Review

A Survey on Quantum Cryptography, its Protocols, Applications, and Challenges

Noman Minhas *

Posted Date: 6 August 2024

doi: 10.20944/preprints202408.0333.v1

Keywords: Quantum Cryptography; Quantum Key Distribution; Quantum Secure Direct Communication; Deterministic Quantum Secure Communication

Review

A Survey on Quantum Cryptography, Its Protocols, Applications, and Challenges

Noman Nasir Minhas

Department of Cyber Security, Air University; contact.nomanminhas@gmail.com; Tel.: +92-306-055-3656

Abstract: This paper focuses on the concepts used in Quantum Cryptography and recent progress made. We look at the different categories of key distribution protocols that have been proposed and issues related to those. We then take an overview of two main approaches of communication using quantum cryptography concepts, i.e., "Quantum Secure Direct Communication" and "Deterministic Secure Quantum Communication", and limitations related to the usage of these schemes in a real-world system. At last, we list down the problems identified in the research and conclude our discussion by proposing areas of focus for future research.

Keywords: quantum cryptography; quantum key distribution; quantum secure direct communication; deterministic quantum secure communication

1. Introduction

Cryptography is an essential element of network communication. Every message communicated over a network uses one type of cryptographic algorithm or another. These algorithms have evolved from shift and transposition schemes to much complex schemes like DES, 3DES, AES, and digital signatures like RSA and RSA-FDH. At the same time computing power has also expanded exponentially, which poses a potential threat to these algorithms. In order to mitigate these threats, cryptography first moved to cipher machines instead of manual encryption, then incorporated mathematically complex algorithms including Symmetric and Asymmetric schemes. The most recent advance in this regard came from the use of quantum mechanics concepts for cryptography which is known as Quantum Cryptography (QC).

1.1. Research Questions

This paper aims to seek answers to the following questions.

- What are the basic ideas behind QC?
- How QC provides security over classic cryptography?
- What are the major applications areas of QC?
- What are the important categories of key distribution protocols used in QC?
- How can QC be used for secure communication?
- What are the issues faced in using QC schemes in the real-world?
- What are the security attacks possible on different QC protocols and schemes?

1.2. Research Objectives

This paper aims to achieve the following objectives from the conducted research.

- To have a clear understanding of concepts that constitute QC.
- To identify applications of QC for secure communication.
- To get an overview of recent advances in the QC domain and its sub-domains.
- To get brief technical details of protocols and schemes used in QC.
- To identify security issues and comprehend the threat surface of current advancements in QC.
- To identify limitations and hurdles faced in implementing QC in practical systems.

2. Quantum Cryptography

2.1. Overview

Quantum Cryptography (QC) uses concepts of encryption and Physics at the same time. It leverages the quantum mechanics branch of Physics for cryptographic purposes by using all quantum states of the system. This approach is different from the classic and post-quantum cryptographic schemes as it uses concepts of quantum mechanics for cryptographic operations instead of using complex mathematical algorithms for the same purpose. This unique approach makes QC resistant to computer attacks, both classic and quantum computers, because QC uses mathematics and hence can not be broken by conventional computational attacks. Moreover, the use of QC also makes undetected eavesdropping impossible due to concepts of uncertainty and the non-cloning of information in quantum mechanics.

2.2. Related Terms

Following are some of the terms which will often be encountered when studying Quantum Cryptography and hence need to be defined briefly.

- Quantum Cryptography (QC): It is a cryptographic domain that uses concepts of quantum mechanics for encryption processes instead of relying on mathematical complexities.
- Quantum Key Distribution (QKD): It is a protocol for key distribution between parties by using the non-cloning principle of the non-orthogonal single quantum state. It ensures that the process of key distribution is free from undetected eavesdropping.
- Quantum Secure Direct Communication (QSDC): It is a QC scheme used for communication without using any key or data exchange for establishing the channel.
- Deterministic Secure Quantum Communication (DSQC): It is a QC scheme that requires the exchange of one classical bit for each qubit for communication.
- Quantum Entanglement: It is a quantum phenomenon through which two particles are connected to each other such that the state of one particle can be predicted by observing the state of the other one.

2.3. Notable Protocols

Quantum Key Distribution Protocols (QKDPs) are mainly of two types, i.e., Discrete Variable (DV) and Continuous Variable (CV) QKDPs. Discrete Variable QKDPs use the spin of an electron or polarization of a single photon for key distribution purposes, which produces discrete results. While CV-QKDPs use light for storing information which has an advantage because coherent light is easy to produce than a single proton used in Discrete Variable QKDPs[1]. DV protocols use single photons, while CV protocols employ homodyne or heterodyne detection mechanisms. [2].

2.3.1. Discrete Variable QKDPs

Some protocols of this type are

- BB84 Protocol: Proposed by Bennett and Brassard in 1984, it uses the polarization state of a single photon to encode individual bits of the key.
- E91 Protocol: Proposed in 1991, E91 distributes Bell states emitted from a common Spontaneous Parametric Down-Conversion(SPDC) source from which the parties randomly choose polarization bases.
- B92 Protocol: It uses orthogonal states for representing both states of a bit i.e., 0,1. It can also be applied to CV-QKPDs as well but is less secure than B92. [3]
- SARG04: It is very similar to BB84 as both have the same quantum state transmission phase and measurement phase. The main difference is the classical post-processing phase of both protocols, and SARG04 is more secure than BB84 as it is secure even when two photons are emitted by the source. [4]

2.3.2. Continuous Variable QKDPs

Besides of usage of B92 Protocol as CV-QKPDs, there is a number of other protocols as well. Some of those are

- Ralph [5] proposed two different schemes of CV-QKPDs based on their source state i.e., Coherent and Squeezed, where the Coherent state corresponds to a state without quadrature and Squeezed state is the one with one quadrature having very high variance and the other one very low.
- Another protocol, an analog of BB84, was proposed by Hillery [6], which used the light in the squeezed state.
- In 2009, another CV-QKPD was proposed [7], which was based on the squeezed state of light, but a heterodyne detection mechanism was used for greater security against noisy transmission lines.
- Another unique approach was adopted by Leverrier and Grangier [8] in 2010, proposing two schemes that used two-state protocol and coherent states for discrete modulation. [3]

Besides Discrete Variable and Continuous Variable, there are other classes of QCKDPs as well; some of those are:

2.3.3. Distributed Phase Reference QKDPs

These protocols use sequential pulses in a coherent manner. It encodes information in the phase or arrival time of photons between adjacent pulses. There are two important protocols of this class which are [9]

- Coherent-One-Way (COW) protocol
- Differential-Phase-Shift (DPS) protocol
- Round-Robin Differential Phase Shift (RRDPS) protocol

2.3.4. Two-Way Protocols

These protocols initialize with Alice sending states to Bob over an insecure quantum channel; Bob does encoding on these states and sends them back to Alice, where he performs measurements on these encoded states sent from Bob. Hence these protocols are referred as "Two-Way" Protocols [10]. Some of these protocols are

- Super-Dense Coding (SDC) or also known as the "Ping-Pong" Protocol
- LM05 Protocol

3. Issues in Quantum Cryptography Key Distribution Protocols

Although QC provides a formidable encryption method, it is still in its infancy stage, and there remain multiple challenges in implementing it practically over large networks besides some theoretical issues. It is challenging to get practical key exchange rates over large distances besides the high cost associated with deploying QKD-based systems. Moreover, DV-QKDPs use polarization pulses stimulating true single-photon states, which need single-photon sources and detectors that are more difficult to build. On the other hand, although DPR protocols are generally tolerant to “Photon-Number Splitting” (PNS) attacks, DV protocols are still susceptible to these attacks, and this forms one of the major limitations of these protocols.[2]

Quantum Cryptography is also susceptible to different types of attacks that can be categorized mainly into three categories on the basis of preparation, interaction, and measurement of qubits.

- **Individual Attacks:** These are the most applicable attacks in the context of technology available till now. It requires the attacker to prepare ancilla qubits and interact with each qubit on the channel independently, as well as measure them individually.
- **Coherent Attacks:** The Attacker prepares an entangled state of all ancilla qubits and also interacts as well measures the qubits and ancilla qubits collectively.

- **Collective Attack:** It is a sub-class of Coherent Attacks, where preparation of ancilla qubits and interaction with qubits on the channel is done individually, but measurement of all ancilla qubits is done collectively.[1]

Furthermore, there is an entire category of attacks called “Side-Channel Attacks” (SCAs) which take advantage of the gaps that exist between the theory and implementation of QKD. These attacks can be launched at multiple points, including source, detector, and even at the physical implementation of post-processing steps. For example, when multiple laser sources are used introduces a vulnerability while distinguishing the sources, and here spectral, temporal, and spatial distinction of sources can be exploited to launch soft channel attacks.[11]

One type of SCAs is called “Trojan Horse Attack” (THA), which obtains information about quantum signals by injecting and analyzing the reflected-back light from the transmitter. Although it is not considered a real security threat, it does negates the purpose of the secrecy of QC [12]. In 2019, an attack was demonstrated called the "Laser-Seeding" attack, which controlled the light emission from the laser diode being used for transmission in the QKD system. It uses, controls, and manipulates the laser diode directly and tries to increase the intensity of quantum states, which makes it more efficient than THA[13].

There are other attacks that can be launched on QC, like “Faked State Attacks” (FSA) or also known as the Quantum MITM attacks. It is an “Intercept-and-Resend” (IR) attack that uses light pulses to give both parties quantum states that they think of as origin without them knowing. This attack gives full knowledge of the key to the attacker, which compromises the channel eventually. An Attacker can use multiple wavelength pulses to exploit reflection and transmission coefficients and sensitivity of the detector more efficiently. The effectiveness of this attack depends upon the attacker’s ability to stage attacks on the apparatus being used in communication, the ability to tap the idle optical quantum channel, the time difference between transmission and communication between parties, and whether there is a monitoring mechanism present on the target equipment.[14]

Another attack that is very common in QC is called “Photon-Number-Splitting” (PNS) attack. This attack becomes significantly effective when coherent states are introduced to multi-photonic pulses and can result in the breaking of the key. This type of attack is reasonably strong against QKDPs, which use single photon sources like BB84 protocol.[15] In PNS, if an eavesdropper detects a single photon, it either blocks the channel or launches a perturbs the single state. In case of more than photons, the eavesdropper stores a part of it in quantum memory and redirects the rest to the receiver.[16]

A technique called “Decoy State Method” (DSM) can be used to detect a PNS attack, and this technique is accepted widely to prove the secrecy of QC, but this method can also be evaded through different attacks. One of these attacks is known as Beam Splitting (BS) attack, and the decoy-state method turns out to be insensitive to it. In this attack, the attacker splits the beam or channel into two parts. One part of the coherent state is directed towards quantum memory, and the other is transmitted to the receiver with low loss or, ideally, lossless. The attacker then waits for disclosure of the bases and uses the state in quantum memory to perform measurements and intrude into the channel.[16]

4. Quantum Secure Direct Communication

Although QC successfully counters the problems of the conventional cryptography, but we still use key distribution mechanisms in QC, which provide a credible threat surface to attackers. Hence in 2000, “Quantum Secure Direct Communication” (QSDC) scheme was initially proposed by using “Einstein-Podolsky-Rosen” (EPR) pairs [17]. QSDC overcomes the attack surface of QCKDPs by communicating directly without using key distribution and hence further eliminates loopholes in ciphertext attacks and key storage [18].

The non-existence of a cryptographic key makes the channel open, and an attacker can cut through the quantum channel; therefore, communicating parties need to verify the reliability of the transferred data. For this purpose, both parties perform different probabilistic tests. QDSC is achieved by going through two steps; where the first one is distributing quantum carriers between parties, and classical info is encoded, transmitted, and decoded. An attacker needs to have access to both stages in order to access the actual information transmitted; otherwise, at most, he will end up decoding random messages. QSDC has protocols of its own which include but is not restricted to "Ping-Pong" (PP), "Two Step" (TS), and "Deng Fu-Guo and Long Gui Lu" (DL), also known as Quantum OTP Protocols [19].

There are different approaches that can be used to achieve QSDC, and each approach tries to solve different challenges in implementing QDSC. One method that we saw earlier was the DSM which uses "Weak-Coherent Pulses" (WCPs) of multiple intensities to estimate the contribution of single-photon pulses. The proposed two-decoy-state was demonstrated to make its implementation easy and to outperform the four-decoy-state over large distances while improving secrecy capacity as well secure distance at the same time by using a Genetic Algorithm to perform parameter optimization [20].

Another approach, called "Measurement-Device-Independent" (MDI) QSDC, is used to mitigate detector SCAs by using a third party that is responsible for performing all measurements with imperfect measurement devices. User Identity Authentication can also be used with approach, and it ensures secrecy against common attacks [21]. Similarly, an approach was proposed recently proposed [22], which is based on single particles. It uses Z Pauli Operation instead of Y for encoding messages without changing the polarization of the particle, which makes it easier to implement. This further bridges the gap between the theory and implementation of the QSDC. This scheme is resistant to undetected measurement attacks, IR attacks, and entangle-and-measure (EM) attacks.

As QSDC is still in its infancy stage hence transmitting messages over large distances still remains a challenge. But recently, it was demonstrated [23] that QSDC can be achieved in distances over 100km fiber using phase states and photonic time-bin states. It enables ultra-low "Quantum Bit Error Rate" (QBER) by avoiding phase and polarization drift. It also proposed a design of a "Quantum-Memory-Free" (QMF) QSDC scheme, and its results depicted extreme resistance to losses. Besides QSDC, some CQKDPs have achieved a distance of 421km [24] and even as long as 1,120km [25] for key distribution purposes. These schemes can help to achieve QSDC over such and even larger distances as well.

Moreover, another scheme was proposed that aimed at reducing resource usage in a multi-user quantum network. This built a "QSDC network using Switches" (QNUS) and enabled switchover capability for links, and used quantum routers and transceivers. The proposed scheme reduces the number of transceivers to half of the networks without optical switches [26].

To overcome the possible issues in QSDC like detector efficiency mismatch, source imperfection, and side-channel effects, a generic security framework was proposed in 2021 [27] to fill the gap between protocols and their practice. This framework proposes a generic QSDC protocol and constructs the framework on top of it, and then further optimizing methods are applied to bridge the target gap. This framework can be generalized by using the statistical method and aims to ensure the forward channel secrecy. This framework can be considered as significant progress in mainstreaming QSDC as it reduces the gaps in the implementation of the concepts.

5. Deterministic Secure Quantum Communication

Quantum Cryptography has another important application known as "Deterministic Secure Quantum Communication" (DSQC), which allows the receiver to read the message only after one-bit additional transmission of classical nature for each qubit. It is in contrast to the QSDC mechanism, which does not require any such operation and can directly transmit data between parties. The first significant DSQC scheme was proposed in 1999, which used "Bell-basis measurement", followed by two notable schemes in 2002, one of which was based on the two-qubit state of single-photon and the other was based on entangled pairs. Further DSQC schemes were proposed in 2004 and 2005, which were based on EPR pairs and entanglement swapping, respectively. A novel approach was found when different semi-quantum DSQC protocols were proposed as well, allowing part of the users to remain classical. Another class of DSQC protocols was proposed, which used high-dimensional systems, freedom of photons, data block transmission, order rearrangement, EPR pairs, single photons, W class states, cluster state, polarization-spatial-mode (PSM) degree of freedom, and many more.

In 2017, a DSQC protocol was proposed, which used a single d-level system that utilized photon sequence as a message carrier. In this protocol, Alice and Bob use forward and backward transmission, respectively, to ensure the security of the channel. Any eavesdropper will be detected by the affected error rate. Moreover, the use of a higher dimension system gives this protocol higher security and efficiency against IR attacks than single photon DSQC protocols. Moreover, any THA will also be detected as any such attack will increase the multi-photon rate significantly [28].

Another research conducted in 2017 proposed a robust deterministic communication in a lossy channel which can be used for establishing a key or direct communication as well. It used a two-way six-state scheme which ensured that no information was leaked before the public discussion took place, even if an attacker measured and prepared all the qubits. This protocol ensures security against PNS attacks without using the DSM, although this method can be integrated with this protocol by making some modifications. This scheme also does not need quantum memory, which needs near absolute temperature, which is not a feasible option. This protocol, called SQ16, ensures security against zero-quantum bit error rate (PNS) attacks when photons emitted from a pulse are less than or equal to four [29].

Another protocol was proposed later, which used four-qubit GHZ states, which not only had a high capacity for communication, but also used all of the quantum resources, which maximizes the efficiency of communication whose value is 100% theoretically speaking. Furthermore, this protocol also uses a three-step strategy and decoy photon detection, which provides protection against any eavesdropping. In order to steal some information, the attacker must capture three sub-sequences for manipulation, and he can not adopt only one IR attack. This scheme ensures efficient and secure communication, but it faces problems when it is implemented in a noisy channel; therefore, we need to implement entanglement purification and concentration techniques to perform amplification and reduce loss, respectively, to ensure the smooth working of this protocol [30].

To provide security against third-party intervention, a scheme was proposed in 2020, which was based on the BB84 system and included “Quantum Entity Authentication” (QEA), providing security against IR attacks as well as EM attacks. By using sufficient authentication/verification and source pairs, all IR and EM attacks can be detected with 100% certainty. This protocol uses a non-entangled, single-photon stream for efficiency, and this scheme also remains feasible in a lossy channel. It also proposes multiple generations and shuffling techniques as step-0 for message loss prevention [31].

To mitigate the challenge of polarization (which is used by most protocols for encoding) degradation of photons over large distances, a spatial encoding based scheme was proposed. It uses the decoy photon approach to ensure the security of the protocol. This protocol is credibly resistant to IR attacks as well as EM attacks. Although this protocol may be susceptible to Trojan Attacks, it can be resisted by using PNS and wavelength quantum filters [32].

Another recent scheme aims to improve the efficiency of communication and remove the detector side channels in DSQC by using a method similar to MDI-QKD. This protocol is based on 16 PSM hyperencoded qudit and seven hyperentangled states. This protocol proves to be more efficient and less resource-consuming than QSDC as it uses the classical resource and increases the bit rate and security of the channel. In order to avoid unambiguous identification of some of the hyperentangled Bell states, cross-Kerr non-linearity are used to distinguish all Bell states [33].

6. Analysis and Future Work

After going through different QC protocols for communication and key distribution, we can draw the following structure of QC.

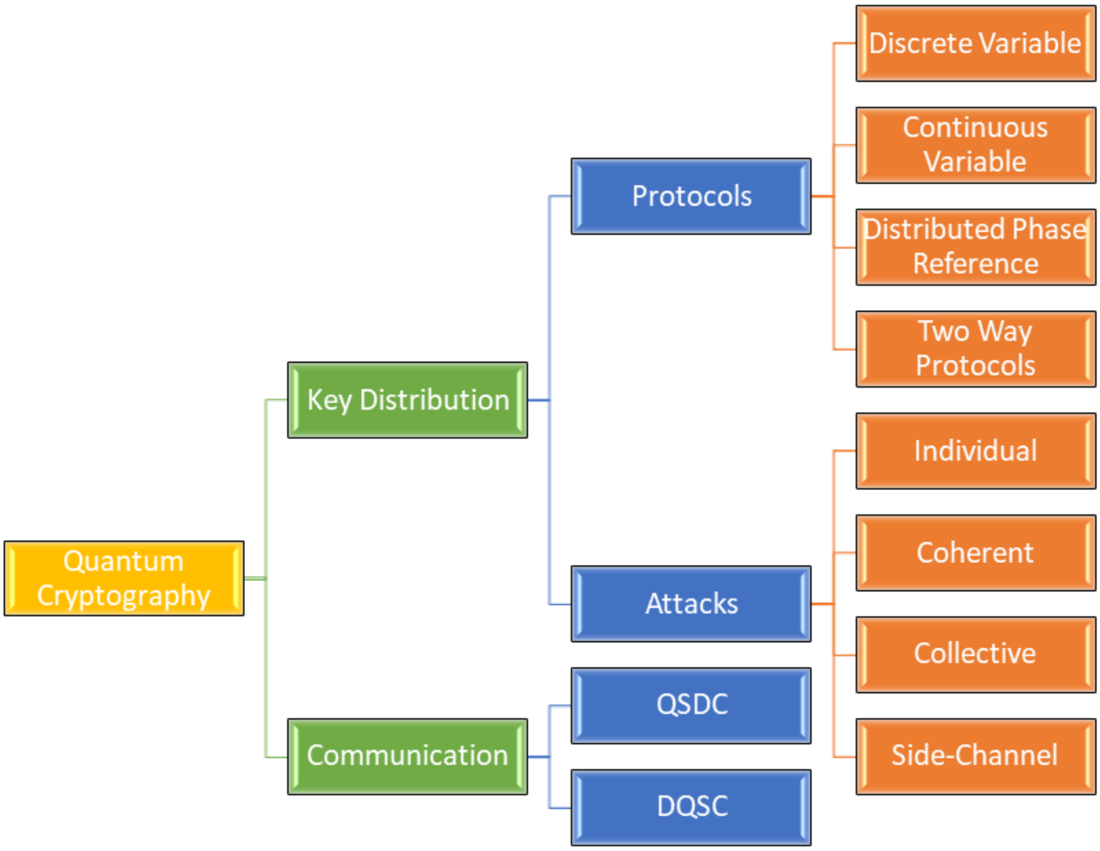

Figure 1. Overview of Quantum Cryptography

Quantum Cryptography has two main applications, namely Key Distribution and Communication. QCKD Protocols use quantum mechanics concepts only for generating a key which is then used with classic cryptographic schemes. QCKDPs can be classified into DV, CV, DPR, and Two-Way categories. These protocols provide security for the key and not for the communication that is taking place over the channel. We saw that QCKDPs could also have multiple attacks, and communication can still be compromised. To overcome these issues with keys, we avoid using keys at all, and quantum concepts are applied to the actual communication over the channel. There are two major approaches for this area which are QSDC and DSQC. QSDC does not require any type of preliminary steps and can establish communication directly, while DSQC needs one classic bit transfer for each qubit for communication.

6.1. Issues in Quantum Cryptography

After the above discussion, we can come up with two categories of issues that we face in the wide use of QC

6.1.1. Practical Issues in QC

Although several protocols have been proposed and are mature enough for use in a real-world application, it is the practical issues that are the biggest challenge to using QC schemes in general. The issues discussed below are in the context of currently demonstrated technological developments in quantum cryptography only and have been identified in lab environments. It does not consider problems that might be considered when QC is used in real-world, large-scale systems. These issues can be listed as

- Noisy Channels prevent transmission over large distances.
- Quantum devices are much more expensive than classic ones.
- Detector Efficiency mismatch, source imperfection, and side-channel compromise the security of the quantum channel.
- Some QC schemes require quantum memory, which requires a temperature near to absolute zero, which is very infeasible.

6.2. Security Issues in QC

Besides practical issues, there are other security issues as well which can occur when using QC like

- Side-Channel vulnerabilities can be used to launch attacks like THA, IR, PNS, EM, and ciphertext attacks.
- A Laser-Seeding attack can be used to control the laser diode directly for intensifying quantum states.

7. Future Research and Conclusion

Although QC protocols still need focus to mitigate their security issues, but our main focus should be on solving issues faced in implementing QCKDPs, QSDC, and DSQC, which will not only spread the use of QC but will also test the limits of QC protocols and help to increase their maturity.

To conclude our discussion, we can state that QC is manifold secure than classic cryptography and have many applications in key distribution and communication. But we still need to work more on integrating the QC schemes with current systems easily and economically. This will enhance the security of cryptographic applications significantly.

Funding: This research received no external funding.

Data Availability Statement: Not Applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kumar, A.; Garhwal, S. State-of-the-Art Survey of Quantum Cryptography. *Archives of Computational Methods in Engineering* **2021**, *28*, 3831–3868.
2. Sekga, C.; Mafu, M. Security of quantum-key-distribution protocol by using the post-selection technique. *Physics Open* **2021**, *7*, 100075.
3. Bouwmeester, D.; Zeilinger, A. The physics of quantum information. In *The physics of quantum information*; Springer, 2000; pp. 1–14.
4. Fung, C.H.F.; Tamaki, K.; Lo, H.K. On the performance of two protocols: SARG04 and BB84. *arXiv preprint quant-ph/0510025* **2005**.
5. Ralph, T.C. Continuous variable quantum cryptography. *Physical Review A* **1999**, *61*, 010303.
6. Hillery, M. Quantum cryptography with squeezed states. *Physical Review A* **2000**, *61*, 022309.
7. García-Patrón, R.; Cerf, N.J. Continuous-variable quantum key distribution protocols over noisy channels. *Physical Review Letters* **2009**, *102*, 130501.
8. Leverrier, A.; Grangier, P. Continuous-variable quantum key distribution protocols with a discrete modulation. *arXiv preprint arXiv:1002.4083* **2010**.
9. Li, J.; Li, N.; Zhang, Y.; Wen, S.; Du, W.; Chen, W.; Ma, W. A survey on quantum cryptography. *Chinese Journal of Electronics* **2018**, *27*, 223–228.
10. Beaudry, N.J.; Lucamarini, M.; Mancini, S.; Renner, R. Security of two-way quantum key distribution. *Physical Review A* **2013**, *88*, 062302.
11. Arteaga-Díaz, P.; Cano, D.; Fernandez, V. Practical side-channel attack on free-space QKD systems with misaligned sources and countermeasures. *IEEE Access* **2022**, *10*, 82697–82705.
12. Navarrete, Á.; Curty, M. Improved finite-key security analysis of quantum key distribution against Trojan-horse attacks. *Quantum Science and Technology* **2022**.

13. Huang, A.; Navarrete, Á.; Sun, S.H.; Chaiwongkhot, P.; Curty, M.; Makarov, V. Laser-seeding attack in quantum key distribution. *Physical Review Applied* **2019**, *12*, 064043.
14. Fei, Y.Y.; Meng, X.D.; Gao, M.; Wang, H.; Ma, Z. Quantum man-in-the-middle attack on the calibration process of quantum key distribution. *Scientific reports* **2018**, *8*, 1–10.
15. Abdulqadir, D.F.; Mustafa, O.S.; Yousef, A.H. Photon-number Splitting Attack on SARG04 Protocol: An Extended Work. *Polytechnic Journal* **2020**, *10*, 157–162.
16. Molotkov, S.; Kravtsov, K.; Ryzhkin, M. Are there enough decoy states to ensure key secrecy in quantum cryptography? *Journal of Experimental and Theoretical Physics* **2019**, *128*, 544–551.
17. Long, G.L.; Liu, X.S. Theoretically efficient high-capacity quantum-key-distribution scheme. *Physical Review A* **2002**, *65*, 032302.
18. Qi, R.; Sun, Z.; Lin, Z.; Niu, P.; Hao, W.; Song, L.; Huang, Q.; Gao, J.; Yin, L.; Long, G.L. Implementation and security analysis of practical quantum secure direct communication. *Light: Science & Applications* **2019**, *8*, 1–8.
19. Zawadzki, P. Advances in quantum secure direct communication. *IET Quantum Communication* **2021**, *2*, 54–62.
20. Liu, X.; Li, Z.; Luo, D.; Huang, C.; Ma, D.; Geng, M.; Wang, J.; Zhang, Z.; Wei, K. Practical decoy-state quantum secure direct communication. *Science China Physics, Mechanics & Astronomy* **2021**, *64*, 1–8.
21. Das, N.; Paul, G. Measurement-Device-Independent Quantum Secure Direct Communication with User Authentication. *arXiv preprint arXiv:2202.10316* **2022**.
22. Qin, H.; Sun, W.; Tang, W.K. Quantum secure direct communication based on single particles. *Optical and Quantum Electronics* **2022**, *54*, 1–11.
23. Zhang, H.; Sun, Z.; Qi, R.; Yin, L.; Long, G.L.; Lu, J. Realization of quantum secure direct communication over 100 km fiber with time-bin and phase quantum states. *Light: Science & Applications* **2022**, *11*, 1–9.
24. Boaron, A.; Boso, G.; Rusca, D.; Vulliez, C.; Autebert, C.; Caloz, M.; Perrenoud, M.; Gras, G.; Bussières, F.; Li, M.J.; others. Secure quantum key distribution over 421 km of optical fiber. *Physical review letters* **2018**, *121*, 190502.
25. Yin, J.; Li, Y.H.; Liao, S.K.; Yang, M.; Cao, Y.; Zhang, L.; Ren, J.G.; Cai, W.Q.; Liu, W.Y.; Li, S.L.; others. Entanglement-based secure quantum cryptography over 1,120 kilometres. *Nature* **2020**, *582*, 501–505.
26. Niu, P.H.; Zhang, F.H.; Chen, X.W.; Wang, M.; Long, G.L. QNUS: Reducing Terminal Resources in Quantum Secure Direct Communication Network Using Switches. *Quantum Engineering* **2022**, *2022*.
27. Ye, Z.D.; Pan, D.; Sun, Z.; Du, C.G.; Yin, L.G.; Long, G.L. Generic security analysis framework for quantum secure direct communication. *Frontiers of Physics* **2021**, *16*, 1–9.
28. Jiang, D.; Chen, Y.; Gu, X.; Xie, L.; Chen, L. Deterministic secure quantum communication using a single d-level system. *Scientific Reports* **2017**, *7*, 1–11.
29. Qaisar, S.; Jeong, Y.; Shin, H.; others. Practical deterministic secure quantum communication in a lossy channel. *Progress of Theoretical and Experimental Physics* **2017**, *2017*.
30. Yuan, H.; Song, J.; Liu, X.Y.; Yin, X.F. Deterministic secure four-qubit GHZ states three-step protocol for quantum communication. *International Journal of Theoretical Physics* **2019**, *58*, 3658–3666.
31. Jeong, Y.C.; Ji, S.W.; Hong, C.; Park, H.S.; Jang, J. Deterministic secure quantum communication on the bb84 system. *Entropy* **2020**, *22*, 1268.
32. Li, J.; Yang, Y.G.; Li, J.; Wang, Y.C.; Yang, Y.L.; Zhou, Y.H.; Shi, W.M. Deterministic secure quantum communication based on spatial encoding. *Quantum Information Processing* **2022**, *21*, 1–12.
33. Yang, Y.G.; Dong, J.R.; Yang, Y.L.; Li, J.; Zhou, Y.H.; Shi, W.M. High-capacity measurement-device-independent deterministic secure quantum communication. *Quantum Information Processing* **2021**, *20*, 1–19.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.