Journal Article
Journal of Generative Artificial Intelligence in Public Sector
www.aipost.com
Volume 1 July 2025 Issue 1

An Analysis of Quantum Secure Direct Communication

By NURULLAH NAQVI*

Abstract

Quantum secure direct communication is a process in quantum communication to allow users to communicate securely and directly using quantum mechanics and without the need of generating and sharing secure keys. In recent years, many quantum secure direct communication (QSDC) protocols have been established and proposed. This paper seeks to explore three such QSDC protocols. The first protocol relies on hyperentanglement and complete Bell-state measurements for encoding and decoding of classical information. The second protocol relies on hyperentanglement and a complete polarization Bell-state analysis for encoding and decoding of classical information. The third protocol creates a 15-user quantum network and uses a Bell-state measurement based on the sum-frequency generation to decode classical bits. This paper will provide an in-depth look at the steps of these protocols, test these protocols in conjunction with previously designated criteria for QSDC schemes, and compare and contrast these protocols.

Keywords: Quantum, Secure Direct Communications, QSDC Protocols

1. Introduction

As quantum computing has developed as a field in recent years, we have seen a growth in its applications in cryptography, leading to further development in quantum cryptography. Quantum cryptography was originally proposed in the 1970s; however, information theory, classical cryptography, and quantum physics first had to further mature as fields before quantum cryptography could truly develop. (Gisin et al., 2002). As the development of the field has increased, its applications and implementations have also greatly increased. Prior to the introduction of quantum cryptography, traditional secure communication was conducted using encryption,

* Nurullah Naqvi is the President and Chief technology Officer of the American Institute of Artificial Intelligence

mathematically created in such a way that the computational complexity of breaking it would take too long to be feasible (Gisin et al., 2002). With the implementation of quantum computers, many classical cryptography protocols will be breakable, and thus, vulnerable (Long et al., 2007). This clearly presents an issue, as all modern day encryption may be under threat from quantum computers in the near future. However, with the introduction of quantum cryptography, new techniques have been created to securely communicate.

This leads to the field of quantum communication. Quantum communication uses principles of quantum mechanics to ensure the unconditional security of communication (Sheng et al., 2021). The origins of quantum communication began with quantum key distribution (QKD) (Sheng et al., 2021). As stated by Long et al. (2007), quantum key distribution provides a novel way for two legitimate parties to establish a common secret key over a long distance. Thus, QKD makes it possible to create and distribute secure keys for encryption. Further stated by Long et al. (2007), a new method of quantum communication developed, furthering the processes used in QKD. This method is quantum secure direct communication (QSDC). While QSDC is similar to QKD, in that the goal of both is secure communication relying on quantum mechanics, QSDC differs in that the goal is to communicate a message securely without generating a key (Long et al., 2007).

2. Background

One of the first quantum secure direct communication protocols was proposed in 2002 by Beige et al., based on single photon two-qubit states. While this protocol operated similar to a quantum key distribution protocol, a secure message could be read after the transmission of additional classical information with each qubit. Thus, one of the first means of conducting direct secure communication using quantum principles was developed. Since then, many potential protocols have emerged to conduct QSDC. As stated by Sheng et al. (2022), the purpose of quantum secure direct communication is to directly transmit secret messages without the need of generating or sharing a key. Furthermore, as covered by Long et al. (2007), in QSDC, secret messages can be securely communicated directly between a sender (Alice) and receiver (Bob) without the classical communication of ciphertext. Thus, the quantum key generation and distribution and classical communication of a ciphertext message are combined into a singular form of quantum communication. This provides evidence as to why QKD served as a *stepping stone* to QSDC, as well as evidence to why QSDC may be more secure than QKD but more complicated. Since the purpose of QKD is key distribution, this implies that the information shared between parties may not be controllable, and thus random, while in QSDC the goal is to share information directly. This introduces the need to be able to *control* what information is exactly sent. In addition, to securely communicate with QKD, the sender needs to send information classically (Long et al., 2007), while in QSDC information is shared using quantum principles.

Long et al. (2007), goes on to define the criteria and requirements of a quantum secure direct communication protocol - for a real secure QSDC scheme there are four requirements.

1) After the quantum states are transmitted through a quantum channel from the sender (Alice) to the receiver (Bob), Bob should be able to read the secret message directly without the need of any additional classical information to be sent.
2) The eavesdropper (Eve) cannot obtain any useful information about the sent message, regardless of her steps taken.
3) Alice and Bob can detect if Eve is eavesdropping even before they encode the secret messages onto quantum states.
4) The encoded quantum states are transmitted sequentially in a block by block way.

These four requirements present a basis for satisfying the goals of QSDC. The first criteria helps to ensure that once encoded quantum information has been shared between two users, no classical information needs to be sent, thus, ensuring the quantum and direct aspect of QSDC. The second and third criteria are necessary to ensure that a QSDC protocol is secure. Since QSDC does not use security keys, the safety and security of the protocol lies in the inability of an eavesdropper from obtaining any usable information about a sent message and the ability for the users of the protocol to be aware if any eavesdropping is occurring. Finally, the fourth criteria ensures that direct communication is occurring through a quantum channel. Each of the following three QSDC protocols will be tested against these criteria established by Long et al. (2007).

3. Quantum Secure Direct Communication Protocol 1 (Gao et al., 2021)

This section of this paper will now cover a quantum secure direct communication protocol proposed by Gao et al., in 2021. This section will seek to define, explain, and analyze this protocol, and all information on the protocol is referenced from Gao et at. (2021).

Gao et al.'s protocol for quantum secure direct communication is proposed using the complete Bell-state measurement (CBSM) resorting to linear optical elements and temporal-polarization hyper-entanglement. The proposed protocol relies on polarized entangled photons to be the carriers of information where the detection events of CBSM are identified with common single-photon detectors. Since all two-photon detection events in CBSM are effective and can be preserved with 100% efficiency rather than 50% efficiency of previous QSDC protocols, the quantum efficiency of QSDC is doubled by encoding more messages on entangled photon pairs.

Thus, this protocol of QSDC is based on the polarization entanglement of photons. Four polarized entangled Bell-states are used as the means of securely transmitting a message. These four entangled Bell-states are written as:

$$|\psi^{\pm}(t)\rangle_{AB} = |\psi^{\pm}\rangle_{AB} \otimes |\phi(t)\rangle_{AB},$$
$$|\phi^{\pm}(t)\rangle_{AB} = |\phi^{\pm}\rangle_{AB} \otimes |\psi(t)\rangle_{AB}$$

Step 1: First, Alice prepares n pairs of hyperentangled photon pairs $\{A_1B_1, \ldots, A_nB_n\}$, which are in the hyperentangled state $|\phi^{\pm}(t)\rangle_{AB}$. Hyperentanglement is defined as the entanglement in multiple degrees of freedom (DOFs) of a quantum system, such as polarization of photons (Dent et al., 2017). Next, the hyperentangled photon pairs are divided into sequences S_A and S_B, such that $S_A = \{A_1, \ldots, A_n\}$ and $S_B = \{B_1, \ldots, B_n\}$. Alice sends sequence S_B to Bob through an optical channel and retains sequence S_A.

Step 2: Upon receiving the photon sequence, S_B , sent by Alice, Bob performs a security test. Bob randomly chooses some photons from the sequence to perform a single photon measurement on the polarization degrees of freedom, using the single photon measurement basis of
$\sigma_z = \{|H\rangle, |V\rangle\}$. Bob publicly announces the outcome of his measurements along with the positions and the measurement basis of the detected photons. After, Alice makes the same measurements on the photon sequence she retained, S_A, for the corresponding positions. Alice and Bob should theoretically have the same measurement results for their measured samples. Prior to the protocol, some security threshold is agreed upon between Alice and Bob. If the estimated error rate of the sample measurements falls below the security threshold, Alice and Bob can assume that the quantum channel is secure and no eavesdropping exists. If the estimated error rate of the sampled measurements is greater than the security threshold, then Alice and Bob will cease communication and can assume that eavesdropping may be occurring and that the channel is insecure.

Step 3: Once Alice and Bob have ensured that their estimated error rate falls below the security threshold, Alice will make unitary operations on the polarization modes of the remaining photon sequences in S_A. The unitary operations are defined as:

$$U_i = |H\rangle\langle H| + |V\rangle\langle V|,$$
$$U_x = |V\rangle\langle H| + |H\rangle\langle V|,$$
$$U_y = |V\rangle\langle H| - |H\rangle\langle V|,$$
$$U_z = |H\rangle\langle H| - |V\rangle\langle V|$$

Using the four unitary operations from above, U_i, U_x, U_y, U_z, the initial hyperentangled state of $|\phi^+(t)\rangle_{AB}$ can be transformed into four hyperentangled states: $|\phi^+(t)\rangle_{AB}$, $|\phi^-(t)\rangle_{AB}$, $|\psi^+(t)\rangle_{AB}$, and $|\psi^-(t)\rangle_{AB}$. Prior to the start of transmission, Alice and Bob will agree that the unitary operations U_i, U_x, U_y, U_z denote 00, 01, 10, and 11 bits, respectively. Alice will randomly choose and encode some photons for the purpose of the security check. Then, Alice will send the encoded photon sequences to Bob.

Step 4: Bob performs the complete Bell-state measurement on the polarization degrees of freedom of photon pair sequences, differentiating four temporal-polarization hyperentangled states: $|\phi^+(t)\rangle_{AB}$, $|\phi^-(t)\rangle_{AB}$, $|\psi^+(t)\rangle_{AB}$, and $|\psi^-(t)\rangle_{AB}$. A schematic diagram shows the complete Bell-state measurement, including t_o and t_1 temporal delays, where $t_0 > t_1$. When a photon pair is in each of the four hyperentangled states, two separate detectors for the CBSM will trigger. If two detectors are triggered, the corresponding event is assumed to be successful. There are four detectors present,

D_1, D_2, D_3, D_4, and the combination of the detectors and the time delay reveal the encoded bit. If the detectors D_1D_2 or D_3D_4 occur at the same time, then the encoded two photons are in the state $|\phi^+(t)\rangle_{AB}$. If the detectors D_1D_4 or D_2D_3 occur at the same time, then the encoded two photons are in the state $|\phi^-(t)\rangle_{AB}$. If the two detectors $D_1D_2, D_3D_4, D_1D_3,$ or D_2D_4 are triggered with the time delay t_0, the two encoded photons are in the state $|\psi^+(t)\rangle_{AB}$. If the two detectors $D_1D_1, D_2D_2, D_4D_4, D_1D_4,$ or D_2D_3 are triggered with the time delay t_1, the two encoded photons are in the state $|\psi^-(t)\rangle_{AB}$. Using the previously agreed upon (with Alice) encoding of 00, 01, 10, and 11, Bob is able to determine what encoded bits he received from Alice. Bob will then publicly announce (over a public channel) the successful detection signatures. Alice and Bob will then keep a record of the occurrences with the successful detections and discard all remaining detections as failures. Another security check can then be performed by Alice with Bob estimating the error rate according to the measurement results of the photons. If the security check is passed, and thus, communication secure, error correction and privacy amplification are performed and the secret message is successfully transmitted between Alice and Bob.

The essence of this QSDC protocol lies in the setup of the complete Bell-state measurement design. The CBSM design allows for the ability to detect which hyperentangled state was received after a unitary operation was conducted on it. The CBSM provides a way to distinguish the four hyperentangled states: $|\phi^+(t)\rangle_{AB}$, $|\phi^-(t)\rangle_{AB}$, $|\psi^+(t)\rangle_{AB}$, and $|\psi^-(t)\rangle_{AB}$. The necessity of the detectors and temporal delays in the CBSM is to allow for a proper way to determine which of the four original hyperentangled states was encoded. Upon running the CBSM and recording the results, all Bob must do is compare the results with the predetermined encoding of the classical bits 00, 01, 10, and 11. Thus, it can easily be seen how key distribution is no longer needed. The classical bits are encoded into a quantum state, the quantum state is sent after performing security checks to ensure no eavesdropping, the quantum state is measured using a complete Bell-state measurement, the measurement result is then compared and mapped back to the classical bit. Another security check is performed, and if it passes, a quantum secure direct communication has occurred.

To further verify that this CBSM protocol classifies as a quantum secure direct communication protocol, we will review if it satisfies the four requirements and criteria established by Long et al. (2007) for a QSDC scheme.

1) *After the quantum states are transmitted through a quantum channel from the sender (Alice) to the receiver (Bob), Bob should be able to read the secret message directly without the need of any additional classical information to be sent.*
   In this protocol, the secure quantum channel is established by photon pairs in temporal-polarization hyperentangled states. Once Alice sends the quantum states after the unitary operations are performed, Bob receives the quantum states. Bob then performs a complete Bell-state measurement and can decode the measurement results into classical bits, based upon the agreed upon mappings between Alice and Bob prior to the sending of the quantum states. Thus, after Alice transmits the quantum states through the quantum channel, Bob does not

need any classical information to read the message. Therefore, the QSDC protocol satisfies the first criteria.

2) *The eavesdropper (Eve) cannot obtain any useful information about the sent message, regardless of her steps taken.*
   The security of this QSDC protocol is reliant on the non-locality of the hyperentangled photon pair with double security checks. The first security check performed detects if an attack on the first transmitted photon sequence is occurring before the encoding with the block by block transmission technique. The second security check guarantees the security of the second transmitted photon sequence after the encoding has taken place. Thus, the security checks performed prevent any information from being obtained by Eve during attempted eavesdropping. Therefore, the QSDC protocol satisfies the second criteria.
3) *Alice and Bob can detect if Eve is eavesdropping even before they encode the secret messages onto quantum st*ates.
   The first security check is performed prior to the encoding of the message into the quantum state. Thus, Alice and Bob will be aware of whether Eve is eavesdropping prior to the encoding. Therefore, the QSDC protocol satisfies the third criteria.
4) *The encoded quantum states are transmitted sequentially in a block by block way.*
   This QSDC uses a block-transmission technique for encoding and transmission. Thus, the QSDC protocol satisfies the fourth criteria.

Since all four criteria established by Long et al. (2007) are satisfied by this quantum secure direct communication protocol, it can be further concluded that QSDC occurs with this protocol.

The physical implementation of this QSDC protocol requires the use of nonlinear optical elements. Nonlinear optical elements are necessary to differentiate properly between the four Bell-states. However, without the use of nonlinear optical elements (resorting to linear optical elements), it is challenging to properly execute this protocol, in both theory and experimentally. Linear optical elements prove difficult to properly distinguish between the four Bell-states, thus making it difficult to decode the proper message. In previous QSDC protocols relying on Bell-state measurements, the success probability was 50%. Quantum efficiency, defined as the amount of messages encoded on an entangled photon pair, is directly related to the successful probability of the Bell-state measurements. The addition of the complete Bell-state measurement, in which the photon pairs are in the temporal-polarization hyperentangled state, increases the quantum efficiency by encoding two bits of messages (00, 01, 10, 11) on an entangled photon pair. This leads to double the efficiency than previously. Thus, the usefulness of using hyperentangled states and the complete Bell-state measurement can be seen in a quantum secure direct communication protocol.

4. Quantum Secure Direct Communication Protocol 2 (Sheng et al., 2022)

This section of this paper will now cover a quantum secure direct communication protocol proposed by Sheng et al., in 2022. This section will seek to define, explain, and analyze this protocol, and all information on the protocol is referenced from Sheng et al. (2022).

Sheng et al., propose a one-step quantum secure direct communication protocol. This protocol requires the distribution of polarization-spatial-mode hyperentanglement for one round only. The security of this protocol is ensured by preventing any way for an eavesdropper from obtaining information on the message. Furthermore, this protocol is a two-way quantum communication, rather than a one-way message from a sender to a receiver. In addition, this protocol has a high capacity to transmit two bits of secret messages with one pair of hyperentanglement, rather than just one bit. Using entanglement fidelities of polarization and spatial-mode degrees of freedom at 0.98, the maximal communication distance of this protocol is 216 km.

Traditionally, quantum secure direct communication protocols require two-steps. In the first step, two users distribute the entanglement to set up a quantum channel. In the second step, the message sender (Alice) encodes, using the dense encoding approach, and sends their message to the receiver (Bob). One of the photons in each photon pair is sent back to perform a Bell-state analysis to read out the secret message. Major developments have allowed great progress in these protocols in recent years. For example, hyperentanglement, which is the simultaneous entanglement in more than one degree of freedom, has been used to increase channel capacity. This protocol can transmit two bits of secret message by distributing the hyperentanglement in only one round.

This QSDC protocol adopts the polarization-spatial-mode hyperentanglement with the form of:

$$|\Phi^+\rangle = |\phi^+\rangle_P \otimes |\phi^+\rangle_S$$

where $|\phi^+\rangle_P$ is one of the four Bell-states in polarization degrees of freedom with the form:

$$|\phi^\pm\rangle_P = \frac{1}{\sqrt{2}}(/H\rangle/H\rangle \pm /V\rangle/V\rangle),$$
$$|\psi^\pm\rangle_P = \frac{1}{\sqrt{2}}(/H\rangle/V\rangle \pm /V\rangle/H\rangle)$$

and $|\phi^+\rangle_S$ is one of the four Bell-states in spatial-mode degrees of freedom with the form:

$$|\phi^\pm\rangle_S = \frac{1}{\sqrt{2}}(/a_1\rangle/b_1\rangle \pm /a_2\rangle/b_2\rangle),$$
$$|\psi^\pm\rangle_S = \frac{1}{\sqrt{2}}(/a_1\rangle/b_2\rangle \pm /a_2\rangle/b_1\rangle)$$

where $/H\rangle$ denotes horizontal polarization, $/V\rangle$ denotes vertical polarization, and a_1, b_1, a_2, b_2 denote different spatial modes.

To accomplish this quantum secure direct communication protocol, the following steps must be taken:

Step 1: Alice prepares N ordered pairs of polarization-spatial-mode hyperentangled states, $|\Phi^+\rangle_i \; s.t. \; i = 1,2,\ldots,N$. These ordered N pairs construct the message sequence. Alice then prepares an ordered M pairs of hyperentangled states $|\Phi^+\rangle_j \; s.t. \; j = 1,2,\ldots,M$, for the purpose of security testing. The security testing photon pairs are inserted into the message at random. Thus, the complete message sequence has $N + M$ hyperentangled photon pairs.

Step 2: For every hyperentangled photon pair in the complete message sequence, Alice will retain the first photon and send the second photon to Bob using block transmission. Once the photon transmission has been completed, both Alice and Bob measure the security testing photons and store the remaining photons in quantum memories.

Step 3: In the security checking sequence, Alice will randomly choose the basis $\{|H\rangle, |V\rangle\}$ or $\{|\pm\rangle_P = \frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle)\}$ in polarization degrees of freedom and $\{|a_1\rangle, |a_2\rangle\}$ or $\{|\pm\rangle_S = \frac{1}{\sqrt{2}}(|a_1\rangle \pm |a_2\rangle)\}$ in spatial-mode degrees of freedom for the purpose of measuring the security checking photons. Alice will then tell Bob the position and measurement she has chosen for each security checking photon, and Bob will use the same measurement basis to measure the corresponding photon. Alice and Bob will then compare their measurement results. Alice and Bob communicate the previous two steps over a standard, classical communication channel. If no eavesdropping has occurred, Alice and Bob will obtain the same results in both degrees of freedom. However, if they obtain different measurement results in a degree of freedom, a bit-flip error will occur. If the error rate of the bit-flips is higher in any degree of freedom than some established threshold, Alice and Bob will terminate communication. If the error rate is below the established threshold, then Alice and Bob proceed with the assurance that the photon transmission is secure.

Step 4: After Alice and Bob have completed the security check and if the error rate passes, then Alice distills the photons in the message sequence from the quantum memories and encodes her single photons with four single-qubit unitary operations. These four unitary operations can be written as:

$$U_0 = I = |H\rangle\langle H| + |V\rangle\langle V|,$$
$$U_1 = \sigma_x = |H\rangle\langle V| + |V\rangle\langle H|,$$
$$U_2 = \sigma_z = |H\rangle\langle H| - |V\rangle\langle V|,$$
$$U_3 = i\sigma_y = |H\rangle\langle V| - |V\rangle\langle H|$$

The unitary operation $U_k \; for \; k = 0,1,2,3$ will transform the state of $|\phi^+\rangle_P$ into $|\phi^+\rangle_P, |\psi^+\rangle_P, |\phi^-\rangle_P, |\psi^-\rangle_P$, respectively. The operators U_0, U_1, U_2, U_4 are encoded as 00, 01, 10, and 11, respectively. Notice, some of these steps, equations, and encoding follow very closely to the previous protocol established by Gao et al. (2021). This occurs since both QSDC protocols rely on hyperentanglement and Bell-state measurements.

Step 5: Alice and Bob perform nonlocal complete polarization Bell-state analysis assisted with spatial-mode entanglement. The complete polarization Bell-state analysis measurement result depends on the output modes of Alice and Bob.

Step 6: Alice then publishes the positions and her measurement results of the secret message photons.

Step 7: Based on Alice's measurement results, Bob can decode the secret messages with his own measurement results. These measurements require similar detectors to the previously referenced QSDC protocol (Gao et al., 2021).

From the steps, it can be seen that the key element in this QSDC protocol is the nonlocal complete polarization Bell-state analysis. In linear optics, it is known that only two of the four Bell-states can be distinguished. However, with hyperentanglement, i.e. with the entanglement in other degrees of freedom, complete polarization Bell-state analysis is possible. Letting D_iD_j represent the photon detectors, then the measurement result of D_1D_5, D_2D_6, D_3D_7 or D_4D_8 represent the state $|\phi^+\rangle_P$. The measurement result of D_1D_7, D_3D_5, D_4D_6 or D_2D_8 represent the state $|\psi^+\rangle_P$. The measurement result of D_1D_6, D_2D_5, D_3D_8 or D_4D_7 represent the state $|\phi^-\rangle_P$. The measurement result of D_1D_8, D_2D_7, D_3D_6 or D_4D_5 represent the state $|\psi^-\rangle_P$.

To ensure that the protocol fulfills the requirements of a QSDC scheme, each of the four criteria established by Long et al. (2007) will be checked:

1) *After the quantum states are transmitted through a quantum channel from the sender (Alice) to the receiver (Bob), Bob should be able to read the secret message directly without the need of any additional classical information to be sent.*
   After Bob receives the encoded message through a quantum channel, Alice and Bob both perform nonlocal complete polarization Bell-state analysis assisted with spatial-entanglement. However, for Bob to truly decode the message, Alice must share her positions and measurement results of the message photons. Thus, this protocol does not satisfy the first criteria since after the quantum states are transmitted, Bob needs additional classical information from Alice, regarding her positions and measurement results.
2) *The eavesdropper (Eve) cannot obtain any useful information about the sent message, regardless of her steps taken.*
   Similarly to the previous protocol established by Gao et al. (2021), this protocol relies on security checks to be performed by Alice and Bob. Alice and Bob will be aware of whether there is eavesdropping occuring. Thus, preventing the chance of eavesdropping from occurring. Therefore, this protocol satisfies the second criteria.
3) *Alice and Bob can detect if Eve is eavesdropping even before they encode the secret messages onto quantum st*ates.
   Alice and Bob perform a security check prior to the encoding done by Alice onto quantum states, i.e. the performance of the unitary operators. Thus, Alice and Bob

will know if there is an eavesdropper prior to the encoding of the secret message. Therefore, this protocol satisfies the third criteria.

4) *The encoded quantum states are transmitted sequentially in a block by block way.* This QSDC uses a block-transmission technique for encoding and transmission. Thus, the QSDC protocol satisfies the fourth criteria.

Since this protocol fails the first criteria established by Long et al. (2007) for quantum secure direct communication protocols, this protocol does not fit Long et al.'s (2007) definition for a QSDC. The key failure occurs since Long et al. (2007) requires a QSDC protocol to not need any further classical information to be sent for Bob to decode the message after receiving the quantum states. In this protocol, Alice must send Bob her positions and measurements after Bob has already received the encoded quantum states. Despite failing to fulfill the criteria established by Long et al. (2007) for a QSDC, this protocol still fulfills the pure goal of quantum secure direct communication - to communicate directly and securely using quantum principles without the need for a secret key.

The steps for both protocols present several key differences between this protocol and the QSDC protocol proposed by Gao et al. (2021). While hyperentanglement, forms of complete Bell-state measurements, unitary operators to encode, security checking random phases, and a mapping for encoding and decoding were necessary for both protocols, differences in the implementation arise. For one, while both the Gao et al. (2021) protocol and the Sheng et al. (2022) protocol require Alice to generate two sequences, one of the message itself and one for the security check, in the Sheng et al. (2022) protocol, Alice combines the sequences and retains a photon before transmitting to Bob, rather than sending one sequence to Bob, as in the Gao et al. (2021) protocol. Furthermore, both protocols had a variation in the method of the complete Bell-state measurement. The Gao et al. (2021) protocol included time delays while the Sheng et al. (2022) protocol needed a greater number of photon detectors for the measurement. Finally, there were slight variations in the unitary operators and phase equations between both protocols. Despite these differences, since both protocols use hyperentanglement, they can both transmit two bits of information at a time, leading to higher quantum efficiency than other quantum secure direct communication protocols which can only transmit one bit of information at a time.

5. Quantum Secure Direct Communication Protocol 3 (Qi et al., 2021)

This section of this paper will now cover a quantum secure direct communication protocol proposed by Qi et al., in 2021. This section will seek to define, explain, and analyze this protocol, and all information on the protocol is referenced from Qi et al. (2021).

Qi et al. (2021) published a framework for a new QSDC protocol. The goal of this protocol was to overcome two major issues of QSDC. One, overcoming the difficulty of differentiating simultaneously between four sets of encoded entangled states. Two, overcoming the traditional limitations of one-to-one communication between one sender and one receiver. The Qi et al. (2021) protocol manages to accomplish these tasks by creating a QSDC network based on time-energy entanglement and sum-frequency generation that connects 15 users together with a greater than 97% fidelity rate.

Furthermore, this protocol's results maintain a fidelity rate of greater than 95% for any two users performing QSDC over a 40 km optical fiber over the network.

Assume that any two users, U_1 and U_2, wish to communicate directly, where U_1 wants to send information to U_2. They will share N pairs of the time-energy entangled states:

$|\phi^+\rangle = \frac{|ss\rangle + |ll\rangle}{\sqrt{2}}$,

where s and l indicate whether the entangled photons travel through a short or long path. The steps of this protocol are as follows:

Step 1: Detect the quantum channel to ensure its absolute safety.

Step 2: The users agree that $|\phi^+\rangle$, $|\psi^+\rangle$, $|\phi^-\rangle$, $|\psi^-\rangle$ encode the bit values 00, 01, 10, and 11, respectively. $|\phi^\pm\rangle = \frac{|ss\rangle \pm |ll\rangle}{\sqrt{2}}$ and $|\psi^\pm\rangle = \frac{|ls\rangle \pm |sl\rangle}{\sqrt{2}}$ are the four sets of Bell-states.

Step 3: User 1 will perform one of four unitary operations, $I, \sigma_x, \sigma_z, i\sigma_y$, on the photons in their possession to convert $|\phi^+\rangle$ into $|\phi^+\rangle$, $|\psi^+\rangle$, $|\phi^-\rangle$, $|\psi^-\rangle$, respectively. Thus, after the unitary operation, the converted $|\phi^+\rangle$ will represent an encoded bit value of 00, 01, 10, or 11.

Step 4: User 2 performs the Bell-state measurement based on the sum-frequency generation to decode the information, allowing User 2 to differentiate between the four sets of encoded Bell-states.

The main factor of this QSDC protocol lies in its network design. The network composition is divided into two layers, the communication network and the subnet. The quantum network is fully connected by five subnets (A, B, C, D, and E). The communication network is the network connecting these 5 subnets. These 5 subnets are made of 3 users each. Between the five subnets are a total of ten connections that represent the correlated time-energy photon pairs between subnets. Thus, each subnet is connected to the other four subnets. Each subnet contains a 1 x 3 passive beam splitter and a delay controlling module, which functions to split a frequency-correlated entangled photon pair and randomly sends them to the three users in that subnet. The ten time-energy-entangled photon pairs between the subnets are divided into 20 ITU (International Telecommunication Union) channels via a 100 GHz DWDM (dense wavelength division multiplexing). DWDM is placed in the quantum-network processor, and then, the output modules of the multichannel are connected to the users in each subnet. To properly realize the interconnection between the three users of a subnet, the quantum processor must distribute five pairs of entangled photons.

To ensure that the protocol fulfills the requirements of a QSDC scheme, each of the four criteria established by Long et al. (2007) will be checked:

1) *After the quantum states are transmitted through a quantum channel from the sender (Alice) to the receiver (Bob), Bob should be able to read the secret message directly without the need of any additional classical information to be sent.*
   After a sender, Alice, sends the receiver(s) the encoded quantum message, all the receiver is required to do is to perform a Bell-state measurement on the sum-frequency generation, and thus, decoding the message. Since, the receiver(s) do

not need any further information after they receive the quantum states, this protocol does satisfy the first criteria.

2) *The eavesdropper (Eve) cannot obtain any useful information about the sent message, regardless of her steps taken.*
   The security of this protocol lies in the ability of the users to perform eavesdrop and security checking at any time in the process. If the monitored error rate is lower than a predetermined threshold, then the communication is successful. Thus, this protocol satisfies the second criteria.
3) *Alice and Bob can detect if Eve is eavesdropping even before they encode the secret messages onto quantum st*ates.
   Since the users can perform security checking at any time, and thus, in this protocol perform a security check prior to the sender encoding the secret message onto quantum states, the sender and receiver(s) can determine if eavesdropping is occurring. Therefore, this protocol satisfies the third criteria.
4) *The encoded quantum states are transmitted sequentially in a block by block way.*
   This QSDC uses the block-transmission and step-by-step transmission methods for transmission. Thus, the QSDC protocol satisfies the fourth criteria.

Since this protocol satisfies all four criteria established by Long et al. (2007) for quantum secure direct communication protocols, this protocol does fit Long et al.'s (2007) requirement for a QSDC.

In summary, this QSDC protocol establishes a fully connected entanglement-based QSDC network with five subnets and 15 users. Then, using the frequency correlations of the 15 photon pairs via time-division multiplexing and dense wavelength division multiplexing, an experiment was performed using a 40 km optical fiber and two-step transmission between users without generating any secure keys. The spectrum of the source single-photon is divided into 30 International Telecommunication Union channels, for which a coincidence event will occur between each user by performing a Bell-state measurement based on the sum-frequency generation. This coincidence even allows the four sets of encoded entangled states to be identified simultaneously without any post selection. Furthermore, in this QSDC network, each user can request to communicate with others at any time once the network is established. This connection relies on transmitting entangled photon states between multiple users. Thus, a fully secure quantum network is established between 15 users, allowing for secure and direct communication.

6. Conclusion

After reviewing all three protocols, several important similarities and key differences arise. All three protocols use Bell-states, entanglement, Bell-state measurements, unitary operations, and security checks. All three protocols depend on four Bell-states being used to encode four classical bits of information, 00, 01, 10, and 11. These Bell-states vary between the protocols; however, the process of encoding is similar. For each protocol, the user starts with a single Bell-state, and the goal, once security is established, is for the sender to conduct a unitary operation from a set of four unitary operators, that will transform the Bell-state either back into itself or into one of

the other three Bell-states. When the receiver has received this transformed Bell-state, they conduct the Bell-state measurement indicated by their protocol to decode the quantum state back into the classical bits.

This process is where the key differences arise between the three protocols. The Gao et al. (2021) protocol uses a complete Bell-state measurement with four detectors and two time delays to decode the quantum state into classical bits. The Sheng et al. (2022) protocol uses a complete polarization Bell-state analysis with eight detectors to decode into classical bits, also requiring positional information and the sender's own measurements to decode. The Qi et al. (2021) protocol requires a Bell-state measurement based on the sum-frequency generation to decode into classical bits. In addition, the Qi et al. (2021) protocol establishes a larger quantum network of 15 users, rather than just two users. Despite these major differences, the overarching goal of all three quantum secure direct communication protocols is to differentiate between four sets of encoded entangled states. Furthermore, all three protocols allow the receiver to decode two bits of classical information rather than one. In addition, the Qi et al. (2021) protocol establishes a quantum network of multiple users. These protocols have shown the abilities to communicate directly and securely using quantum mechanics, with multiple users, and with more classical information encoded. Thus, it can be seen that the recent developments of protocols of quantum secure direct communication have led to major advancements in QSDC and will greatly enhance the viability and importance of quantum communication.

References

1. A. Beige, B.-G. Englert, Ch. Kurtsiefer, and H. Weinfurter, Acta Phys. Pol. A 101, 357 (2002).
2. Deng, F.-G., Ren, B.-C., & Li, X.-H. (2017). Quantum hyperentanglement and its applications in Quantum Information Processing. *Science Bulletin*, *62*(1), 46–68. https://doi.org/10.1016/j.scib.2016.11.007
3. Gao, C. Y., Guo, P. L., & Ren, B. C. (2021). Efficient Quantum Secure Direct Communication with complete bell-state measurement. *Quantum Engineering*, *3*(4). https://doi.org/10.1002/que2.83
4. Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of Modern Physics*, *74*(1), 145–195. https://doi.org/10.1103/revmodphys.74.145
5. Long, G.-lu, Deng, F.-guo, Wang, C., Li, X.-han, Wen, K., & Wang, W.-ying. (2007). Quantum secure direct communication and deterministic secure quantum communication. *Frontiers of Physics in China*, *2*(3), 251–272. https://doi.org/10.1007/s11467-007-0050-3

6. Qi, Z., Li, Y., Huang, Y., Feng, J., Zheng, Y., & Chen, X. (2021). A 15-user quantum secure direct communication network. *Light: Science & Applications*, *10*(1). https://doi.org/10.1038/s41377-021-00634-2
7. Sheng, Y.-B., Zhou, L., & Long, G.-L. (2022). One-step quantum secure direct communication. *Science Bulletin*, *67*(4), 367–374. https://doi.org/10.1016/j.scib.2021.11.002
8. Ye, Z.-D., Pan, D., Sun, Z., Du, C.-G., Yin, L.-G., & Long, G.-L. (2020). Generic Security Analysis Framework for Quantum Secure Direct Communication. *Frontiers of Physics*, *16*(2). https://doi.org/10.1007/s11467-020-1025-x
9. Zhang, H., Sun, Z., Qi, R., Yin, L., Long, G.-L., & Lu, J. (2022). Realization of quantum secure direct communication over 100 km fiber with time-bin and phase quantum states. *Light: Science & Applications*, *11*(1). https://doi.org/10.1038/s41377-022-00769-w