# A Review of Semi-Quantum Secure Direct Communication Protocols

KIRAN MEENA[1]
NARAYAN LAL GUPTA[2]
VIVEK MANDOT[3]

GGTU - Govind Guru Tribal university
DoP - Department of Physics (Sodh Anubhag)
Village Badvi, Mahi Dam Road, Banswara(Rajasthan)-327001, India
[1]octkiran@gmail.com
[2]nlgupt@gmail.com
[3]mandot@gmail.com.com

**Abstract.** This review paper includes five distinct protocols in the field of semi-quantum secure direct communication based on different qubit carriers -single photons, EPR pairs, Cluster states, Mediated third party, and two degrees of freedom-polarisation and spatial mode. These protocols have been analyzed for their security against several methods of attack like- trojan horse attacks, intercept-resend Attacks, double C-not attacks, and modification attacks. Their efficiency is also estimated and described here. Future work direction in the field of SQSDC is summarised.

**Keywords:** SQSDC protocols, Trojan Horse Attacks, Intercept and Resend Attack, Modification Attack, Double C-Not attack.

(Received December 15th, 2024 / Accepted January 22th, 2025)

Classical methods of communication security, based on the difficulty for classical computation like- large Prime number factor problems, are vulnerable and inadequate in the post-quantum communication scenario. Quantum cryptography came into existence as a solution to the mentioned problem with the inception of BB84 protocol for Quantum Key Distribution(QKD) [1]. It has been proven to be unconditionally secure by the principles of quantum mechanics [26, 10, 13].

The other important branch is Quantum Secure Direct Communication (QSDC), which is based on the direct transmission of secret message to legitimate users instead of generating a key for encryption. Since the first protocol Long and Liu [20], this branch has developed a great deal. Numerous protocol schemes based on different quantum resources single photon, EPR pairs, cluster states, de-coherence free states, GHZ states, etc. are proposed [7, 28, 22, 6].

The scarcity of quantum resources and high-cost implementation has inspired the researchers to come up with the hybrid method of Semi Quantum Key Distribution protocol (SQKD) [2]. In this branch, one user is quantum capable while the other is classical- who can perform operations in computational basis $\{ |0\rangle, |1\rangle \}$ only along with using delay lines. Security proof of SQKD protocols has been established [16, 40].

Instead of generating a key with a classical user, protocol for the direct transmission of a message from a classical party was first proposed by Zou et al. [41] and this became the basis of a new branch known as Semi Quantum Secure Direct Communication (SQSDC) protocols. In the last decade, significant work has been carried out by researchers in this field.

This review paper has included five distinct protocols of SQSDC, based on different methods and quantum resources -Single photons, EPR pairs, Cluster states, mediated-third party, Degree of freedom in polarization mode and Spatial mode [41, 24, 33, 23, 38]. In this review paper, we have compared and analyzed their security and efficiency.

This study is organized as follows- in the next Section- a general description of the components of SQSDC protocols is given. Section III includes a brief review of five SQSDC protocols, thereafter in section IV security analyses are done. Efficiency calculations are shown in section V, and finally in section VI discussion and conclusion are provided.

## 1 General Description of Terms in SQSDC Protocols

Alice and Bob are traditional names of legitimate users, Eve is the eavesdropper or attacker while a Third party generally known as Charlie sometimes is a mediator as shown in figure1. In semi-quantum communication protocols, a classical user is capable of

(a) reflecting the qubit without disturbing it known as the CTRL operation

(b) measuring the received qubit in Z basis $\{ |0\rangle\ |1\rangle \}$

(c) preparing the qubit in Z basis $\{ |0\rangle\ |1\rangle \}$ as per the measurement result to return. Both (b) and (c) constitute SIFT operation

(d) using delay lines to re-arrange the order of received qubits

Boyer et al. gave the first semi-quantum key distribution protocol and proved it to be completely robust [2]. Robustness implies that Eve's chance of gaining information on secret message also puts her at risk of detection by legitimate users with the error rate estimation.

## 2 Review of SQSDC protocols

### 2.1 Three Step SQSDC Protocol

Zou et al. [41] implied the idea of sending a message directly to the user without establishing a shared key in the scenario of a classical user as a communicating party. Here Alice is the classical user and sender of the secret message. This protocol is as follows-

Step 1: Quantum user prepares $4n(1 + \delta)$ polarized single photons randomly in one of the Z or X basis $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ states and sends them to Alice as A-batch.

Step 2: Alice randomly selects qubits from the received A-batch to make up the S-batch for the A-batch transmission security check. For each S-batch photon, Alice randomly performs either CTRL or SIFT operation. Information about the position of S-batch qubits, the operation used, and measurement results are announced to Bob, who estimates the error rate for both CTRL qubits and SIFT qubits.

Step 3: On confirmation of security by error rate below the threshold level Bob publishes the Z basis photons position for the remainder T-batch (T=A-S). Z basis photons of T-batch are called the B-batch. Alice checks whether the B-batch is large enough i.e. the number of B-batch qubits greater than or equal to the length of the secret message (M), if so Alice computes the coded secret message as $\hat{M} = M \parallel H(M)$ using a collision-free one-way hash function and encodes her message onto the B-batch qubits using the following rules -

(i) qubit is unchanged if the $\hat{M} = 0$.

(ii) flips the qubit, i.e. measures it in Z basis and prepares a fresh qubit in the opposite state of the measurement result, for $\hat{M} = 1$.

These encoded photons are sent back to Bob.

Step 4: Bob can decode the secret message by measuring the B-batch photons and comparing the result with the initial states of these qubits and obtain $M' \parallel h'$.He checks if $H(M') = h'$ to accepts the $M'$ as un-tampered. This protocol has a robustness similar to the SQKD protocol. The quantum channel was assumed to be ideal, i.e., noiseless and lossless.

### 2.2 SQSDC protocol using Entanglement

Deng et al. designed the first EPR pairs block-based QSDC protocol and established the standards to match for a protocol to be a direct secure communication protocol known as DL-Criteria [8]. This criteria requires that-

(i) Legitimate users can read out the secret message directly from received qubits without needing additional classical information after the transmission of qubits.

(ii) Eve cannot get any valid information of secret message encoded in qubits even if she intercepts the qubits and may get hold of the channel.

Advancement of SQSDC protocols based on EPR states has garnered attention from researchers and many SQSDC schemes have been proposed. SQSDC protocols based on EPR pairs were given [32, 39, 27] but these protocols needed additional classical information after data transmission whereas [21, 30] needed to pre-share a secret key between users. Thus these protocols deviate from the DL criteria of secure direct communication.

In 2020 Rong et al. proposed three SQSDC protocols based on Entanglement, with EPR pairs, with GHZ

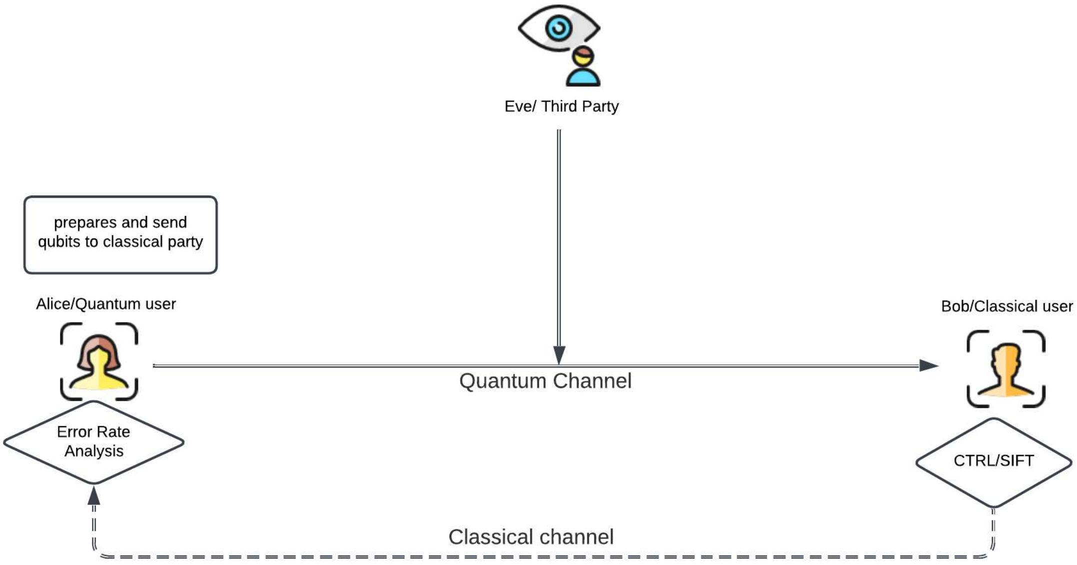

**Figure 1:** A Generalise view of SQSDC Protocol

state for three parties, and generalized it to N-party protocols [24]. We have included only one protocol based on Bell state in this study. In this protocol, a message can be transmitted either way i.e. from quantum to classical user or from classical to quantum user, step 4 and 5 are different while steps 1-3 are the same. Here Alice is quantum capable and Bob is a classical party -

Step 1: Quantum user prepares $N = 4n(1+\delta)$ EPR pairs in $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ Bell state, and divide them into two ordered sequences $S_a$-Home sequence and $S_b$-Travel sequence by taking one qubit from each EPR pair. Alice sends the $S_b$ to Bob over the quantum channel.

Step 2: Bob randomly chooses to either reflect the qubits i.e. CTRL or to measure it with Z basis and replace it with freshly prepared qubits i.e. SIFT. Measurement result in the SIFT process is stored in a classical string $S_c$. The number of SIFT qubits should not be below $n$ to go to the next step.

Step 3: After Alice announces the receipt of all $S_b$ qubits back, Bob publishes the position of CTRL and SIFT in $S_b$. For detecting Eve, Alice does the Bell State Measurement (BSM) on qubits for CRTL position in $S_b$ and its corresponding qubit $S_a$. Alice records the string $S'_c$ using the first $n$-values of Z basis measurement result on $S_a$ qubits corresponding to SIFT position in $S_b$.

*For message transmission from Bob to Alice*

Step 4: Bob chooses first $n$-bits of $S_c$ as $S''_c$ and produces code sequence $S_e$ for secret message $S_m$ using the bit-wise XOR operation on $S''_c$ and $S_m$. The Code sequence $S_e$ is again encoded into Z basis qubits as $S'_e$ and sent to Alice.

Step 5: Alice measures qubits on receiving the $S'_e$ in Z basis to get the result sequence $S''_e$. She decodes the message as $S_d$= $S''_e \oplus S_c = S_e \oplus S'_c = S_m \oplus S''_c \oplus S'_c = S_m$ as $S'_c = S''_c$ because initially generated EPR pairs are fixed to be in $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ Bell state.

*For message transmission from Alice to Bob*

Step 4: Alice chooses first $n$-bits of $S'_c$ as $S''_c$ and produces code sequence $S_e$ for secret message $S_m$ using the bit-wise XOR operation on $S''_c$ and $S_m$. The $S_e$ is again encoded into Z basis qubits as $S'_e$ and sent to Bob.

Step 5: Bob measures qubits on receiving $S'_e$ in Z basis to get the result sequence $S''_e$. He decodes the message using the first $n$-bits of string $S_c$. Thus $S_d$= $S''_e \oplus S_c = S_e \oplus S_c = S_m \oplus S''_c \oplus S_c = S_m$ as the first $n$ bits of $S_c = S''_c$ because EPR pairs are fixed to be in $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ Bell state.

## 2.3 Multi-party SQSDC protocol with cluster states

Quantum Entanglement is one of the most important phenomena of quantum mechanics used in quantum communication. Bell pairs and GHZ-states are examples of two qubits and three qubits maximal entanglement states respectively. Entanglement in a higher number of qubits is unalike the GHZ state generalized to

N-qubits and shows strong entanglement. Hans has defined the cluster states possessing persistent entanglement and stable self-associated structure [3]. In such states, Entanglement among all qubits is not destroyed by the measurement of a qubit. Cluster states are used as the qubit resource in QSDC protocol to improve efficiency [6] whereas a multi-party SQSDC protocol based on four correlated particles was given by Xu et al. in 2020 [33]. The four-particle cluster state is given as-

$$|\Phi\rangle_{1234}) = \frac{1}{2}(|0000\rangle + |0110\rangle + |1001\rangle - |1111\rangle)_{1234}$$
$$= \frac{1}{\sqrt{2}}(|0\rangle|\phi^+|0\rangle + |1\rangle|\phi^-\rangle|1\rangle)_{1234}$$

or

$$= \frac{1}{\sqrt{2}}(|0\rangle|\phi^+|0\rangle + |1\rangle|\phi^-\rangle|1\rangle)_{2143} \qquad (1)$$

Here the subscript 1234 indicates the four correlated particles. In this SQSDC protocol both users, Alice and Bob, are classical capable whereas the third-party Charlie is quantum capable. This protocol is as follows-

Step 1: Quantum user generates $N = 2n(1+\delta)$ ordered four-particle cluster states and divides these cluster states into four sequences $S_1, S_2, S_3$, and $S_4$ then sends over the $S_1$ and $S_2$ to Alice and Bob respectively while storing the $S_3$ and $S_4$ to himself.

Step 2: Classical users randomly adopt the received qubit either as a checking qubit or as a coding qubit thus each user Alice/Bob obtains a checking sequence $S_{checka}/S_{checkb}$ and a coding sequence $S_{codea}/S_{codeb}$. For each $S_{checka}/S_{checkb}$ qubit Alice/bob randomly implements either the CRTL operation or the SIFT operation, whereas the $S_{codea}/S_{codeb}$ qubits are operated on with the operation as per the bit-value of the message being 0 or 1 as follows-

(i) if $m_a/m_b = 0$ then qubit is reflected undisturbed.

(ii) if $m_a/m_b = 1$ then the qubit is measured and replaced with the opposite qubit.

Classical users reorder the reflected qubits after recording their order using the delay lines.

Step 3: Charlie the quantum user, stores all reflected qubits in two N-qubit registers. Alice and Bob publish the correct order, chosen operation, and measurement result for $S_{checka}$ and $S_{checkb}$ qubits respectively after receiving the receipt from Charlie for all reflected qubits. Eve detection cases as per Alice and Bob's qubit position and their choice of operation on their respective qubits and Charlie's measurement action are summarized in table 1. These measurement results are used to check if they are as per the correlation of equation (1) for Eve detection.

Step 4: If no Eve is detected in step 3, Alice and Bob publish the correct order for their coding sequences. Charlie restores the correct order and measures the coding sequences and remaining particles of $S_3$,$S_4$ in Z basis. Charlie can read out messages by comparing the measurement results of coding particles with the results of $S_3$ and $S_4$. Alice and Bob compute the checksum value using a one-way hash function for their message strings and announce their checksum values. Charlie computes the checksum values of retrieved messages and accepts messages as undisturbed if and only if his checksum values are the same as the announced ones by Alice and Bob.

### 2.4 Mediated SQSDC protocol

To further minimize the quantum resource requirements in semi-quantum communication protocols, schemes with two classical users communicating with the assistance of a fully quantum server were developed. Krawec proposed a mediated-SQKD (MSQKD) protocol with two classical users and an untrusted fully quantum third party (TP) [15]. The concept of mediated-SQKD protocols is utilized to develop the mediated-SQSDC (MSQSDC) protocol. Rong et al. proposed an MSQSDC protocol with two classical users and one untrusted quantum third party (TP) in 2021 [23]. TP prepares the Bell states and measures the qubits with a Bell basis. The four bell states are as

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$$

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$$

This protocol involves the following steps-

Step 1: TP prepares $N = 16n(1+\delta)$ EPR pairs in $\psi^+$ Bell states as $S_{ab}$ and constitutes ordered sequences $S_a$ and $S_b$ by taking one qubit from each EPR pair. TP send $S_a$ to Alica and $S_b$ to Bob.

Step 2: Alice and Bob randomly select SIFT or CRTL for each received qubit and return all qubits to TP.

Step 3: TP reassemble all returned qubits from Alice and Bob as $S'_{ab}$ and measure them with the Bell basis. As per the result of BSM, TP sends the message M to classical users as

(i) If BSM result is $\psi^-$, sends $M = 0$.

(ii) If BSM result is $\psi^+$ (in case of noise BSM result could be $\phi^{\pm}$ too ), sends $M = 1$. After TP announcement of $M$ Alice and Bob publish their opera-

**Table 1:** Charlie's measurement action as per the position of Classical users qubits and their action on them respectively

| Case/Action | Alice's Action | Bob's Action | Charlie's Action |
|---|---|---|---|
| Case 1: both qubit $S_1, S_2$ are in checking sequences | CTRL | CTRL | BSM on either $S_1, S_4$ or $S_2, S_3$ remaining in Z basis |
| | CTRL<br>SIFT | SIFT<br>CTRL | BSM on CTRL and its corresponding in $S_1, S_4$ / $S_2, S_3$ and Z basis measurement on SIFT $S_2$ / $S_1$ |
| | SIFT | SIFT | All in Z basis |
| Case 2: one is in checking and the other is in coding sequence (assuming qubit of $S_1$ is in checking) | CRTL | - | BSM on $S_1, S_4$ and Z basis on $S_3$ |
| | SIFT | - | Z basis on $S_1, S_4$, and $S_3$ |

tions SIFT/CRTL for each qubit in the classical channel. The initial state being $\psi^+$, if Alice and Bob both opt to CRTL on their respective qubit, corresponding to the same Bell state, they expect the result of BSM to be $\psi^+$ i.e. TP is supposed to announce $M = 1$, these are noted as CRTL-CRTL bits all other cases for CRTL-CRTL are considered errors. The error rate for CRTL-CRTL bits is checked to be lower than the preset threshold value to proceed further otherwise the process is halted. The error rate estimation in CRTL-CRTL bits provides security of the channel.

Step 4: Alice and Bob consider the qubits of Bell states where they both have used the SIFT operation on their qubits. These are called SIFT-SIFT bits and the BSM result for this case will be $\psi^+$ or $\psi^-$ with equal probability. Alice and Bob consider the SIFT-SIFT bits with TP announcing $M = 0$, the number of these should be greater than $2n$ to continue the protocol otherwise it is aborted here and starts from the beginning. Alice and Bob randomly select $n$ bits to be Test bits from SIFT-SIFT bits, and check for the errors on these Test bits using their measurement result values for SIFT operation. The initial state being $\psi^+$, the value of their measurement result must be opposite. This provides the security of SIFT-SIFT bits.

Step 5: Alice tells Bob that the first $n$ bits of remaining SIFT-SIFT bits are taken as Code bits as string $S_c = (S_{c1}, S_{c2}, ..., S_{cn})$ and Code sequence $S_e$ is produced using XOR operation between $S_c$ and secret message string $S_m$ i.e. $S_e = S_c \oplus S_m$. Alice encoded the $S_e$ into Z basis as $S_e'$ and sent it to Bob through TP. Bob on receiving $S_e'$ measures the qubits and records the result as $S_e''$. Bob can decode the secret message using the first $n$ bits of the remaining SIFT-SIFT bits $S_c'$. So decoded $S_d = S_e'' \oplus S_c' \oplus 1 = S_m \oplus S_c \oplus S_c' \oplus 1 = S_m$ as $S_c'$ and $S_c$ are opposite.

### 2.5 SQSDC with single photons in both polarization and spatial mode degree of freedom

Improving the channel capacity has drawn the attention of researchers and the concept of hyper-entanglement and hyper-dense coding using photon pairs in both polarization and spatial mode degree of freedom (DoF) came into existence as a tool to increase the number of bits carried per qubit [11, 31]. In 2012 Liu et al. presented the high capacity QSDC using single photons in both polarization and spatial mode DoF [19]. The local unitary operators in each DoF are used to encode the secret message. Bob can read out the message directly after transmission. Each photon carries 2-bits of secret message thus doubling the capacity compared to DL04 QSDC protocol [8] based on single photons only in polarization mode. The polarization and spatial mode DoF in single photons has been used for multiparty QSDC protocol [29]. Single photon state in both polarization and spatial mode DoF is described as $|\phi\rangle = |\phi\rangle_p \otimes |\phi\rangle_s$, here $|\phi\rangle_p$ is polarization mode DoF and $|\phi\rangle_s$ is in spatial mode DoF. Two non-orthogonal measuring basis for each mode are as

$$Z_p\{|H\rangle, |V\rangle\}$$

$$X_p\{|S\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle), |A\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)\}$$

and

$$Z_s\{(|b_1\rangle, |b_2\rangle\}$$

$$X_s\{|s\rangle = \frac{1}{\sqrt{2}}(|b_1\rangle + |b_2\rangle), |a\rangle = \frac{1}{\sqrt{2}}(|b_1\rangle - |b_2\rangle)\}$$

$|H\rangle$ and $|V\rangle$ are horizontal and vertical polarisation while $|b_1\rangle, |b_2\rangle$ are upper and lower spatial mode. A beam splitter produces the spatial mode of an already polarised single photon. SQSDC protocol with single photons in both polarization and spatial mode DoF [38] is as follows-

Step 1: Quantum user, Alice prepares $N = 2.5n(1+\delta)$ single photons in both polarization and spatial mode DoF each randomly in one of the sixteen $\{(|H\rangle \otimes |b_1\rangle), (|V\rangle \otimes |b_1\rangle), (|R\rangle \otimes |b_1\rangle), (|A\rangle \otimes |b_1\rangle), (|H\rangle \otimes |b_2\rangle), (|V\rangle \otimes |b_2\rangle), (|R\rangle \otimes |b_2\rangle), (|A\rangle \otimes |b_2\rangle), (|H\rangle \otimes |s\rangle), (|V\rangle \otimes |s\rangle), (|R\rangle \otimes |s\rangle), (|A\rangle \otimes |s\rangle), (|H\rangle \otimes |a\rangle), (|V\rangle \otimes |a\rangle), (|R\rangle \otimes |a\rangle), (|A\rangle \otimes |a\rangle)\}$ states, and sends them to Bob one by one i.e. second photon is transmitted only after receiving back the first one. Here $n = l + k$, $l$ is the length of secret message $I$, and $k$ is the length of the one-way hash function value of input $I$.

Step 2: For each received qubit Bob chooses to SIFT i.e. measuring with $Z_p \otimes Z_s$ basis and returning qubit in $Z_p \otimes Z_s$ basis, with probability 9/10 or to CRTL i.e. reflected undisturbed with probability 1/10

Step 3: Alice notifies Bob of receiving qubits back and continues the security check with Bob. Bob randomly selects 1/9 single photons from SIFT qubits, known as SIFT-CHECK single photons. Bob publishes the position of CRTL, SIFT-CHECK qubits, and measurement results of SIFT-CHECK single photons. Alice computes the error rates for both CRTL and SIFT-CHECK qubits with the help of Bob's published information and her knowledge of the initial state prepared, measurement result in the preparing basis for the CRTL, and measurement result in $Z_p \otimes Z_s$ basis for SIFT-CHECK qubits. If error rates of both CRTL and SIFT-CHECK single photons are low enough protocol moves ahead to the next step otherwise stops here.

Step 4: For the remaining SIFT single photons Alice announces the positions of which were prepared in $Z_p \otimes Z_s$ basis known as SIFT-Message single photons. The number of these is $n(1+\delta)$ and Bob randomly selects $n/2$ out of these SIFT-Message single photons to produce the classical $n$-bit string $M$ as per table 2.

**Table 2:** Producing Classical $n$ bit string from Measurement result of $n/2$ SIFT Message single photons

| Measurement result of $t^{th}$ SIFT-Message single photons $t = 1, 2 \ldots n/2$ | Classical bits produced for $2t^{th}$and $2t-1^{th}$ position of string M |
|---|---|
| $\|H\rangle + \|b_1\rangle$ | 00 |
| $\|H\rangle + \|b_2\rangle$ | 01 |
| $\|V\rangle + \|b_1\rangle$ | 10 |
| $\|V\rangle + \|b_2\rangle$ | 11 |

Bob computes $\hat{M} = M + I \parallel HS$ using $M$ and secret message bits concatenated with the hash value of the one-way hash function with the secret message as input. From $\hat{M}$ Bob generates the single photons in $Z_p \otimes Z_s$ basis as per the table 3 and sends them to Alice.

**Table 3:** Producing Single photons in $Z_p \otimes Z_s$ basis using the bit values of $\hat{M}$

| If $2t^{th}$and $2t - 1^{th}$ value of bits in $\hat{M}$ are | Generated single photons for $t^{th}$ position in $Z_p \otimes Z_s$ basis |
|---|---|
| 00 | $\|H\rangle + \|b_1\rangle$ |
| 01 | $\|H\rangle + \|b_2\rangle$ |
| 10 | $\|V\rangle + \|b_1\rangle$ |
| 11 | $\|V\rangle + \|b_2\rangle$ |

Step 5: Alice measures the fresh single photons in $Z_p \otimes Z_s$ basis and gets the classical bit sequence $\hat{M}$. Bob tells the position of chosen SIFT-Message single photons. Alice produces the $M$ string, with the same rules as used by Bob, using the position information of SIFT-Message single photons and their initial basis in which they were prepared by her. Alice retrieves $I \parallel HS$ using $\hat{M} + M$ and checks whether $HS$ is the same as $h(I)$ or not to know if the message has been tampered or not.

## 3 Security Analysis

The term *unconditional security* used regarding the security level of QKD/ SQKD protocols does not implicate absolute security rather it is called so as there are no restrictions on computational resources or manipulation power of the quantum attacker/eavesdropper Eve [25]. This security is based on the principles of quantum mechanics, any attempt to gain information on transmitted qubits requires interaction with them which causes the detectable disturbance in quantum states. The following assumptions are considered for this - (i)

Alice and Bob have secure devices so Eve canât get any info on prepared states. (ii) Random number generator is unbiased. (iii) Classical channel is authenticated. (iv) Eve's powers are within the laws of quantum physics. This is more of a theoretical concept in ideal conditions like noise-less and loss-less channels.

The robustness of any protocol is its resilience to the maintenance of its security considering the effects of imperfect devices and losses of channels i.e. closer to the security in a practical scenario. Security from side-channel attacks and eavesdropping is achieved with error correction methods, fault tolerance, and careful design for the optimization of protocols. *Theorem-1* in [2] is proof of the robustness of the protocol. The resilience against Eve's General-Attack strategy, which is comprised of two unitary operators $U_E$ and $U_F$ acting on qubits during transmission from Alice to Bob and back to Alice is provided in this theorem. If the Implementation of $U_F$ is based on the knowledge obtained from $U_E$, these two unitaries share a common probe space otherwise two independent unitaries are to be considered of composite system. For Eve, to induce no error on CRTL bits and Test bits it is proven that the final state of Eve's probe is independent of Bob's operation choice thus no useful information is gained by Eve. This theorem establishes a security level of robustness against various attacks on SQSDC protocols. Attacks mentioned in reviewed SQSDC protocols are described here.

### 3.1 Trojan Horse Attack

Trojan horse attack (THA) exploits the quantum channel as a potential tool to gain information about quantum states prepared by the quantum user. This attack is launched by sending a light pulse same as Bob, in the quantum channel during the time window of legitimate users and then analyzing the back-reflected light to know about the apparatus of Alice [13]. It is counter measured by reducing the maximum information gain attained by Eve through this attack. Additional privacy amplification and auxiliary detectors to monitor the incoming light are included in the design of quantum communication system to improve the secure bit rate. The Delay Photon THA involves the interception of the transmitted signal and inserting a photon of shorter time than the time windows, thus doesnot click on the detectors [13, 9]. As a single photon detector is sensitive only to a special wavelength Eve utilizes the spy photon of faraway wavelength compared to the one used by Alice and Bob thus making the spy photons invisible to single photon detectors, this attack strategy is known as invisible photon THA [9, 5]. These can be counter-measured by implementing a photon number splitter device and wavelength filters.

### 3.2 Intercept and Re-send Attacks

In the intercept and resend attack, Eve intercepts the quantum states sent by the sender and measures them, and prepares quantum states according to her measurement result. These new quantum states are then transmitted to the receiver. Quantum mechanics fundamentals No-cloning theorem and collapse of states on measurement provide security against this type of attack. The disturbance introduced by Eve's measurement process manifests an increase in the quantum bit error rate (QBER) [18]. Decoy photons in all four basis $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ are also used to provide security against such attacks [37].

### 3.3 Modification Attacks

This attack is considered to be a special case of denial-of-service attack. Eve modifies the message sent by Alice without detection i.e. without inducing errors, though Eve is not able to know the message, but can make the message unreliable. Protocols based on ping-pong way of quantum state transmission are porn to such attacks. Eve captures the qubit during the encoded message transmission and measures with Z basis. She either sends the qubit as the measurement result or replaces the captured qubit with a new qubit prepared in the non-orthogonal basis [5, 36, 35]. The one-way hash functions are used to improve the authentication against such attack [5, 36].

### 3.4 Double C-Not Attack

A sequence of photons used as ancilla and C-Not gate between the transmitted qubit as control and ancilla as target qubit is a powerful tool for Eve to extract information without being detected [17, 34, 14]. Both types of qubit sources single photon and EPR are prone to double C-Not attack. This attack gains information without being detected by legitimate users provided Eve can distinguish the checking states from the message-carrying states [12].

Zou et al. protocol [41] is secure against eavesdropping as the T-batch transmission is secure just like in SQKD protocol [2]. The encoding of the secret message is identical to the classical one-time pad encryption with random states which is completely safe as no information can be obtained even if the cipher text is intercepted. A one-way hash function is further used

**Table 4:** Security of SQSDC protocols

| Protocol | Qubit carrier | Robustness | Other Security measure |
|---|---|---|---|
| Zou et al.[41] | Single Photon | Robustness against eavesdropping,THA,I and R Modification | OTP like encryption, One-way Hash Function |
| Rong et al.[24] | Bell-States (GHZ, GHZ-ike state) | Robustness against General attack strategy, | XOR for OTP like encryption |
| Xu et al.[33] | Four Particle Cluster State | Secure against Common Individual attack Strategy | One-way Hash function |
| Rong et al.[23] | Bell State | Robustness against General attack strategy | XOR for OTP like encryption |
| Yu Ye et al.[38] | Single Photons with polarisation and spatial mode DoF | Robustness against General attack strategy | OTP like encryption, One-way Hash Function |

to check the integrity of the secret message. Similarly, the security measures and robustness of protocols [24],[33],[23], and[38] are summarised in table 4

## 4 Efficiency

Concerning quantum resources efficiency can be understood as the measurement of the quantum resource used for sending a secret message bit. This is given [4] as

$$\eta = \frac{b_s}{q_t + b_t} \times 100\%$$

Here $b_s$, $q_t$, and $b_t$ are the number of secret bits received, total qubits generated, and classical bits needed by communicators. Classical bits needed for detecting Eve are ignored here and $\delta$ being very small is also not considered in this estimation of efficiency. For [41] quantum user initially prepares $4n$ qubits and $n$ qubits are generated in the SIFT process and $n/2$ in the encoding of $\hat{M}$ being 1 considered to appear with probability half of secret bits. Hence the efficiency $\eta = 18.18\%$. In [24] for sending n bits of secret message $2n$-EPR pairs are generated i.e. $4n$ qubits in the first step then $n$ qubits are produced in SIFT operation and again $n$ qubits are used for encoding of message bits thus giving $\eta = 16.66$. Similarly efficiency of [33],[23], and [38] is calculated as in Table 5.

**Table 5:** Efficiency of SQSDC protocols

| Protocol | $b_s$ | $q_t$ | $Efficiency(\eta)$ |
|---|---|---|---|
| Zou et al.[41] | n | 4n+n+0.5n | 18.18 |
| Rong et al.[24] | n | 4n+n+n | 16.66 |
| Xu et al.[33] | 2n | 4n+n+n | 33.33 |
| Rong et al.[23] | n | 32n+16n+n | 2.04 |
| Yu Ye et al.[38] | n | 2(2.5n+2.25n+0.5) | 9.52 |

## 5 Discussion and conclusion

This paper has presented a comprehensive review of SQSDC protocols with different kinds of qubit carriers and various communicator participation. First SQSDC protocol [41] based on single photons shows the secret message transmission from a classical user to a quantum user only, whereas [24] with EPR pairs offered the transmission of secret message in either direction from classical to quantum user or from quantum to classical user. This protocol did not establish responding to a message by the receiver, which is required to develop the semi-quantum dialogue (SQD), and further research in this aspect is also of interest.

SQSDC protocol with cluster states [33] delivered the multi-party communication, here Charlie is a quantum participant whereas we have two classical participants Alice and Bob. An SQD has also been proposed as an extension of the SQSDC with a cluster state. The efficiency is higher with cluster state but their security is checked against individual attacks only and research for the improvements in robustness against more complex attacks is needed to address.

Protocol of [23] embark on a new branch further where two classical parties are the communicators and able to communicate securely with the assistance of a third party functioning as a quantum server even if the third party is dishonest. This protocol is robust as all outside attacks are involved in a dishonest third party. The efficiency is very low here and research for higher qubit efficiency is a gap to work on for researchers.

The polarization mode and spatial mode DoF of single photons are exploited to double the channel capacity in [38] protocol compared to the [41]. Improving the channel capacity by increasing the number of bits carried per qubit using the concept of hyper-entanglement and higher dimensions is also attracting researchers.

## References

[1] Bennett, C. H. and Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.*, 560:7–11, 2014.

[2] Boyer, M., Kenigsberg, D., and Mor, T. Quantum key distribution with classical bob. *Physical Review Letters*, 99(14), Oct. 2007.

[3] Briegel, H. J. and Raussendorf, R. Persistent entanglement in arrays of interacting particles. *Physical Review Letters*, 86(5):910â913, Jan. 2001.

[4] Cabello, A. Quantum key distribution in the holevo limit. *Physical review letters*, 85:5635–8, 01 2001.

[5] Cai, Q.-Y. Eavesdropping on the two-way quantum communication protocols with invisible photons. *Physics Letters A*, 351(1â2):23â25, Feb. 2006.

[6] Cao, Z., Song, D., Chai, G., He, C., and Zhao, G. Quantum secure direct communication based on four-particle cluster state grouping. *Chinese Journal of Physics*, 60, 02 2019.

[7] Deng, F.-G., Long, G. L., and Liu, X.-S. Two-step quantum direct communication protocol using the einstein-podolsky-rosen pair block. *Physical Review A*, 68(4), Oct. 2003.

[8] Deng, F.-G., Measurements, B., and Long, G. Secure direct communication with a quantum one-time pad. *Physical Review. A*, 69, 05 2004.

[9] Deng, F.-G., Zhou, P., Li, X.-H., Li, C.-Y., and Zhou, H.-Y. Robustness of two-way quantum communication protocols against trojan horse attack, 2005.

[10] Ekert, A. Quantum cryptography based on bell's theorem. *Physical review letters*, 67 6:661–663, 1991.

[11] et al, G. B. Atwo-step quantum secure direct communication protocol with hyperentanglement. *Chinese Phys. B 20 100309*, 2011.

[12] Gao, F., Lin, S., Wen, Q.-Y., and Zhu, F.-C. A special eavesdropping on one-sender versus n - receiver qsdc protocol. *Chinese Physics Letters - CHIN PHYS LETT*, 25:1561–1563, 05 2008.

[13] Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H. Quantum cryptography. *Reviews of Modern Physics*, 74(1):145â195, Mar. 2002.

[14] Gu, J. and Hwang, T. Double c-not attack on a single-state semi-quantum key distribution protocol and its improvement. *Electronics*, 11:2522, 08 2022.

[15] Krawec, W. O. Mediated semiquantum key distribution. *Physical Review A*, 91(3), Mar. 2015.

[16] Krawec, W. O. Security proof of a semi-quantum key distribution protocol: Extended version, 2015.

[17] Lin, C.-Y. and Hwang, T. Cnot extraction attack on "quantum asymmetric cryptography with symmetric keys". *Science China: Physics, Mechanics and Astronomy*, 57, 04 2014.

[18] Lin, T.-H., Yang, C.-W., and Hwang, T. Attacks and improvement on âquantum direct communication with mutual authenticationâ. *International Journal of Theoretical Physics*, 53, 10 2013.

[19] Liu, D., Chen, J.-L., and Jiang, W. High-capacity quantum secure direct communication with single photons in both polarization and spatial-mode degrees of freedom. *International Journal of Theoretical Physics*, 51:2923 – 2929, 2012.

[20] Long, G. L. and Liu, X. S. Theoretically efficient high-capacity quantum-key-distribution scheme. *Physical Review A*, 65(3), Feb. 2002.

[21] Luo, Y.-P. and Hwang, T. Authenticated semi-quantum direct communication protocols using bell states. *Quantum Information Processing*, 15, 02 2016.

[22] Qin, S.-J., Wen, Q., Meng, L., and Zhu, F. Quantum secure direct communication over the collective amplitude damping channel. *Science in China Series G Physics Mechanics and Astronomy*, 52:1208–1212, 08 2009.

[23] Rong, Z., Qiu, D., Mateus, P., and Zou, X. Mediated semi-quantum secure direct communication. *Quantum Information Processing*, 20, 02 2021.

[24] Rong, Z., Qiu, D., and Zou, X. Semi-quantum secure direct communication using entanglement. *International Journal of Theoretical Physics*, 59, 06 2020.

[25] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., DuÅ¡ek, M., LÃ¼tkenhaus, N., and Peev, M. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81(3):1301â1350, Sept. 2009.

[26] Shor, P. W. and Preskill, J. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441–444, Jul 2000.

[27] Sun, Y., Yan, L., Chang, Y., Zhang, S., Shao, T., and Zhang, Y. Two semi-quantum secure direct communication protocols based on bell states. *Modern Physics Letters A*, 2019.

[28] Wang, C., Deng, F., and Long, G. L. Multi-step quantum secure direct communication using multi-particle greenâhorneâzeilinger state. *Optics Communications*, 253:15–20, 2005.

[29] Wang, L., Ma, W., Wang, M., and Shen, D. Three-party quantum secure direct communication with single photons in both polarization and spatial-mode degrees of freedom. *International Journal of Theoretical Physics*, 55:2490–2499, 05 2016.

[30] Wang, M.-M., Liu, J.-L., and Gong, L.-M. Semiquantum secure direct communication with authentication based on single-photons. *International Journal of Quantum Information*, 17(03):1950024–, 2019.

[31] Wang, T.-J., Li, T., Du, F.-F., and Deng, F.-G. High-capacity quantum secure direct communication based on quantum hyperdense coding with hyperentanglement. *Chinese Physics Letters*, 28(4):040305, Apr. 2011.

[32] Xie, C., Li, L., Situ, H., and He, J. Semi-quantum secure direct communication scheme based on bell states. *International Journal of Theoretical Physics*, 57:1881–1887, 06 2018.

[33] Xu, L.-C., Chen, H.-Y., Zhou, N., and Gong, L.-H. Multi-party semi-quantum secure direct communication protocol with cluster states. *International Journal of Theoretical Physics*, 59:1–12, 07 2020.

[34] Yang, C.-W. Efficient and secure semi-quantum secure direct communication protocol against double cnot attack. *Quantum Information Processing*, 19, 12 2019.

[35] Yang, C.-W. and Hwang, T. Improved qsdc protocol over a collective-dephasing noise channel. *International Journal of Theoretical Physics*, 51, 12 2012.

[36] Yang, C.-W., Hwang, T., and Lin, T.-H. Modification attack on qsdc with authentication and the improvement. *International Journal of Theoretical Physics*, 52:2230 – 2234, 2013.

[37] Yang, C.-W. and Tsai, C.-W. Intercept-and-resend attack and improvement of semiquantum secure direct communication using epr pairs. *Quantum Information Processing*, 18, 08 2019.

[38] Ye, T.-Y., Geng, M.-J., Xu, T.-J., and Chen, Y. Semiquantum secure direct communication with single photons in both polarization and spatial-mode degrees of freedom, 2021.

[39] Zhang, M., Li, H., Xia, Z., Feng, X., and Peng, J. Semiquantum secure direct communication using epr pairs. *Quantum Information Processing*, 16, 2017.

[40] Zhang, W. and Qiu, D. Security of a single-state semi-quantum key distribution protocol. *Quantum Information Processing*, 17, 04 2018.

[41] Zou, X. and Qiu, D. Three-step semiquantum secure direct communication protocol. *Science China Physics, Mechanics Astronomy*, 57, 09 2014.