International Journal on Engineering Technologies and Informatics

The Efficiency of Modern Quantitative Secure Direct Encryption Algorithms in Threat Detection and Prevention

Review Article

Volume 3 Issue 3- 2022

Author Details

*Asia Othman Aljahdali *, Nouran Nassibi, and Manal Alshahrani*

College of Computer Science and Engineering, University of Jeddah, Saudi Arabia

*Corresponding author

Asia Othman Aljahdali, Nouran Nassibi College of Computer Science and Engineering, University of Jeddah, Saudi Arabia

Article History

Received: October 15, 2022 Accepted: : October 18, 2022 Published: October 19, 2022

Abstract

Quantum Secure Direct Communication (QSDC) is one of the newest fields in the technology world today. It is a new research direction in quantum cryptography. Due to its great importance and role in providing reliable communications, it has been constantly striving to find the best protocols and algorithms that would increase the level of confidentiality in communications that take place and work to increase reliability and efficiency as much as possible. Many security vulnerabilities can appear in this type of communication, which causes them to be exposed to various and varied eavesdropping attacks. This research paper is presenting a comprehensive study that dealt with quantitative secure direct communication and its importance, as it presents three of the most recent algorithms in this field, as well as discusses the most prominent threats to security within the environments of such communications of loopholes that allow intruders to eavesdrop and break the confidentiality and security of these protocols. The performance of these algorithms is analyzed and the security holes they addressed were identified, and the types of attacks that succeeded in addressing, detecting, and preventing them.

Keywords: Attack; Detection; Prevention; Quantum secure direct communication

Abbreviations: QSDC: Quantum Secure Direct Communication; QKD: Quantum key communication; CSS: Calderbank-Shor-Steane; DSQC: Deterministic protocols for secure quantum communication; EPR: Einstein's, Podolsky-Rosen; SPM: Single Photon Memory;

Introduction

For decades, the issue of security has been the most attracted attention due to its importance, sensitivity, and extent of its role in various fields, especially technology communications. Our current era is the age of wide networks, massive communications, conducting business and exchanging information completely electronically using various computer networks. This reality and the features of technology that invaded our planet, especially in the past few decades, imposed many procedures and processes in order to ensure the confidentiality and integrity of information and to preserve the validity of the data transmitted electronically. Quantum Secure Direct Communication (QSDC) is one of the different types of quantum communication methods. Additionally, it is one of an important quantum cryptography branch that has the ability to transmit secret messages directly over a quantum channel. QSDC reduces the couple stages process of other communications into a single quantum communication [1]. It does not require the prior existence of a private code or key between the two terminals for secure communication. In addition, it could avoid the leakage of information transmitted before the detection of Eve. It also offers site protection of the communication parties (Alice and Bob), as well to the transmission security, as there is no exchange of key between the quantum terminal and the classical terminal. Also, it could be a cryptographic basic for other cryptographic protocols such as quantum signature, quantum dialogues and quantum direct secret sharing. The other scheme that has been studied by many groups [2-12] is Quantum secure direct communication (QSDC) which transmit the secret message directly without generating the private key first, that is what distinguished it from QKD, and then encrypt the secret message and then send the cipher text by classical communication. The study investigates the most recent security models that were proposed in the field of quantum information science and gives a scientific comparison and analysing of the quality and effectiveness of each of these algorithms in providing a secure, confidential, robust, and effective transmission system.

Quantum decure direct communication

Quantum key communication (QKD) was proposed by Beenetand brassard in 1984[2]. It was the first protocol in Quantum communication series, providing unconditionally secure key exchange, attracting a widespread attention, and progressing quickly in the last two decades. Quantum secure direct communication (QSDC) is known to be an important branch of quantum communication that provides reliable communication and the ability to send covert messages directly over a quantum channel. It can also be considered a complete quantum communication protocol and does not require a separate secret key negotiation phase. In contrast, Quantum Key Distribution (QKD) counterpart is a covert key negotiation protocol, which must be followed by a separate classic communication session. However, the original mass-based data transfer required quantum memory [3]. Many years later, several other quantum cryptography concepts have been proposed such as the one proposed in [13] which is performed well within quantitative communication networks and trust management. [13] touched on the state of research in theory and technology in quantum communication and the quantum communications network. Trust management is considered an essential and important task for quantitative secure communication, and is not just a simple security issue, the fundamentals of trust management in quantitative communication networks have been discussed in [13] and their importance are demonstrated in an accurate manner. A comparison was made with other techniques and theories in quantum communication, the from comparison reveals that the quantum communication trust and the model provided for trust management in the quantum communication network environment is still in its initial stage. The study in [13] provides a classification of the basic techniques used to create reliable and secure quantum communication networks. It also discusses the range of fields, trends, and potential approaches for each direction in managing the confidence of the quantum communication network in a deep and accurate degree. Finally, the study emphasized the importance of following up with the theoretical and practical study of quantum communication networks and developing them to be of the highest safety and reliability. The study also predicts that quantitative communication will exceed the thresholds of classical communication technology in aspects of communication security, measurement accuracy and channel capacity, computing power, and information transmission, and that it will become the new and dominant trend in the field of communications and information in the twenty-first century.

Xiangfu Zou in [14] illustrates how the Quantum Calderbank-Shor-Steane Error Correction Code (CSS) is a weak scheme and cannot stand and resist the attack of the man in the middle. The study proposed an improved QSDC diagram based on quantum CSS debugging codes. The improved scheme demonstrates its ability to withstand man-in-the-middle attacks, and the security of an enhanced QSDC scheme incorporates a perfect noise-free channel. The proposed system is efficient in resisting the attack without eavesdropping.

Jian-Yong Hu et al [15] Leveraged and used the DL04 protocol to provide an experimental demonstration of quantitative secure direct communication, particularly quantum communication related to quantitative dialogue and quantitative authentication. The DL04 protocol is equipped with a single photon frequency coding which provides a clear demonstration of how the block is being transmitted. In the experiment, 16 different frequency channels were introduced, meaning that the information was transmitted directly by the binary number of four bits. Their experience has proven the superiority and high capacity of quantum safe direct communication, especially with the presence of noise and loss in the quantum channel.

Dintomon Joy et al [16] have proposed two deterministic protocols for secure quantum communication (DSQC). Three qubit quantum channels, exactly the same as the GHZ and ve-qubit Brown cases, were used to transmit information securely. The two- and three-bit units that formed the multi-part teleportation diagrams developed in this study were adopted. Using these diagrams, the transmitter is able to choose the measurement rules for quantum channels that have been used to improve and increase the efficiency of qubits in protocols. The study provides an extension of the Nandi-Mazumdar scheme for simultaneous transport of a special class of two states of particles and a method for simultaneous transport of a special class of tripartite state is developed using the five-qubit Brown state as an entanglement channel. The various teleport schemes were then merged with the aim of building new DSQC protocols. This study gives a new idea of how remote transmission of DSQC friendly protocols can be used. The qubit frequency comparison shows the superiority of the proposed protocol over other DSQC protocols based on teleportation. Finally, a method has been proposed to increase the effectiveness of using the brown five-qubit case, in the event that the transmitter uses more suitable meshing channels and uses an appropriate measurement basis.

Related Works

This section investigates several algorithms, which are considered among the most recent in the field of quantum cryptography and modern quantum secure direct communication. The methodology for the work of each algorithm will be dealt with separately as well as the types of attacks that these algorithms can detect, and the mechanisms used in preventing these attacks will be discussed. Finally, the effectiveness and efficiency of these algorithms in bridging security gaps and providing a level of security and confidentiality within direct quantum-based communications will be presented.

Yann et al [17] have introduced Quantum Secure Direct Communication Protocol (QSDC) with authentication using single photons and EPR pairs. This work demonstrates that the QSDC protocol is not safe against an intercept and retransmission attack and impersonation attack. An eavesdropper can get the complete secret message by applying these attacks. An amendment has been proposed to this protocol, which eliminates the aforementioned attacks along with all the familiar attacks. An overview of quantum cryptography is shown which is an application of quantum mechanics to the field of cryptography, and which provides unconditional security based on the laws of physics. Another direction of quantum encryption is Quantum Secure Direct Communication (QSDC), which provides secure communication without any common key in QSDC protocols. The sender encrypts the secret message into some qubits using some pre-encryption rules and sends those qubits to the receiver. After some security checks, the recipient can recover the confidential message. Some generalizations addressed to QSDC protocols are quantitative dialogue or bidirectional QSDC, multiparty QSDC and so on.

If QSDC or any quantum encryption protocol is not designed properly, it presents an opportunity for eavesdropping to impersonate an authorized party. In this regard, it is emphasized that each legitimate party must verify the validity of the other parties, which requires quantitative authentication protocols; The first QSDC protocol was proposed with validation in 2006, followed by much research in this field. There are several quantum encryptions protocols, which have shown to be insecure against many familiar attacks, such as intercept and retransmission attack, impersonation attack, denial of service attack, man-in-the-middle attack, entanglement attack, Trojan horse attack etc. These are all active attacks, that is the eavesdropper has access to the called qubits in the quantum channel between the legitimate parties and is actively participating in the protocol. Some inactive attacks also cause information leakage problems in some communication protocols.

In 2020, [17] provides QSDC protocol based on single photons and EPR pairs, which also achieve mutual authentication. We'll name this QSDC protocol YZCSS. In this protocol, Alice, the message sender,

sets up the corresponding qubit pairs for the secret message and her authentication ID. All qubits are sent to Bob, the message recipient, who uses his authentication ID to retrieve the secret message. However, the YZCSS protocol was found to be not secure against an intercept, retransmission, and spoofing attack. If an eavesdropper applies any of these attacks, he/she can get the complete secret message, that is not only part of the message is exposed, but the whole message is also compromised. Moreover, for the impersonation attack, the legitimate parties cannot be aware of the presence of an eavesdropper. The security of QSDC protocols was analyzed with authentication (YZCSS protocol) and it was found that it is vulnerable to two specific attacks, namely, retransmission attack, and an impersonation attack. An eavesdropper who adopts either of these attacks gets the full secret message. The authentication process in YZCSS is one-way causing an impersonation attack. To get rid of these problems, it was proposed to amend the YZCSS protocol, in which a mutual authentication process was introduced, and it was noted that the modified protocol handles and resists the interception and retransmission attack. It has been shown to be safe against many of the familiar attack strategies that we detailed previously.

The second selected protocol is the single-photon memory QSDC protocol (SPM QSMC) [18]. It is based on entangled pairs of photons. The so-called two-step QSDC protocol [7] designed for deterministic QKD is modified by reducing the number of bits in a block to one, where Alice sets up pairs of Einstein's, Podolsky-Rosen (EPR) photons and then splits them into two parts: the so-called Pioneer qubit and follow-up qubits. The pioneering photon is first transmitted to Bob, while the follow-up photon is used to either perform the encryption or to detect the eavesdropping. Bob extracts the filter key by combining the two particles of the EPR pair to perform a Bell basis measurement. The protocol is then converted to SPM QSDC using coding theory. QSDC relies on mass transfer of quantum states and requires that the users have the capability of storing quantum states which requires quantum memory. There has been substantial progress toward the realization of quantum memory, however there are still substantial challenges. The realizing of perfectly secure communication in a metropolitan area, has the requirement of quantum memory as an obstacle. QSDC protocols without quantum memory is a pressing issue for practical QSDC. Recently, a coding technique was proposed for replacing or mitigating the requirement of quantum memory. This has led to the design of a new QSDC schemes such quantum-memory-free (QMF) QSDC protocols [19] or single-photon memory (SPM) QSDC protocols.

Against this background, a new contribution is the concept of SPM QSDC based on the intrinsic amalgam of the QSDC core protocol and the two-step QSDC protocol; As the security level of the quantum channel is determined by randomly selecting EPR pairs to detect eavesdropping. It is found that any individual attack will affect the resulting error rate and thus may be detected unexpectedly. In the security analysis of this protocol, they considered families of direct measure attack, retransmission intercept attack, and opaque attack strategy, but none of them posed a threat. Moreover, the protocol has been shown to be safe, robust, and resistance against individual attacks. It is found that QSDC protocols become equivalent to deterministic QKD protocols, if the number of bits in a block is reduced to one. All can be converted to QSDC free quantum memory or single photon memory using coding technology. Thus, in the current modern case of QSDC it can be achieved for ergonomic applications using block-based data transfer, while relying on classical coding techniques. Based on the theoretical analysis, it was noted that the High connection efficiency has been achieved.

Lastly, in this study, we select a protocol that is a bit different from the above protocols. It is measurement-device-independent QSDC (MDI QSDC) protocol [20], that uses the sequence of entangled photon pairs and single photons i.e. EPR-pairs and single qubits. It removes the security vulnerabilities associated with the measuring device. Additionally, the MDI technology is able to double the communication distance of its traditional counterpart which works without using the introduced MDI technology.

The secure communication structure in QKD will address three potential security vulnerabilities in this field: the key leaked while distributing it. loss of the key in storage and relocation in users' sites, and encrypted text is intercepted while it is being transmitted. In the other hand, as we know that QSDC sends a message directly through a quantum channel. It does not use key, thus there is the security loopholes associated with the key are all eliminated. However, QSDC is secure under ideal conditions, such as perfect quantum source, noiseless channel, perfect devices, and detectors. Therefore, QSDC in practical application requires measurement-device-independent. In [20], Alice prepares a series of EPR pairs, while Bob prepares a series of single photon states and "sends" it to Alice with the help of teleportation, in which the Bell basis measurement is performed by an unreliable party, which is Charlie. Then, after a safety check, Alice encodes her message into the single instantaneously transmitted photons and sends it to Charlie who measures the single qubits attached to Bob. MDI-QSDC greatly enhances QSDC security under realistic conditions. Since a practical quantum repeater is still not available, increasing the communication distance is also an important issue pursued in the quantum communication community. In addition to the security feature provided by MDI-QSDC, it also doubles the communication distance, because both Alice and Bob send their qubits to the meter that is located at a reduced distance in the middle of it. With current technology, QSDC can be performed at a distance of 100 km, and MDI-QSDC can increase this distance to 200 km. The MDI-QKD protocol does not use block transfer technology, and security is not guaranteed until after random numbers are distributed. Therefore, this protocol does not secure the direct transmission of confidential information, because all the data sent may lead to Eve before its discovery. Classic communications are imperative but fail to sense the presence of eavesdropping. QKD can detect an eavesdropping, but it cannot prevent Eve from accessing the transmitted data, that is, Eve can access the encrypted text by eavesdropping on the classic transmission. On the flip side and by contrast, QSDC is able to detect eavesdropping, preventing Eve from obtaining secure transmitted data, which is also sent over the quantum channel as the MDI-QSDC uses both EPRpairs and a single qubit.

A linked protocol is measured with Bell basis measurements of linear optics, in which only two of the four Bell basis states can be measured. QSDC enables secure direct transmission of information by invoking so-called block data transfer technology for rulers. As the quantum information carriers are sent in a long block containing a large number of qubits. It is found that when the number of qubits in a block is reduced to 1, the QSDC protocols degrade into deterministic QKD protocols. In the end, the discussed algorithms were chosen because they address the field of Quantum Secure Direct Communication (QSDC), as they focus and discuss possible attacks, and provide mechanisms to solve and address these attacks within environments of this type of communication. This gives a good opportunity to provide an accurate comparison between the effectiveness and efficiency of these algorithms in providing the highest possible level of security

Comparison and Result

After presenting an overview of QSDC algorithms, which are considered among the most recent algorithms in the field of quantitative secure direct communication and quantitative coding, we present a comparison and analysis of the efficiency and quality of each algorithm in the field of attack detection and prevention, where the capacity of each algorithm is discussed as well as the types of attacks that were able to resist and be detected. Table 1 shows the most prominent comparison points that were approved and conducted. The comparison includes the techniques it relies on the processing mechanism, type of attacks that each algorithm can resist and respond to by detecting and preventing it, and the role this algorithm plays and its efficiency in bridging security gaps and achieving the highest possible amount.

Table 1: Comparison of the Three Algorithms.

Algorithm Name	YZCSS	The single-photon memory QSDC based on entangled pairs of photons	MDI-QSDC
Techniques which based on	single photons and EPR pairs	of Single Photon Memory (SPM) based on the intrinsic amalgam of the QSDC core protocol and the two-step QSDC protocol; Also, randomly selecting EPR pairs to detect eavesdropping.	Bell basis measurements of linear optics, EPR pairs and a single qubit
Attacks type that overcome the algorithm	1. Intercept-and-resend attacks.	1. direct measure attack.	1. The key leaked while distributing it.
	2. Impersonation attack.	2. retransmission intercept attack	2. Loss of the key in storage and relocation in users' sites.
	3. A denial of service (DoS) attack	3. opaque attack strategy	3. Encrypted text is intercepted while it is being transmitted.
	4. A man-in-the-middle attack.		
	5. The Entangle-measure attack		
	6. Trojan horse attack.		
Algorithm role	It handles and resists the interception and retransmission attack. It has been shown to be safe against many of the familiar attack strategies.	It proves that the protocol has been shown to be safe against individual attacks.	It is able to detect eavesdropping, preventing Eve from obtaining secure transmitted data
Limitation	YZCSS protocol is unidirectional, which	It needs two steps for applying the security	A practical quantum repeater is still not available
	Causes the impersonation attack.		
Strength	Proposed to modification protocol to be mutual authentication	Proposed a new QSDC scheme requiring no block transmission and mitigating the requirement of quantum memory	Enhance QSDC security under realistic conditions. Also increase the communication distance

For each algorithm, the attacks that can be detected and prevented were identified, and in this field, The YZCSS algorithm demonstrated its role in detecting and preventing intercept-and-resend attack, Impersonation attack, A denial of service (DoS) attack, a man-in-the-middle attack, The Entangle-measure attack and trojan horse attack. It handles and resists the interception and retransmission attack. It has been shown to be safe against many of the familiar attack strategies that we detailed previously by using the techniques of single photons and EPR pairs. The single-photon memory QSDC based on entangled pairs of photons algorithm demonstrated its role in detecting and preventing 1-direct measure attack, retransmission intercept attack and opaque attack strategy. It proves that the protocol has been shown to be safe against individual attacks by using the techniques of Single Photon Memory (SPM) based on the intrinsic amalgam of the QSDC core protocol and the two-step QSDC protocol; also, randomly selecting EPR pairs to detect eavesdropping.

The MDI-QSDC algorithm demonstrated its role in detecting and preventing key leaked while distributing it, loss of the key in storage and relocation in users' sites, and encrypted text is intercepted while it is being transmitted. It is able to detect eavesdropping, preventing Eve from obtaining secure transmitted data by using the techniques of Bell basis measurements of linear optics, EPR pairs and a single qubit.

Conclusion

This research provides a presentation of the most recent quantitative safe direct encryption algorithms and discusses the working mechanisms used in each algorithm. Additionally, vulnerabilities and attacks that could be present in quantum direct communications from the retransmission attack are analyzed including man in the middle attack, trojan horse attack, and retransmission intercept attack. The efficiency of the discussed algorithms and their ability to avoid these gaps are studied and analyzed. The study shows whether each algorithm is able to detect or prevent these attacks, and the mechanisms used to detect the attack is discussed. YZCSS algorithm demonstrated its role in detecting and preventing intercept-and-resend attack, Impersonation attack, A denial of service (DoS) attack, a man-in-the-middle attack, The Entangle-measure attack and trojan horse attack. The single-photon memory QSDC based on entangled pairs of photons algorithm demonstrated its role in detecting and preventing 1-direct measure attack, retransmission intercept attack and opaque attack strategy. The

MDI-QSDC algorithm demonstrated its role in detecting and preventing key leaked while distributing it, loss of the key in storage and relocation in users' sites, and encrypted text is intercepted while it is being transmitted.

References

1. Long GL (2017) Quantum secure direct communication: principles, current status, perspectives. In 2017 IEEE 85th Vehicular Technology Conference (VTC Spring) 1-5.
2. Bennett CH, Brassard G (1984) Quantum cryptography: Public key distribution and con tos5. In Proceedings of the International Conference on Computers, Systems and Signal Processing.
3. L Xiao, G L Long, F Deng, J Pan (2004) Efficient multiparty quantum-secret sharing schemes. PHYSICAL REVIEW A 69(5).
4. K Bostr¨om, T Felbinger (2002) Deterministic Secure Direct Communication Using Entanglement. PHYSICAL REVIEW 89(18).
5. A Beige, BG Englert, C Kurtsiefer, H Weinfurter (2002) Secure Communication with a publicly Known Key. ACTA PHY SIC A POLONIC 101(3).
6. FG Deng, GL Long (2004) Secure direct communication with a quantum one-time pad. PHYSICAL REVIEW A 69(5).
7. FG Deng, GL Long, XS Liu (2003) Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. PHYSICAL REVIEW A 68.
8. T Gao, FL Yan, ZX Wang (2004) NUOVE CIMENTO DELLA SOCIETA ITALIANA DI FISICA B 119.
9. QY Cai , BW Li (2004) Chin. Phys. Lett 21.
10. XM Xiu, L Dong, YJ Gao, F Chi, (2007) Multiparty-Controlled Quantum Secure Direct Communication. Journal of Experimental and Theoretical Physics 105(6): 1132-1135.
11. B Ren, H Wei, M Hua, F Deng (2013) Photonic spatial Bell-state analysis for robust quantum secure direct communication using quantum dot-cavity systems. The Europian Physical Journal.
12. Q Y Cai, B W Li (2004) Deterministic Secure Communication Without Using Entanglement. PHYSICAL REVIEW A 69.
13. Zhang S, Chang Y, Yan L, Sheng Z, Yang F, et al. (2019) Quantum communication networks and trust management: A survey. CMC-COMPUTERS MATERIALS & CONTINUA 61(3): 1145-1174.
14. Zou X, Qiu D (2011) Attacks and improvements of QSDC schemes based on CSS codes. In International Conference on Intelligent Computing pp. 239-246.
15. Hu JY, Yu B, Jing MY, Xiao LT, Jia S T, et al. (2016) Experimental quantum secure direct communication with single photons. Light: Science & Applications, 5(9): e16144.
16. Joy D, Surendran S P, Sabir M (2017) Efficient deterministic secure quantum communication protocols using multipartite entangled states. Quantum Information Processing 16: 157.
17. Das N, Paul G (2022) Cryptanalysis of Quantum Secure Direct Communication Protocol with Mutual Authentication Based on Single Photons and Bell States. Europhysics Letters 138(4).
18. D Pan, K Li, D Ruan, SX Ng, L Hanzo (2020) Single-Photon-Memory Two-Step Quantum Secure Direct Communication Relying on Einstein-Podolsky-Rosen Pairs. IEEE 8.
19. Z Sun, R Qi, Z Lin, L Yin, G Long, et al. (2018) Design and implementation of a practical quantum secure direct communication system, in Proc. IEEE Globecom Workshops (GC Wkshps).
20. Z Zhou, Y Sheng, P Niu, L Yin, G Long, et al. (2020) Measurement-device-independent quantum secure direct communication. SCIENCE CHINA Physics Mechanics & Astronomy 63002E