3174
239. Wang P, Sun Z, Sun X (2017) Multi-party quantum key agreement protocol secure against collusion attack. Quantum Inf Process 16:170-1–170-10
240. Zhou NR, Zhu KN, Zou XF (2019) Multiparty semiquantum key distribution protocol with four-particle cluster states. Ann Phys 531(8):1800520-1–1800520-12
241. Sun Z, Cheng R, Wu C, Zheng C (2019) New fair multiparty quantum key agreement secure against collusive attacks. Sci Rep 9:17177-1–17177-8
242. Cao H, Ma W (2017) Multiparty quantum key agreement based on quantum search algorithm. Sci Rep 7:45046-1–45046-10
243. Cao WF, Zhen YZ, Zheng YL, Li L, Chen ZB, Liu NL, Chen K (2018) One-sided measurement-device-independent quantum key distribution. Phys Rev A 97:012313
244. Sun Z, Wu C, Zheng S, Zhang C (2019) Efficient multiparty quantum key agreement with a single d-level quantum system secure against collusive attack. IEEE Access 7:102377–102385
245. Huang WC, Yang YK, Jiang D, Chen LJ (2019) Efficient travelling-mode quantum key agreement against participant's attacks. Sci Rep 9:16421-1–16421-9
246. He WT, Wang J, Zhang TT, Alzahrani F, Hobiny A, Alsaedi A, Hayat T, Deng FG (2019) High-efficiency three-party quantum key agreement protocol with quantum dense coding and Bell states. Int J Theor Phys 58:2834–2846
247. Jo Y, Park HS, Lee SW, Son W (2019) Efficient high-dimensional quantum key distribution with hybrid encoding. Entropy 21:80
248. Mohajer R, Eslami Z (2017) Cryptanalysis of a multiparty quantum key agreement protocol based on commutative encryption. Quantum Inf Process 16:197-1–197-9
249. Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J, Makarov V (2010) Hacking commercial quantum cryptography systems by tailored bright illumination. Nat Photonics 4:686–689
250. Mayers D, Yao A (1998) Quantum cryptography with imperfect apparatus. In: Proceeding 39^{th} annual symposium on foundations of computer science, Palo Alto, CA, USA, 8–11 Nov 1998, pp 1–7
251. Barrett J, Hardy L, Kent A (2005) No signalling and quantum key distribution. Phys Rev Lett 95:010503
252. Acin A, Masanes L (2016) Certified randomness in quantum physics. Nature 540:213–219

253. Clauser JF, Horne MA, Shimony A, Holt RA (1969) Proposed experiment to test local hidden-variable theories. Phys Rev Lett 23:880–884
254. Colbeck R (2006) Quantum and relativistic protocols for secure multi-party computation, PhD Thesis, University of Cambridge
255. Pironio S, Acin A, Brunner N, Gisin N, Massar S, Scarani V (2009) Device-independent quantum key distribution secure against collective attacks. New J Phys 11:045021-1–045021-26
256. Acin A, Brunner N, Gisin N, Massar S, Pironio S, Scarani V (2007) Device-independent security of quantum cryptography against collective attacks. Phys Rev Lett 98:230501-1–230501-4
257. Lucamarini M, Vallone G, Gianani I, Mataloni P, Giuseppe GD (2012) Device-independent entanglement-based Bennett 1992 protocol. Phys Rev A 86(3):032325
258. Branciard C, Cavalcanti EG, Walborn SP, Scarani V, Wiseman HM (2012) One-sided device-independent quantum key distribution: security, feasibility, and the connection with steering. Phys Rev A 85(1):010301
259. Tomamichel M, Fehr S, Kaniewski J, Wehner S (2013) One-sided Device-independent QKD and position-based cryptography from monogamy games, advances in cryptology-EUROCRYPT. In: 32nd annual international conference on the theory and applications of cryptographic techniques, Athens, Greece, May 26–30. Lecture notes in computer science (LNCS), vol 7881, pp 609–625
260. Walk N, Hosseini S, Geng J, Thearle O, Haw JY, Armstrong S, Assad SM, Janousek J, Ralph TC, Symul T, Wiseman HM, Lam PK (2016) Experimental demonstration of Gaussian protocols for one-sided device-independent quantum key distribution. Optica 3(6):634–642
261. Lo HK, Curty M, Qi B (2012) Measurement-device-independent quantum key distribution. Phys Rev Lett 108(13):130503
262. Xu F, Curty M, Qi B, Lo HK (2015) Measurement-device-independent quantum cryptography. IEEE J Sel Top Quantum Electronics 21(3):148–158
263. Tang Z, Wei K, Bedroya O, Qian L, Lo HK (2016) Experimental measurement-device-independent quantum key distribution with imperfect sources. Phys Rev A 93:042308
264. Valivarthi R, Umesh P, John C, Owen KA, Verma VB, Nam SW, Oblak D, Zhou Q, Tittel W (2019) Measurement-device-independent quantum key distribution coexisting with classical communication. Quantum Sci Technol 4(4):045002
265. Xu F, Curty M, Qi B, Lo HK (2013) Practical aspects of measurement-device-independent quantum key distribution. New J Phys 15:113007
266. Roberts GL, Lucamarini M, Yuan ZL, Dynes JF, Comandar LC, Sharpe AW, Shields AJ, Curty M, Puthoor IV, Andersson E (2017) Experimental measurement-device-independent quantum digital signatures. Nat Commun 8:1098
267. Hu XL, Cao Y, Yu ZW, Wang XB (2018) Measurement-device-independent quantum key distribution over asymmetric channel and unstable channel. Sci Rep 8:17634
268. Qiao Y, Wang G, Li Z, Xu B, Guo H (2019) Monitoring an untrusted light source with single-photon detectors in measurement-device-independent quantum key distribution. Phys Rev A 99(5):052302
269. Cui ZX, Zhong W, Zhou L, Sheng YB (2019) Measurement-device-independent quantum key distribution with hyper-encoding. Sci China Phys Mech Astron 62:110311
270. Dellantonio L, Sorensen AS, Bacco D (2018) High-dimensional measurement-device-independent quantum key distribution on two-dimensional subspaces. Phys Rev A 98:062301
271. Pawlowski M, Brunner N (2011) Semi-device-independent security of one-way quantum key distribution. Phys Rev A 84(1):010302
272. Yang W, Wan-Su B, Hong-Wei L, Chun Z, Yuan L (2014) Security of a practical semi-device-independent quantum key distribution protocol against collective attacks. Chin Phys B 23(8):080303
273. Dall'Arno M, Passaro E, Gallego R, Pawlowski M, Acin A (2015) Detection loophole attacks on semi-device-independent quantum and classical protocols. Quantum Inf Comput 15:0037
274. Chaturvedi A, Ray M, Veynar R, Pawlowski M (2018) On the security of semi-device-independent QKD protocols. Quantum Inf Process 17:131
275. Woodhead E, Lim CCW, Pironio S (2012) Semi-device-independent QKD based on BB84 and a CHSH-type estimation. In: 7^{th} conference, TQC: conference on quantum computation, communication, and cryptography, Tokyo, Japan, May 17–19, Theory of Quantum Computation, Communication, and Cryptography, vol 7, pp 107–115
276. Lim CCW, Korzh B, Martin A, Bussieres F, Thew R, Zbinden H (2014) Detector-device-independent quantum key distribution. Appl Phys Lett 105:221112
277. Gonzalez P, Rebon L, Silva TFD, Figueroa M, Saavedra C, Curty M, Lima G, Xavier GB, Nogueira WAT (2015) Quantum key distribution with untrusted detectors. Phys Rev A 92(2):022337
278. Wei K, Liu H, Ma H, Yang X, Zhang Y, Sun Y, Xiao J, Ji Y (2017) Feasible attack on detector-device-independent quantum key distribution. Sci Rep 7:449-1–449-8
279. Qi B, Siopsis G (2015) Loss-tolerant position-based quantum cryptography. Phys Rev A 91:042337
280. Sajeed S, Huang A, Sun S, Xu F, Makarov V, Curty M (2016) Insecurity of detector-device-independent quantum key distribution. Phys Rev Lett 117(25):250505
281. Diffie W, Hellman M (1976) New directions in cryptography. IEEE Trans Inf Theory 22(6):644–654
282. Rivest RL, Shamir A, Adleman L (1978) A method for obtaining digital signatures and public-key cryptosystems. Commun ACM 21(2):120–126
283. Rivest AL, Adleman L, Dertouzos M (1978b) On data banks and privacy homomorphisms. Found Secure Comput 4(11):169–180
284. Koblitz N (1987) Elliptic curve cryptosystems. Math Comput 48(177):203–209
285. Buchmann J, Williams HC (1988) A key-exchange system based on imaginary quadratic fields. J Cryptol 1(2):107–118
286. Bernstein DJ (2009) Introduction to post-quantum cryptography. In: Bernstein DJ, Buchmann J, Dahmen E (eds) Post-quantum cryptography. Springer, Berlin, pp 1–14
287. Bernstein DJ, Lange T (2017) Post-quantum cryptography. Nature 549:188–194
288. McEliece RJ (1978) A public-key cryptosystem based on algebraic coding theory. The deep space network progress report, DSN PR 42-44, pp 114–116
289. Overbeck R, Sendrier N (2009) Code-based cryptography. Book chapter in post-quantum cryptography. Springer, Berlin, pp 95–145
290. Hoffstein J, Pipher J, Silverman JH (1998) NTRU: a ring-based public key cryptosystem. In: International algorithmic number theory symposium ANTS 1998: algorithmic number theory. Lecture notes in computer science, LNCS, Springer, vol 1423, pp 267–288
291. Biasse JF, Song F (2016) Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. In: Proceedings of the twenty-seventh annual ACM-SIAM symposium on Discrete algorithms (SODA'16), pp 893–902
292. Cramer R, Ducas L, Wesolowski B (2017) Short stickelberger class relations and application to ideal-SVP. In: Proceeding of international association for cryptologic research (EUROCRYPT 2017), Lecture notes in computer science (LNCS), vol 10210, pp 324–348

293. Laarhoven T (2015) Sieving for shortest vectors in lattices using angular locality-sensitive hashing. In: 35th annual cryptology conference on advances in cryptology (CRYPTO 2015), Santa Barbara, CA, Lecture notes in computer science, vol 9215, pp 3–22
294. Laarhoven T, Weger BD (2015) Faster sieving for shortest lattice vectors using spherical locality-sensitive hashing. In: Proceedings of 4^{th} international conference on cryptology and information security in Latin America (LATINCRYPT 2015), Lecture notes in computer science book series (LNCS), vol 9230, pp 101–118
295. Becker A, Ducas L, Gama N, Laarhoven T (2016) New directions in nearest neighbor searching with applications to lattice sieving. In: Proceedings of the twenty-seventh annual ACM-SIAM symposium on discrete algorithms (SODA 2016), Arlington, VA, USA, January 10–12 2016, pp 10–24
296. Lamport L (1979) Constructing digital signatures from a one way function. In: SRI international computer science laboratory. Report no SRI-CSL-98, vol 1423, pp 1–7. https://www.microsoft.com/en-us/research/uploads/prod/2016/12/Constructing-Digital-Signatures-from-a-One-Way-Function.pdf
297. Merkle RC (1989) A certified digital signature. In: Conference on the theory and application of cryptology CRYPTO 1989: advances in cryptology-CRYPTO'89. Lecture notes in computer science book series (LNCS), vol 435, pp 218–238
298. Dods C, Smart NP, Stam M (2005) Hash based digital signature schemes. In: 10th proceeding of IMA international conference on cryptography and coding (IMACC 2005), Lecture notes in computer science. Springer, Berlin, vol 3796, pp 96–115
299. Hulsing A (2013) $W-OTS^{+}-$shorter signatures for hash-based signature schemes. In: Proceeding of 6^{th} international conference on cryptology in Africa, Cairo, Egypt, June 22–24, Lecture notes in computer science. Springer, Berlin, Heidelberg, vol 7918, pp 173–188
300. Patarin J (1997) The oil and vinegar signature scheme. Presented at the Dagstuhl workshop on cryptography
301. Ding J, Schmidt D (2005) Rainbow, a new multivariable polynomial signature scheme. In: International conference on applied cryptography and network security—ACNS 2005. Lecture notes in computer science, Springer, vol 3531, pp 164–175
302. Patarin J, Courtois N, Goubin L (2001) QUARTZ, 128-bit long digital signatures, cryptographers track at the RSA conference, CT-RSA 2001: topics in cryptology, CT-RSA2001, Lecture notes in computer science (LNCS). Springer, Berlin, Heidelberg, vol 2020, pp 282–297
303. NIST Post Quantum Cryptography. https://csrc.nist.gov/news/2019/pqc-standardization-process-2nd-round-candidates. 26 Feb 2020
304. Chen L, Jordan S, Liu YK, Moody D, Peralta R, Perlner R, Smith-Tone D (2016) Report on post-quantum cryptography. Report of National Institute of Standards and Technology, US Department of Commerce, NISTIR 8105. https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf
305. EL-Latif A A A, Abd-El-Atty B, Hossain M S, Elmougy S, Ghoneim A (2018) Secure quantum steganography protocol for fog cloud internet of things. IEEE Access 6:10332–10340
306. Amer O, Krawec WO (2019) Semiquantum key distribution with high quantum noise tolerance. Phys Rev A 100:022319-1–022319-16
307. Chun H, Choi I, Faulkner G, Clarke L, Barber B, George G, Capon C, Niskanen A, Wabnig J, O'Brien D, Bitauld D (2017) Handheld free space quantum key distribution with dynamic motion compensation. Opt Express 25(6):6784–6795
308. Nordholt JE, Hughes RJ, Newell RT, Peterson CG, Rosenberg D, McCabe KP, Tyagi KT, Dallman N(2010) Quantum key distribution using card, base station and trusted authority, US Patent, Los Alamos National Security, LLC (Los Alamos, NM) DOE Contract Number AC52–06NA25396
309. Hughes RJ, Nordholt JE, Peterson CG (2010) Secure multi-party communication with quantum key distribution managed by trusted authority, US Patent, Los Alamos National Security, LLC (Los Alamos, NM) DOE Contract Number AC52–06NA25396
310. Battelle (2020) The future of security: zeroing in on un-hackable data with quantum key distribution https://www.wired.com/insights/2014/09/quantum-key-distribution/. Accessed 20 Feb 2020
311. Xue P, Zhang X (2017) A simple quantum voting scheme with multi-qubit entanglement. Sci Rep 7:7586
312. Yin J, Cao Y, Li YH, Liao SK, Zhang L, Ren JG, Cai WQ, Liu WY, Li B, Dai H, Li GB, Lu QM, Gong YH, Xu Y, Li SL, Li FZ, Yin YY, Jiang ZQ, Li M, Jia JJ, Ren G, He D, Zhou YL, Zhang XX, Wang N, Chang X, Zhu ZC, Liu NL, Chen YA, Lu CY, Shu R, Peng CZ, Wang JY, Pan JW (2017) Satellite-based entanglement distribution Over 1200 kilometers. Science 356:1140–1144
313. Liao SK, Cai WQ, Liu WY, Zhang L, Li Y, Ren JG, Yin J, Shen Q, Cao Y, Li ZP, Li FZ, Chen XW, Sun LH, Jia JJ, Wu JC, Jiang XJ, Wang JF, Huang YM, Wang Q, Zhou YL, Deng L, Xi T, Ma L, Hu T, Zhang Q, Chen YA, Liu NL, Wang XB, Zhu ZC, Lu CY, Shu R, Peng CZ, Wang JY, Pan JW (2017) Satellite-to-ground quantum key distribution. Nature 549:43–60
314. Liao SK, Cai WQ, Handsteiner J, Liu B, Yin J, Zhang L, Rauch D, Fink M, Ren JG, Liu WY, Li Y, Shen Q, Cao Y, Li FZ, Wang JF, Huang YM, Deng L, Xi T, Ma L, Hu T, Li L, Liu NL, Koidl F, Wang P, Chen YA, Wang XB, Steindorfer M, Kirchner G, Lu CY, Shu R, Ursin R, Scheidl T, Peng CZ, Wang JY, Zeilinger A, Pan JW (2018) Satellite-relayed intercontinental quantum network. Phys Rev Lett 120:030501-1–030501-4
315. Sharma V, Banerjee S (2019) Analysis of atmospheric effects on satellite-based quantum communication: a comparative study. Quantum Inf Process 18:Article no 67
316. Bedington R, Arrazola JM, Ling A (2017) Progress in satellite quantum key distribution. npj Quantum Inf 3:Article no 30
317. First quantum video call. https://www.innovations-report.com/html/reports/information-technology/austrian-and-chinese-academies-of-sciences-successfully-conducted-first-inter-continental-quantum-video-call.html. Accessed 6 Feb 2020
318. Arrighi P, Salvail L (2006) Blind quantum computation. Int J Quantum Inf 4(5):883–898
319. Broadbent A, Fitzsimons J, Kashefi E (2009) Universal blind quantum computation. In: 50^{th} annual IEEE symposium on foundations of computer science. Atlanta, CA, USA 25–27 Oct, pp 517–526
320. Fitzsimons JF (2017) Private quantum computation: an introduction to blind quantum computing and related protocols. NPJ Quantum Inf 3:23
321. Barz S, Kashefi E, Broadbent A, Fitzsimons JF, Zeilinger A, Walther P (2012) Demonstration of blind quantum computing. Science 335:303–308
322. Greganti C, Roehsner MC, Barz S, Morimae T, Walther P (2016) Demonstration of measurement-only blind quantum computing. New J Phys 18:013020
323. Huang HL, Zhao Q, Ma X, Liu C, Su ZE, Wang XL, Li L, Liu NL, Sanders BC, Lu CY, Pan JW (2017) Experimental blind quantum computing for a classical client. Phys Rev Lett 119:050503
324. Gottesman D, Chuang IL (2001) Quantum digital signatures, p 050503. arXiv.org/abs/quant-ph/0105032
325. Andersson E, Curty M, Jex I (2006) Experimentally realizable quantum comparison of coherent states and its applications. Phys Rev A 74:022304
326. Amiri R, Andersson E (2015) Unconditionally secure quantum signatures. Entropy 17(8):5635–5659

327. Cai XQ, Wang TY, Wei CY, Gao F (2019) Cryptanalysis of multiparty quantum digital signatures. Quantum Inf Process 18(8):252
328. Shi WM, Wang YM, Zhou YH, Yang YG (2018) Cryptanalysis on quantum digital signature based on asymmetric quantum cryptography. Optik 154:258–260
329. Collins RJ, Donaldson RJ, Buller GS (2018) Progress in experimental quantum digital signatures. In: Proceedings of quantum communications and quantum imaging XVI, San Diego, California, United States, p 10771
330. Collins RJ, Amiri R, Fujiwara M, Honjo T, Shimizu K, Tamaki K, Takeoka M, Sasaki M, Andersson E, Buller GS (2017) Experimental demonstration of quantum digital signatures over 43db channel loss using differential phase shift quantum key distribution. Sci Rep 7:3235
331. Donaldson RJ, Collins RJ, Kleczkowska K, Amiri R, Wallden P, Dunjko V, Jeffers J, Andersson E, Buller GS (2016) Experimental demonstration of kilometer-range quantum digital signatures. Phys Rev A 93(1):012329
332. Mirhosseini M, Magana-Loaiza OS, O'Sullivan MN, Rodenburg B, Malik M, Lavery MPJ, Padgett MJ, Gauthier DJ, Boyd RW (2015) High-dimensional quantum cryptography with twisted light. New J Phys 17:033033
333. Canas G, Vera N, Carine J, Gonzalez P, Cardenas J, Connolly PWR, Przysiezna A, Gomez ES, Figueroa M, Vallone G, Villoresi P, Silva TFD, Xavier GB, Lima G (2017) High-dimensional decoy-state quantum key distribution over multicore telecommunication fibers. Phys Rev A 96:022317
334. Ding Y, Bacco D, Dalgaard K, Cai X, Zhou X, Rottwitt K, Oxenlowe LK (2017) High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits. NPJ Quantum Inf 3:25
335. Mower J, Zhang Z, Desjardins P, Lee C, Shapiro JH, Englund D (2013) High-dimensional quantum key distribution using dispersive optics. Phys Rev A 87:062322
336. Brougham T, Barnett SM, McCusker KT, Kwiat PG, Gauthier DJ (2013) Security of high-dimensional quantum key distribution protocols using Franson interferometers. J Phys B At Mol Opt Phys 46(10):104010
337. Brougham T, Wildfeuer CF, Barnett SM, Gauthier DJ (2016) The information of high-dimensional time-bin encoded photons. Eur Phys J D 70:214
338. Islam NT (2018) High-rate, high-dimensional quantum key distribution systems, PhD Thesis, Duke University
339. Islam NT, Lim CCW, Cahall C, Qi B, Kim J, Gauthier DJ (2019) Scalable high-rate, high-dimensional quantum key distribution, pp 1–10. arXiv:1902.00811
340. Chandran N, Goyal V, Moriarty R, Ostrovsky R (2009) Position based cryptography. In: Proceedings of the 29^{th} annual international cryptology conference on advances in cryptology, vol 29. Springer, pp 391–407
341. Chandran N, Fehr S, Gelles R, Goyal V, Ostrovsky R (2010) Position-based quantum cryptography. https://arxiv.org/PS_cache/arxiv/pdf/1005/1005.1750v1.pdf
342. Bilski P, Winiecki W (2013) Analysis of the position-based quantum cryptography usage in the distributed measurement system. Measurement 46(10):4353–4361
343. Buhrman H, Chandran N, Fehr S, Gelles R, Goyal V, Ostrovsky R, Schaffner C (2014) Position-based quantum cryptography: impossibility and constructions. SIAM J Comput 43(1):150–178
344. Chakraborty K, Leverrier A (2015) Practical position-based quantum cryptography. Phys Rev A 92:052304
345. Sibson P, Erven C, Godfrey M, Miki S, Yamashita T, Fujiwara M, Sasaki M, Terai H, Tanner MG, Natarajan CM, Hadfield RH, O'Brien JL, Thompson MG (2017) Chip-based quantum key distribution. Nat Commun 8:13984
346. Roger T, Paraiso T, Marco ID, Marangon DG, Yuan Z, Shields AJ (2019) Real-time interferometric quantum random number generation on chip. J Opt Soc Am B 36(3):B137–B142
347. Zhang G, Haw JY, Cai H, Xu F, Assad SM, Fitzsimons JF, Zhou X, Zhang Y, Yu S, Wu J, Ser W, Kwek LC, Liu AQ (2019) An integrated silicon photonic chip platform for continuous-variable quantum key distribution. Nat Photonics 13:839–842
348. Blum M (1981) Coin flipping by telephone. CRYPTO, pp 11–15
349. Molina-Terriza G, Vaziri A, Ursin R, Zeilinger A (2005) Experimental quantum coin tossing. Phys Rev Lett 94:040501
350. Colbeck R (2007) An entanglement-based protocol for strong coin tossing with bias 1/4. Phys Lett A 362:390–392
351. Spekkens RW, Rudolph T (2001) Degrees of concealment and bindingness in quantum bit commitment protocols. Phys Rev A 65:012310
352. Toshiba (2020) https://www.toshiba.eu/pages/eu/cambridge-research-laboratory/quantum-key-distribution/. Accessed 18 Feb 2020
353. QuantumCTek (2020). http://www.quantum-info.com/english/. Accessed 18 Feb 2020
354. ID Quantique SA, Switzerland (2020). www.idquantique.com. Accessed 18 Feb 2020
355. Cerberis (2020). https://www.idquantique.com/quantum-safe-security/products/cerberis3-qkd-system/. Accessed 18 Feb 2020
356. Boaron A, Boso G, Rusca D, Vulliez C, Autebert C, Caloz M, Perrenoud M, Gras G, Bussieres F, Li MJ, Nolan D, Martin A, Zbinden H (2018) Secure quantum key distribution over 421 km of optical fiber. Phys Rev Lett 121:190502
357. Travagnin M, Lewis A (2019) Quantum key distribution in-field implementations. JRC Technical Reports, pp 1–41
358. Yuan Z, Plews A, Takahashi R, Doi K, Tam W, Sharpe AW, Dixon AR, Lavelle E, Dynes JF, Murakami A, Kujiraoka M, Lucamarini M, Tanizawa Y, Sato H, Shields AJ (2018) 10-Mb/s quantum key distribution. J Lightwave Technol 36(16):3427–3433
359. Broadbent A (2018) How to verify a quantum computation. Theory Comput 14(11):1–37
360. Gheorghiu A, Kashefi E, Wallden P (2015) Robustness and device independence of verifiable blind quantum computing. New J Phys 17(8):083040
361. Klarreich E (2018) Graduate student solves quantum verification problem. QuantaMagazine