

Distributed six-qubit Decoherence Free State Quantum Secure Direct Communication Protocol with Classical Bob

Kiran Meena¹, Narayan Lal Gupta², Vivek Mandot³

^{1,2,3} Department of Research, GGTU, Village Badvi, Mahi Dam Road, Banswara, Rajasthan, India.

To Cite this Article: Kiran Meena¹, Narayan Lal Gupta², Vivek Mandot³, “Distributed six-qubit Decoherence Free State Quantum Secure Direct Communication Protocol with Classical Bob”, Indian Journal of Computer Science and Technology, Volume 05, Issue 02 (May-August 2026), PP: 928-937.



Copyright: ©2026 This is an open access journal, and articles are distributed under the terms of the [Creative Commons Attribution License](#); Which Permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Abstract: A distributed Decoherence Free Space (DFS) state structure based semi-quantum secure direct communication protocol is proposed here. Immunity of DFS states to collective dephasing as well as collective rotation is used to secure the quantum channel. We have used joint bell state measurement of DFS state to detect Eve. The six-qubit DFS state, composed of three singlet states, is used to encode three bits of information in communication. Distributed structure and bell state measurement along with logical invariance of DFS states is explored here for security against various attacks including Trojan Horse attack, Intercept and resend attack, Non unitary attacks Collective attack and establishes no information leakage even in the semi quantum settings.

Keywords: Semi quantum communication protocol, Collective noise, Coherent attack, DFS state, logical invariance.

I. INTRODUCTION

Quantum cryptography has developed significantly from quantum key distribution protocols [1, 2, 3, 4] to quantum secure direct communications protocols (QSDC)[5, 6, 7, 8] and various other branches, including quantum secret sharing protocols, device-independent protocols, and measurement-device-independent protocols. In 2007, Boyer et al. developed the first semi-quantum protocol for key distribution to address the issue of quantum resource scarcity [9] with the introduction of Classical Bob. Classical Bob have a limited quantum capacity that is restricted to z-basis measurement and generation of z-basis qubits. In 2014, Zou et al. [10] presented the first semi-quantum secure direct communication protocol (SQSDC), based on entangled states. Several SQSDC protocols have been proposed based on the various qubit resources[11, 12, 13, 14]. These SQSDC protocols are proposed to reduce the demand for quantum technology at the receiver, making them more practical than QSDC protocols. The security of these protocols is based on an Eve-detection method using induced errors and correlation disturbance. We have done comparative analysis of these protocols with the proposed scheme indicating its superior robustness to attacks and noises.

Quantum secure direct communication faces two key challenges. First, it must remain secure against a powerful quantum-capable eavesdropper, often referred to as Eve. Second, the message must be encoded directly on qubits and decoded at the receiver's end without losing integrity [5]. Security against Eve is also two-fold, first we want to secure the quantum channel to ensure that there is no information leakage to Eve. Second if Eve attacks the quantum channel in attempt to gain information, it should be detected. Another critical aspect is the ability to encode the message directly into the quantum state is a key feature of a QSDC protocol. It is necessary to ensure the integrity of the information transmitted through a quantum channel. In this study, we propose a scheme that uses the distributed six-qubit DFS state structure. Three qubits, one from each singlet state, are in the quantum channel, making them prone to Eve's attack. Due to partial access to the DFS state, Eve obtains the maximal mixed state, which leaks no information. We propose a scheme that maintains secrecy due to the logical invariance of the DFS state. This protocols security is information-theoretic based along with the test qubits to secure against coherent attacks, collective attack, non unitary attacks as well as side channel attacks of Eve. We are not using any key for encryption of the message before encoding it to the quantum state, making it a secure direct communication protocol.

In the next section, we will describe the DFS state. In the third section, we have given the detailed steps of the proposed protocol. The encoding and decoding rules are described with the distributed DFS state. The operations of the limited capacity sender, Bob, are restricted to reflect without disturbance and measure and prepare the state in the Z basis only. In the third section, a security analysis of the proposed protocol is presented. Here we have analyzed the security against the non-unitary and controlled rotation attack of Eve, and also see the security against other side channel attacks. In the fourth section, we discuss the proposed protocol by comparing it to the existing SQSDC protocols. In the final section, we conclude the contribution of this scheme with potential future work. Section text. See Subsection 3.1.

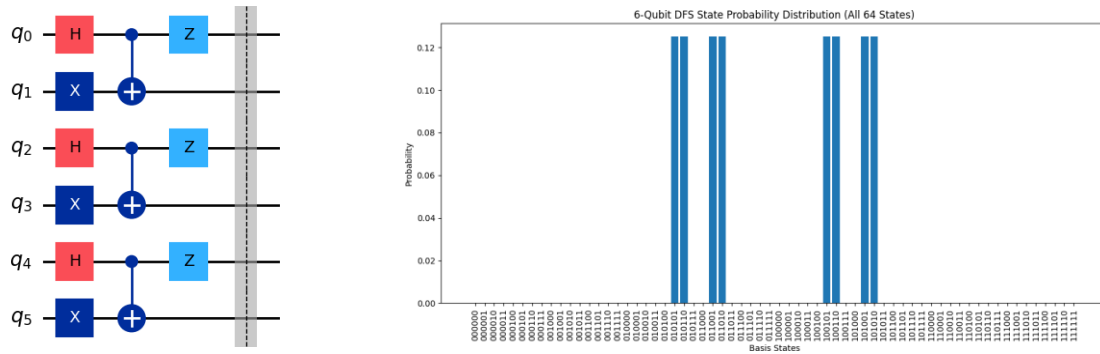


Figure 1: Quantum Circuit and State-Vector representation for Six qubit DF State.

II.DFS

The interaction of the qubit with its environment causes a loss of coherence, known as decoherence, leading to the loss of information. Decoherence has been of interest to researchers, and much research has been conducted that shows resistance of DFS to decoherence using symmetry of DFS Hilbert space [15, 16, 17, 18]. The invariance of DFS is shown as $\rho_N = (U(t))^{\otimes N} \rho_N U^\dagger(t)^{\otimes N}$ where $U(t)^{\otimes N}$ is the collective noise Unitary operator on N qubits. Schemes for DFS generation along with the invariance of logical coding has been analyzed in detail in [19, 20]. The proposed protocol uses the logical invariance of the DFS state to avoid information leakage to Eve.

III.SQSDC PROTOCOL BASED ON SIX-QUBIT DFS STATE

In this SQSDC protocol, Alice is quantum-capable, and Bob is classical-capable. Bob can either reflect the received qubit without disturbing it, known as the CTRL operation, or measure (in the Z-basis) and send the same qubit prepared in the Z-basis, known as the SIFT operation. In this paper, we refer to Bob's action of measuring and sending the opposite qubit in the Z-basis as SHIFT-flipped, which is hereafter denoted as SIFT-f.

3.1 DFS State preparation

Alice prepares the $N = (4n + \delta)$ six-qubit DFS state represented by the tensor product of three singlet states as follows:

$$|\Psi_{\text{DFS}}\rangle = \psi^-_{01} \otimes \psi^-_{23} \otimes \psi^-_{45}$$

Where

$$|\psi^- \rangle_{ij} = \frac{1}{\sqrt{2}}(|0\rangle_i |1\rangle_j - |1\rangle_i |0\rangle_j)$$

On expanding the tensor product terms, we get

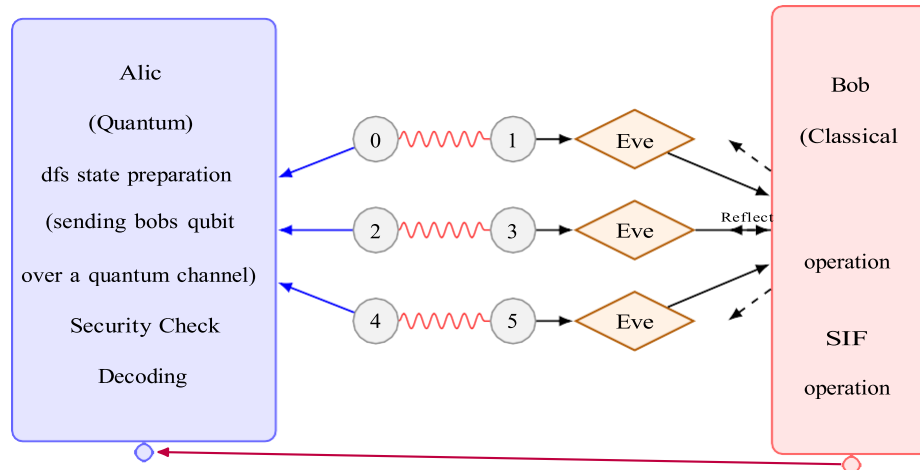
$$|\Psi_{\text{DFS}}\rangle = \frac{1}{\sqrt{8}}(|010101\rangle - |010110\rangle - |011001\rangle + |011010\rangle \\ - |100101\rangle + |100110\rangle + |101001\rangle - |101010\rangle)_{012345}$$

Alice divides each DFS into two sequences consisting of qubits (0, 2, 4) as S_a and qubits (1, 3, 5) as S_b . She keeps sequence S_a to herself and sends sequence S_b to Bob, the Classical user, over a quantum channel.

3.2 State transmission and Bob's Action

Alice transmits qubits of the S_b one-by-one DFS state; that is, she sends the qubits of the next DFS only after receiving the qubits of the previous DFS from Bob. On receiving the DFS qubits, Bob randomly selects them as either the coding sequence or the checking sequence. For each qubit of state chosen in the checking sequence, Bob randomly performs either the CTRL operation or the SIFT operation. He keeps a record of position and Figure 2: Schematic Diagram for the proposed SQSDC protocol. Alice, quantum party generates DFS states and sends 1,2,3 qubits to Bob keeping 0,2,4 qubits to herself. Bob randomly selects as check or code state. He performs the SHIFT or CTRL operation on checking sequence at random, and encode message as per encoding rules on coding sequence except of those selected as test states. Alice checks channel security using check sequence position, operation and measurement result along with the test states. On passing these checks alice readsout the message as per decoding rules.

Measurement results, which he uses with Alice to determine the channel security. He randomly selects the qubits in the coding sequence as the test qubits on which CTRL operation or SIFT operation is performed randomly to check the integrity of the message.



3.3 Encoding of information

For each received DFS state qubit selected as a checking sequence, Bob randomly performs the CTRL or SIFT operation. Similarly, on the qubits of DFS selected as the coding sequence, he encodes the message using the CTRL operation or the SIFT-f operation as per the message bit value, except for the randomly selected test states, where the CTRL operation or the SIFT operation is performed to check the integrity of the message. The encoding of the message is as per the following rules:

- To encode message bit 000, Bob reflects all the qubits of a DFS state.
- To encode the message bits 001, 010 and 100, Bob performs the SIFT-f operation on the 1, 3 and 5 qubits, respectively, reflecting the remaining qubits of the DFS state.
- To encode 011, 101 and 110, Bob performs the CTRL operation on the 1, 3 and 5 qubits respectively, and SIFT-f on the remaining qubits of the DFS state.
- To encode 111, Bob performs the SIFT-f operation on all qubits of the DFS state.

3.4 Eve's detection and channel security

The security of the channel is assessed using the checking sequence. In this sequence for the CTRL position, Alice performs the Joint DFS measurement, along with the X and Y parity checks for each singlet in DFS state. If there is no disparity and no error in the Joint DFS measurement, Alice and Bob use the SIFT operation results to check the correlation as in Table-1, which provides a safeguard against denial-of-service attacks. Only after confirming the security of the channel and the absence of eavesdropping, Alice and Bob use the test qubit position, operation performed, and measurement results to establish the integrity of the message in the coding sequence. The remaining qubits are used to encode the message. Eve's attempt to access any information will lead to a disturbance in the entanglement of Alice and Bob's qubits. If there are no errors, Alice decodes the message from the coding sequence of qubits after verifying the integrity of the information.

3.5 Decoding of information

After the channel security confirmation from the checking sequence and test states, Alice measures the remaining qubits, corresponding to the DFS state, with Bob's qubit using the BSM for the qubits 01,23,45 and stores the result along with the position. After Alice announces receiving all the qubits, Bob announces the position of

<u>Qubits of S_a of DFS</u>	<u>Qubits of S_b of DFS</u>
$ 000\rangle_{024}$	$ 111\rangle_{135}$
$ 001\rangle_{024}$	$ 110\rangle_{135}$
$ 010\rangle_{024}$	$ 101\rangle_{135}$
$ 011\rangle_{024}$	$ 100\rangle_{135}$
$ 100\rangle_{024}$	$ 011\rangle_{135}$
$ 101\rangle_{024}$	$ 010\rangle_{135}$
$ 110\rangle_{024}$	$ 001\rangle_{135}$
$ 111\rangle_{024}$	$ 000\rangle_{135}$

Table 1: Correlation of S_a and S_b of the DFS state

his test qubits, the operation performed, and the measurement result. Alice checks the test qubits for message integrity. If no discrepancies are found, Alice decodes the message from the result of BSM on the DFS qubits as -

- (i) Message bit value is 000 if BMS on 01,23,45, results in 11,11,11
- (ii) Message bit value is 001, 010 and 100 if BMS on 01,23,45, results in $(|\phi^\pm\rangle, 11, 11)$, $(11, |\phi^\pm\rangle, 11)$ and $(11, 11, |\phi^\pm\rangle)$ respectively
- (iii) Message bit value is 011, 101 and 110 if BMS on 01,23,45, results in $(11, |\phi^\pm\rangle, |\phi^\pm\rangle)$, $(|\phi^\pm\rangle, 11, |\phi^\pm\rangle)$ and $(|\phi^\pm\rangle, |\phi^\pm\rangle, 11)$ respectively
- (iv) Message bit value is 111, if the BMS on 01,23,45, results in $|\phi^\pm\rangle, |\phi^\pm\rangle, |\phi^\pm\rangle$

IV. SECURITY ANALYSIS

The security of the proposed protocol is realized owing to the invariance of the logical qubit DFS state against both types of collective attacks, and randomly selected test states are used as a measure for any coherent attacks. In this scheme, we use a six-qubit DFS state that consists of three singlets, each of which is invariant under collective rotation (SU(2) singlet subspace), making the total state an 8-dimensional logical subspace within the 64 dimensional Hilbert space. We show that the DFS state provides an information-theoretic bound on Eve. We also analyzed the detection probability when Eve attempted to measure the traveling qubits to gain information. In the next step, we analyzed the detection probability of Eve when she performs a collective rotation attack on traveling qubits. Finally, we discuss security measures against common attacks.

4.1 Logical Invariance and Zero Information Leakage

Theorem 1 establishes an information-theoretic message secrecy that is independent of the eavesdropping detection. This guarantees that no measurement, including optimal collective or coherent measurements, can provide Eve with any information regarding the transmitted message. This security assurance is independent of fidelity thresholds, error-rate limits, or disturbance identification. Instead, it emerges from the logical invariance protected by symmetry within the six-qubit decoherence-free subspace. Consequently, any attack that enables Eve to gain nonzero information necessarily breaks the DFS symmetry and induces a detectable leakage outside the protected subspace. This takes the security analysis from numerical detection probabilities to a strong information-theoretic proof and sets the suggested protocol apart from other SQSDC methods whose security is essentially disturbance-based.

Theorem 1. Let a classical message $M \in \{0, 1\}$ be encoded by Alice into logical states $\{|\bar{0}\rangle, |\bar{1}\rangle\}$ spanning a six-qubit decoherence-free subspace (DFS) H_{DFS} . The logical states satisfy the following condition:

$$S_\alpha |\bar{m}\rangle = \lambda_\alpha |\bar{m}\rangle, \quad \forall m \in \{0, 1\}, \quad \forall \alpha, \quad (2)$$

where S_α are collective system operators and the eigenvalues λ_α are independent of m .

Alice retains three qubits and transmits the remaining three qubits to a classical (semi-quantum) Bob. Suppose an eavesdropper Eve performs an arbitrary collective attack on the traveling qubits, modeled by a joint unitary

$$U_{SE} = \exp\left(-i \sum_{\alpha} S_{\alpha}^{(T)} \otimes E_{\alpha}\right), \quad (3)$$

where $S^{(T)}$ collectively acts on the traveling subsystem.

Then Eve's reduced density matrix is independent of the encoded message, and the Holevo information between Eve and Alice's message satisfies

$$\chi(M : E) = 0. \quad (4)$$

Consequently, Eve obtains zero information about the message even if she remains undetected. *Proof.* The six-qubit DFS is constructed such that the collective operators decompose as

$$S_\alpha = S^{(A)} \otimes I^{(B)} + I^{(A)} \otimes S^{(B)}, \quad (5)$$

where (A) denotes Alice's retained qubits and (B) denotes the three traveling qubits sent to Bob. By the DFS condition,

$$\left(S_{\alpha}^{(A)} + S_{\alpha}^{(B)}\right) |\bar{m}\rangle = \lambda_{\alpha} |\bar{m}\rangle, \quad (6)$$

which implies

$$S_{\alpha}^{(B)}|\bar{m}\rangle = (\lambda_{\alpha} - S_{\alpha}^{(A)})|\bar{m}\rangle. \quad (7)$$

Eve interacts only with subsystem (B); therefore, the joint evolution of the system and Eve's ancilla $|E_0\rangle$ is

$$U_{SE}(|\bar{m}\rangle \otimes |E_0\rangle) = \exp\left(-i \sum_{\alpha} S_{\alpha}^{(B)} \otimes E_{\alpha}\right) |\bar{m}\rangle \otimes |E_0\rangle. \quad (8)$$

Substituting the DFS relation yields

$$U_{SE} = I_{\text{DFS}} \otimes \exp\left(-i \sum_{\alpha} \lambda_{\alpha} E_{\alpha}\right) \equiv I_{\text{DFS}} \otimes U_E. \quad (9)$$

Therefore,

$$U_{SE}(|\bar{m}\rangle \otimes |E_0\rangle) = |\bar{m}\rangle \otimes |E'\rangle, \quad (10)$$

where $E' = U_E E_0$ is independent of m .

Tracing out the system degrees of freedom yields Eve's reduced state.

$$\rho_E^{(m)} = |E'\rangle\langle E'| \quad \forall m, \quad (11)$$

As Eve's reduced state is independent of the encoded message bit, she does not gain any information. This result proves the Logical Invariance Theorem.

4.2 Security against Eves Non unitary attacks-

We analyze the detection rate for eavesdropping in the case of a Non-unitary Measurement attack model using the Kraus operator [21], where Eve's interaction with the traveling qubit introduces the disturbance that causes the detection of Eve's presence. The quantum channel with the Kraus operator measuring the qubit in the Z-basis with probability p is

$$\mathcal{E}_p(\rho) = \sum_k K_k \rho K_k^{\dagger}, \quad \{K_k\} = \left\{ \sqrt{1-p} \mathbb{I}, \sqrt{p} |0\rangle\langle 0|, \sqrt{p} |1\rangle\langle 1| \right\} \quad (12)$$

Operating $\mathcal{E}_p$ to the second qubit of a singlet density matrix $\rho^- = |\psi^-\rangle\langle\psi^-|$ we get

$$\rho' = (\mathbb{I} \otimes \mathcal{E}_p)(\rho^-) = (1-p)\rho^- + \frac{p}{2}(|01\rangle\langle 01| + |10\rangle\langle 10|), \quad (13)$$

$$(14)$$

Fidelity for one singlet state after the Kraus operation is

$$F_{\text{single}}(p) = \langle\psi^-|\rho'|\psi^-\rangle = (1-p)\langle\psi^-|\rho^-|\psi^-\rangle + \frac{p}{2} \sum_{b \in \{01,10\}} |\langle\psi^-|b\rangle|^2 \quad (15)$$

$$= (1-p) \cdot 1 + \frac{p}{2} \left(\frac{1}{2} + \frac{1}{2} \right) = 1 - \frac{p}{2} \quad (16)$$

Taking into account all three independent singlets of DFS, fidelity becomes

$$F_{\text{nonunitary}}(p) = \left(1 - \frac{p}{2}\right)^3, \quad (17)$$

probability of detection of Eve is

$$p_{\text{det}}^{(\text{nonunitary})}(p) = 1 - \left(1 - \frac{p}{2}\right)^3 \quad (18)$$

For the CTRL operation, Bob reflects all the qubits of the DFS state in the checking sequence. Eve does not know about the position of CTRL or SHIFT operation, to obtain maximum information she applies the attack equally on all the qubits. Therefor all three qubit in the CTRL operation of a DFS state undergoes the same attack, that is, p is one in non unitary attack. The detection probability is then

$$p_{\text{det}}^{(\text{nonunitary})}(p=1) = 1 - \left(1 - \frac{1}{2}\right)^3$$

$$p_{\text{det}}^{(\text{nonunitary})}(p) = 1 - \left(\frac{1}{2}\right)^3 \quad (19)$$

We obtained 87.5 per cent of detection from CTRL position when Eve attacks all traveling qubits, as shown in figure 3.

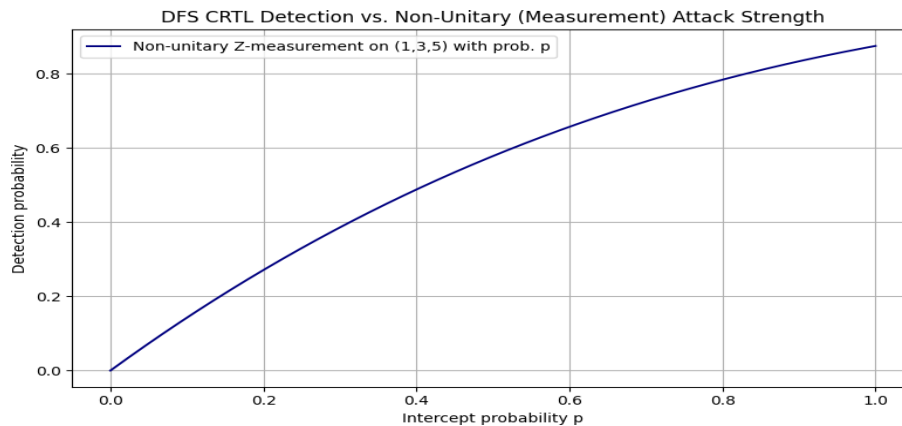


Figure 3: Detection probability vs. non-unitary Z-measurement probability p on traveling qubits.

4.3 Security against Collective Rotation on all traveling qubits

We have observed that any non-unitary attack will be detected owing to the disturbance of the coherence of the DFS state when Eve tries to obtain the information. Now, we will see when Eve applies a coherent rotation $R_y(\theta)$ on each traveling qubit (independently) while having no access to Alice's qubit. The quantum circuit for this is shown in, and the state vector shows that the information is not lost, but redistributed. Here, Eve does not attempt to obtain any information but wants to alter the qubits. In this case, the error in the CTRL qubits and the SIFT qubit correlation detects Eve's presence during checking sequence analysis. For smaller angles, this error is low as shown in Figure 5. The redistribution or loss of fidelity is also low there, but at higher angles, when the state fidelity is disturbed, it is detectable.

We have a singlet and rotation as follows

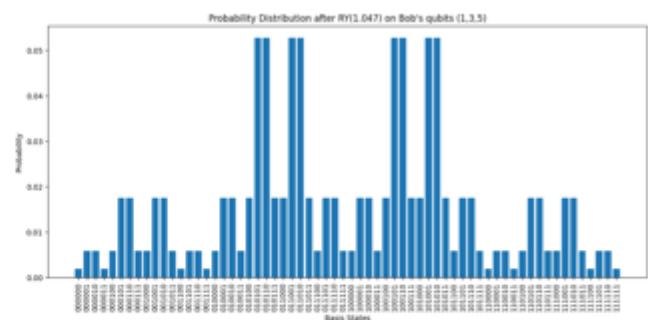
$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle), \quad R_y(\theta) = \begin{pmatrix} \cos \frac{\theta}{2} & -\sin \frac{\theta}{2} \\ \sin \frac{\theta}{2} & \cos \frac{\theta}{2} \end{pmatrix}.$$

let $c = \cos \frac{\theta}{2}$ and $s = \sin \frac{\theta}{2}$. Then

$$R_y(\theta)|0\rangle = c|0\rangle + s|1\rangle, \quad R_y(\theta)|1\rangle = -s|0\rangle + c|1\rangle.$$



(a) Quantum circuit with Eve's Rotation Attack on travel qubits.



(b) Depiction of the basis vector when Eve attacks the rotation angle is $\theta = \pi/3$

Figure 4

on applying $I \otimes R_y(\theta)$ to $|\psi^-\rangle$

$$\begin{aligned}
 (I \otimes R_y)|\psi^-\rangle &= \frac{1}{\sqrt{2}} \left[(I \otimes R_y)|01\rangle - (I \otimes R_y)|10\rangle \right] \\
 &= \frac{1}{\sqrt{2}} \left[|0\rangle \otimes (-s|0\rangle + c|1\rangle) - |1\rangle \otimes (c|0\rangle + s|1\rangle) \right] \\
 &= \frac{1}{\sqrt{2}} \left[-s|00\rangle + c|01\rangle - c|10\rangle - s|11\rangle \right].
 \end{aligned} \tag{20}$$

the overlap with $\langle\psi^-|$ Since $\langle\psi^-| = \frac{1}{\sqrt{2}}(\langle 01| - \langle 10|)$,

$$\begin{aligned}
 \langle\psi^-|(I \otimes R_y)|\psi^-\rangle &= \frac{1}{2} (\langle 01| - \langle 10|)(-s|00\rangle + c|01\rangle - c|10\rangle - s|11\rangle) \\
 &= \frac{1}{2} [0 + c + 0 - 0 - (0 + 0 - c - 0)] \\
 &= \frac{1}{2}(c + c) = c = \cos \frac{\theta}{2}
 \end{aligned} \tag{21}$$

The survival fidelity of the singlet under the attack is

$$F_{\text{singlet}}(\theta) = |\langle\psi^-|(I \otimes R_y(\theta))|\psi^-\rangle|^2 = \cos^2 \frac{\theta}{2},$$

So the single-pair detection probability is the complement:

$$p_{\text{det}}(\theta) = 1 - F_{\text{singlet}}(\theta) = 1 - \cos^2 \frac{\theta}{2}.$$

Hence, for three independent singlets,

$$F_{\text{unitary}}(\theta) = |\langle\Psi_{\text{DFS}}|\Psi_\theta\rangle|^2 = \cos^6 \frac{\theta}{2}, \quad p_{\text{det}}^{(\text{unitary})}(\theta) = 1 - \cos^6 \frac{\theta}{2} \tag{22}$$

4.4 Trojan Horse Attack-

In THA, light pulses are used to get information about the quantum state by analyzing reflected light [4, 22]. Photons are injected into the optical modules of a quantum channel in an attempt to read information directly from the encoding devices by determining about the quantum state. The DFS state does not provide safe-guards against such attacks. To stop Trojan photons, the use of passive optical components like photon number splitters and wavelength filters has been suggested [22].

4.5 Intercept and Resend Attack

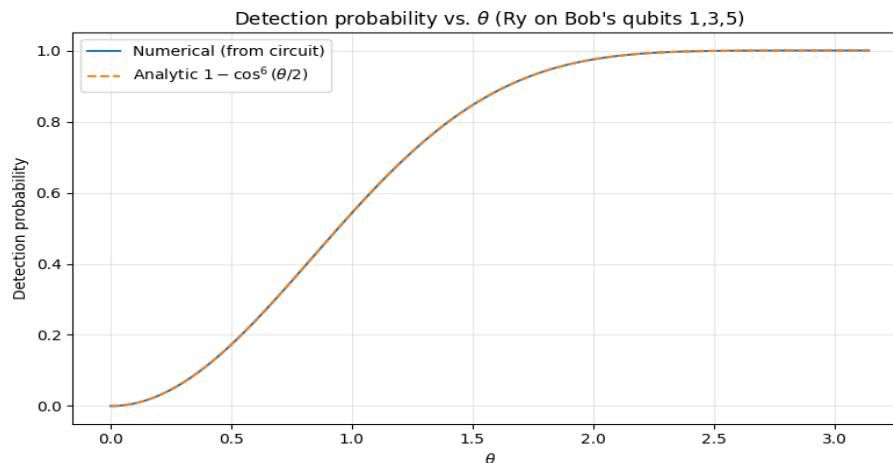


Figure 5: Detection probability vs. unitary rotation angle θ on traveling qubits.

In this case, Eve intercepts the traveling qubit and sends another qubit with or without measuring the intercepted qubit [23]. In the case of measuring it, Eve has 1/4 chance to guess the messaging state qubit, and then with 50 percent probability she can measure it with the right basis, which leads to chances of her knowing the physical qubit is 1/8, that is 7/8 of not knowing. To gain valuable information, she must know all three qubits of the messaging state, which further reduces the chances of knowing the message without being detected. Let us consider when she does not measure to avoid detection. In this case, she intercepts the qubits and reflects them to Alice, and sends her qubits to Bob. Although Eve has not measured, Alice will not be able to detect Eve using the CTRL qubits of the checking sequence, the SHIFT qubit correlation check detects the presence of Eve. The test qubits are checked only after these security checks, and the detection of Eve in these steps will lead to the abandonment of the process and start again.

V.DISCUSSION

The researchers have given several SQSDC protocols [10, 11, 12, 13, 14]. The security and integrity of these protocols rely on Eve's detection and correlation disturbance, providing only a statistical measure, whereas in the proposed scheme, DFS states establish no information leakage along with the detection measure. A comparative analysis of these schemes with the proposed protocol is presented in Table 2. Zou et al [10] used single photons as message carriers. Information is encoded in single-photon degrees of freedom, which requires minimal physical resources. Security measures do not cover collective and coherent attacks. The GHZ states are used in [11] as a qubit resource where correlation disturbance provides for the detection of Eve and has shown robustness against only general attacks. A multiparty SQSDC protocol was proposed by Xu et al. [12]. In this study, cluster state was used to encode the message. This protocol has higher efficiency, but the security was checked only for common individual attacks. Rong et al. [13] came up with a scheme based on Bell states with the structure of a third party as mediator in the SQSDC framework. This has reduced quantum resources by maintaining a quantum mediator with two classical parties, but the efficiency of this protocol is very low. This study also demonstrated robustness against general attacks. Ye et al., in an attempt to address efficiency, proposed a protocol based on single-photon with polarization and spatial mode of degrees of freedom (DOF) [14]. Hyperentanglement of photons in two DOF provides the advantage of higher information capacity per photon, but does not protect against collective and coherent attacks. These protocols use a one-way hash function or XOR for the OTP encryption of messages before being encoded into the quantum state to protect the information against leakage. This study proposes a novel protocol for semi-quantum secure direct communication using a distributed DFS state. We use logical qubits for encoding and decoding the message, and only partial qubits of the DFS states are available in the channel. Eve fails to obtain any information, even if she attacks all the traveling qubits, causing only a higher detection rate. The proposed protocol is demonstrated to be robust against collective attacks, as well as provides security against Eve's attack by detecting it with up to 87.5 per cent probability in a non-unitary attack. Furthermore, it was shown that the rate of detection increases with an increasing angle in a collective attack. The message encoding and decoding are on the logical qubit of the DFS state; thus, logical invariance provides information-theoretic bounds on information leakage. Random selection of checking and message states and the quantum principle of the no-cloning theorem force Eve to be detected in any attempt to learn information. Furthermore, Eve can access three traveling qubits of the DFS state during the operation, making the message encoded in the logical qubit of the DFS state inaccessible.

Qubit / State Type	Security analyses	Efficiency
Single-photon [10]	robust against THA, Intercept and Resend attacks, uses OTP encryption and one-way hash function	18.18
GHZ state[11]	robust against General attacks, XOR for OTP like encryption	16.66
Cluster state[12]	secure against common individual attacks, one-way hash function	33.33
Bell state[13]	robust against general attacks, XOR for OTP like encryption	2.04
Single photon with polarization and spatial mode degree of freedom[14]	robust against general attacks, OTP like encryption and a one-way hash function	9.52
Distributed DFS state proposed here	DFS-based information theoretic secrecy, Robustness against collective attacks, Non-unitary attacks, THA, Intercept and Resend attacks	12.5

Table 2: Comparison of the SQSDC protocol

VI. CONCLUSION

The proposed SQSDC protocol utilizes a distributed six-qubit decoherence-free state (DFS) as a qubit resource, ensuring no information leakage owing to the logical invariance of the DFS state. It is the first protocol to employ a distributed DFS state structure in a semi-quantum setup. This protocol scheme provides an advantage over the existing SQSDC protocols by being robust to collective attacks, non-unitary attacks, and side channel attacks. We have proposed a distinct logical encoding and decoding scheme with a distributed subspace of the DFS state in this protocol. The efficiency $\eta = 2n/(6 - 4n)$ in this scheme is moderate 12.5 as to encode three bits of message information, we have to use four six-qubit DFS states, but this provides for the robustness against collective attack and non-unitary attack.

In this scheme, we have used only collective noise immunity of DFS state, but this work can be extended to other noisy environments by using the inherent quantum Error correction nature of DFS state. The fault tolerance is a dimension to approach the implementable protocols, and logical qubits are a way to create resistance against the environmental noise-induced errors. The overhead cost of using logical qubits is a bottleneck to crack, but with the rapid advancement in quantum technology, it's inevitable to be resolved.

REFERENCES

1. C. H. Bennett, G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Theoretical Computer Science* 560 (2014) 7–11. doi:10.1016/j.tcs.2014.05.025. URL <https://linkinghub.elsevier.com/retrieve/pii/S0304397514004241>
2. P. W. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, *SIAM Journal on Computing* 26 (5) (1997) 1484–1509, eprint: <https://doi.org/10.1137/S0097539795293172>. doi:10.1137/S0097539795293172. URL <https://doi.org/10.1137/S0097539795293172>
3. A. K. Ekert, Quantum cryptography based on Bell's theorem, *Physical Review Letters* 67 (6) (1991) 661–663. doi:10.1103/PhysRevLett.67.661. URL <https://link.aps.org/doi/10.1103/PhysRevLett.67.661>
4. N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Quantum Cryptography, *Reviews of Modern Physics* 74 (1) (2002) 145–195, arXiv:quant-ph/0101098. doi:10.1103/RevModPhys.74.145. URL <http://arxiv.org/abs/quant-ph/0101098>
5. F.-G. Deng, G. L. Long, X.-S. Liu, A Two-Step Quantum Direct Communication Protocol Using Einstein-Podolsky-Rosen Pair Block, *Physical Review A* 68 (4) (2003) 042317, arXiv:quant-ph/0308173. doi:10.1103/PhysRevA.68.042317. URL <http://arxiv.org/abs/quant-ph/0308173>
6. C. Wang, F. G. Deng, G. L. Long, Multi-step quantum secure direct communication using multi-particle Green-Horne-Zeilinger state, *Optics Communications* 253 (1-3) (2005) 15–20, arXiv:quant-ph/0601147. doi:10.1016/j.optcom.2005.04.048. URL <http://arxiv.org/abs/quant-ph/0601147>
7. S. Qin, Q. Wen, L. Meng, F. Zhu, Quantum secure direct communication over the collective amplitude damping channel, *Science in China Series G: Physics, Mechanics and Astronomy* 52 (8) (2009) 1208–1212. doi:10.1007/s11433-009-0140-z. URL <http://link.springer.com/10.1007/s11433-009-0140-z>
8. Z. Cao, D. Song, G. Chai, C. He, G. Zhao, Quantum secure direct communication based on four-particle cluster state grouping, *Chinese Journal of Physics* 60 (2019) 248–254. doi:10.1016/j.cjph.2019.01.019. URL <https://linkinghub.elsevier.com/retrieve/pii/S0577907318310281>
9. M. Boyer, D. Kenigsberg, T. Mor, Quantum Key Distribution with Classical Bob, *Physical Review Letters* 99 (14) (2007) 140501. doi:10.1103/PhysRevLett.99.140501. URL <https://link.aps.org/doi/10.1103/PhysRevLett.99.140501>
10. X. Zou, D. Qiu, Three-step semiquantum secure direct communication protocol, *Science China Physics, Mechanics & Astronomy* 57 (9) (2014) 1696–1702. doi:10.1007/s11433-014-5542-x. URL <http://link.springer.com/10.1007/s11433-014-5542-x>
11. Z. Rong, D. Qiu, X. Zou, Semi-Quantum Secure Direct Communication Using Entanglement, *International Journal of Theoretical Physics* 59 (6) (2020) 1807–1819. doi:10.1007/s10773-020-04447-8. URL <http://link.springer.com/10.1007/s10773-020-04447-8>
12. L.-C. Xu, H.-Y. Chen, N.-R. Zhou, L.-H. Gong, Multi-party semi-quantum secure direct communication protocol with cluster states, *International Journal of Theoretical Physics* 59 (7) (2020) 2175–2186. doi:10.1007/s10773-020-04491-4. URL <https://link.springer.com/10.1007/s10773-020-04491-4>
13. Z. Rong, D. Qiu, P. Mateus, X. Zou, Mediated semi-quantum secure direct communication, *Quantum Information Processing* 20 (2) (2021) 58. doi:10.1007/s11128-020-02965-2. URL <http://link.springer.com/10.1007/s11128-020-02965-2>
14. T.-Y. Ye, M.-J. Geng, T.-J. Xu, Y. Chen, Semiquantum secure direct communication with single photons in both polarization and spatial-mode degrees of freedom.
15. Y. Chang, S.-B. Zhang, L.-L. Yan, G.-H. Han, Robust quantum secure direct communication and authentication protocol against decoherence noise based on six-qubit DF state, *Chinese Physics B* 24 (5) (2015) 050307. doi:10.1088/1674-1056/24/5/050307. URL <https://iopscience.iop.org/article/10.1088/1674-1056/24/5/050307>
16. J. Kempe, D. Bacon, D. A. Lidar, K. B. Whaley, Theory of decoherence-free fault-tolerant universal quantum computation, *Physical Review A* 63 (4) (2001) 042307. doi:10.1103/PhysRevA.63.042307. URL <https://link.aps.org/doi/10.1103/PhysRevA.63.042307>
17. M. Bourennane, M. Eibl, S. Gaertner, C. Kurtsiefer, A. Cabello, H. Weinfurter, Decoherence-Free Quantum Information Processing with Four-Photon Entangled States, *Physical Review Letters* 92 (10) (2004) 107901, arXiv:quant-ph/0309041. doi:10.1103/PhysRevLett.92.107901. URL <http://arxiv.org/abs/quant-ph/0309041>
18. Y.-B. Li, S.-J. Qin, Z. Yuan, W. Huang, Y. Sun, Quantum private comparison against decoherence noise, *Quantum Information Processing* 12 (6) (2013) 2191–2205. doi:10.1007/s11128-012-0517-1. URL <http://link.springer.com/10.1007/s11128-012-0517-1>

19. D. A. Lidar, I. L. Chuang, K. B. Whaley, Decoherence free subspaces for quantum computation, arXiv preprint quant-ph/9807004 (1998).
20. D. A. Lidar, D. Bacon, J. Kempe, K. B. Whaley, Protecting quantum information encoded in decoherence-free states against exchange errors, *Physical Review A* 61 (5) (2000) 052307.
21. M. A. Nielsen, I. L. Chuang, Quantum computation and quantum information, 10th Edition, Cambridge University Press, Cambridge ; New York, 2010.
22. M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. Yuan, A. J. Shields, Practical security bounds against the Trojan-horse attack in quantum key distribution, *Physical Review X* 5 (3) (2015) 031030, arXiv:1506.01989 [quant-ph]. doi:10.1103/PhysRevX.5.031030.
URL <http://arxiv.org/abs/1506.01989>
23. B. Qi, C.-H. F. Fung, H.-K. Lo, X. Ma, Time-shift attack in practical quantum cryptosystems, arXiv:quant-ph/0512080 (May 2006). doi:10.48550/arXiv.quant-ph/0512080.URL <http://arxiv.org/abs/quant-ph/0512080>