AAPPS Bulletin

ORIGINAL ARTICLE

Open Access

Orthogonal-state-based measurement device independent quantum communication: a noise-resilient approach

Chitra Shukla[1,3*], Abhishek Shukla[2*], Symeon Chatzinotas[1] and Milos Nesladek[2]

Abstract

We attempt to propose the first orthogonal-state-based protocols of measurement-device-independent quantum secure direct communication and quantum dialogue employing single basis, i.e., Bell basis as decoy qubits for eavesdropping detection. Orthogonal-state-based protocols are inherently distinct from conventional conjugate-coding protocols, offering unconditional security derived from the duality and monogamy of entanglement. Noise imposes a major challenge to the efficient implementation of these measurement-device-independent based secure direct quantum communication protocols. Notably, these orthogonal-state-based protocols demonstrate improved performance over conjugate-coding-based protocols under certain noisy environments, highlighting the significance of selecting the best basis choice of decoy qubits for secure quantum communication under collective noise. Further, we rigorously analyze the security of the proposed protocols against various eavesdropping strategies, including intercept-and-resend attack, entangle-and-measure attack, information leakage attack, flip attack, and disturbance or modification attack. Our findings also show that, with appropriate modifications, the proposed orthogonal-state-based measurement-device-independent quantum secure direct communication protocol can be transformed into orthogonal-state-based measurement-device-independent versions of quantum key distribution and quantum key negotiation protocols, expanding their applicability. Our protocols leverage fundamentally distinct resources to close the security loopholes linked to measurement devices, while also effectively doubling the distance for secure direct message transmission compared to traditional quantum secure direct communication protocols. Additionally, we calculate the efficiency of our proposed protocols and compare them with standard versions of measurement-device-independent quantum secure direct communication protocols. Ultimately, we discuss system and operational complexity of our proposed protocols in light of experimental elements and the processes.

Keywords Bell measurement, Measurement-device-independent, Quantum secure direct communication, Quantum dialogue, OSB MDI-QSDC, OSB MDI-QD

1 Introduction

Fully Device-Independence (DI) is a well-known approach which does not require the learning of devices working principles [1, 2]. However, it is unfortunate that DI is vulnerable in practice due to imperfect detectors (require unit efficiency) thereby inviting the side channel attacks. Moreover, DI requires the Bell (CHSH) inequality violation to guarantee the security of the protocols. To overcome these limitations, Lo et al. [3] introduced the idea of Measurement-Device-Independence (MDI) which

*Correspondence:
Chitra Shukla
chitra.shukla@uni.lu; chitrashukla07@gmail.com
Abhishek Shukla
abhishek.shukla@uhasselt.be
Full list of author information is available at the end of the article

turned out to be a significant solution to the serious flaws in fully DI, i.e., all the detector side channel attacks can be avoided along with the advantage of it doubles the secure communication distance with conventional lasers as well as it can be implemented with standard optical components with low detection efficiency (unit efficiency is not required) and highly lossy channel. Since then the several MDI-QKD have been proposed in theory and experiment [4]. Further, secure quantum communication comprises of several important branches, each addressing specific aspects of cryptography and secure communication using quantum principles. The most important branches include quantum key distribution (QKD) [5, 6], quantum secret sharing (QSS) [7] and quantum secure direct communication (QSDC) [8–11], and quantum dialogue [12, 13], QSDC being the most promising and advance [14–20] application. QSDC introduced by Long et al. [8, 9] is one of the novel communication techniques to send secret messages directly and securely without the prior generation of quantum keys. Since it alleviates the requirement of generation and encryption processes, it is the best solution to share the secret information directly with low latency. The bottleneck for the implementation of QSDC is the unavailability of quantum memory, which is essential for QSDC protocols. While there are also memory-free QSDC options available [21], recent advancements in quantum memories realizations have optimistically triggered the research community's focus towards QSDC [22, 23], which has further inspired the design and development of DI [24–27] and MDI versions of QSDC following the success of DI-QKD [28] and MDI-QKD [3]. Recent advances in QSDC have brought the field to a significant milestone, marked by the successful demonstration of a practical 100-km QSDC system [29, 30]. These experimental developments clearly show that QSDC is now feasible over distances up to 100 km [30] using current technology. Building on this progress, the design and development of MDI-QSDC is particularly compelling, as it holds the potential to extend the secure communication distance to 200 km and beyond. To the best of our knowledge, in this direction, Long et al. have put forward the first MDI-QSDC protocols [31, 32] using teleportation and entanglement swapping, along with a corresponding security analysis [33]. After that, several MDI-QSDC protocols have been designed and proposed in recent years [23, 34–37], including high-capacity MDI-QSDC protocols [38, 39] using hyper-entanglement, which effectively increases its communication efficiency. The security of all these protocols relies on the BB84 subroutine [5, 40], which implements conjugate coding using two or more mutually unbiased bases (MUBs), such as $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$, where the security arrises from Heisenberg-Uncertainty-Principle (HUP). In this approach, decoy qubits are prepared randomly in non-orthogonal states from either of these bases to detect potential eavesdropping, while the message qubits are encoded and decoded using orthogonal states. In contrast to these traditional protocols, in this work, we aim to explore fundamentally different resources to design orthogonal-state-based (OSB) MDI-QSDC and MDI-QD protocols. In quantum cryptography, the fundamental principle of OSB protocols is the use of orthogonal quantum states (i.e., perfectly distinguishable states) for encoding and transmitting information securely. This contrasts with traditional protocols such as BB84, which rely on non-orthogonal (i.e., indistinguishable) states. The first OSB QKD protocol was proposed by Goldenberg and Vaidman (GV) in 1995 [6] and it was experimentally demonstrated by Avella et al. in 2010 [41]. The GV protocol [6, 41] uses orthogonal states of a single photon, split into two spatiotemporal separated wave packets that arrive at the receiver at different times. The security arises due to duality (for single particle), rather than the use of non-orthogonal states. This represented a paradigm shift from BB84-like protocols and marked the inception of OSB quantum cryptography. Contrary to intuition, orthogonal states can be used to securely transmit secret information, even though Eve can, in principle, distinguish them perfectly. The key lies in designing a protocol where the orthogonal states are transmitted such that Eve does not have access to the basis set in which the communicated states are perfectly measurable. This restriction prevents Eve from performing perfect measurements in correct basis and invokes the no-cloning theorem. Under such constraints, the orthogonal states are effectively transmitted in a non-clonable manner. Specifically, OSB quantum communication protocols utilize a single basis (orthogonal states) for both encoding/decoding and eavesdropping detection, following the GV subroutine [40, 42]. The security framework of OSB protocols stems from the principles of wave-particle-duality [6] (in the single-particle scenario) and the monogamy of entanglement [43] (in the multi-particle scenario), independent of the need for conjugate coding. This establishes that conjugate coding is not a prerequisite for achieving secure quantum communication. As a result, OSB protocols offer significant appeal, particularly from a foundational perspective, by challenging conventional assumptions about the necessity of conjugate coding in quantum communication. This sets the motivation for us to explore OSB-based MDI-QSDC and QD protocols, aiming to advance secure quantum communication beyond standard paradigms, while offering alternative routes to quantum security that are more resilient to real-world or device-imperfect scenarios. Interestingly, a significant body of literature on OSB protocols for secure quantum communication has emerged in recent years [40]. This includes protocols for QKD [6, 41], quantum key agreement (QKA) [44], QSDC and deterministic secure quantum communication (DSQC) [40, 45], as well as quantum dialogue (QD) [13, 46]. Further developments have extended these OSB protocols to semi-quantum settings, including OSB QKA, QSDC/DSQC, and QD [47], which have even led to novel applications such as quantum online shopping [47]. However, to date, no attempts have been made to explore OSB protocols within DI or MDI frameworks. The proposed protocols represent the first efforts to develop OSB MDI-QSDC and OSB MDI-QD protocols.

Apart from the security aspect, a key motivation for proposing the OSB MDI-QSDC and OSB MDI-QD protocols is that the decoy Bell qubits employed form a decoherence-free subspace under collective noise. Given that collective noise is a major source of decoherence in quantum communication experiments, identifying decoherence-free states that can safeguard quantum information from such noise is crucial for reliable implementation. Interestingly, it has been shown that $|\phi^{\pm}\rangle$ are decoherence free as decoy qubits [42, 48] under collective dephasing noise. The study in [42] further demonstrates that when using $|\psi^{\pm}\rangle$ as decoy qubits, the fidelity reaches unity for phase angles $\varphi = n\pi/2$, while it drops to zero for $\varphi = (2n+1)\pi/2$. In contrast, the average fidelity in the BB84 subroutine (uses conjugate coding) does not exhibit this phase-dependent behavior. Similarly, [42] also investigated and revels that $|\psi^{+}\rangle$ and $|\phi^{-}\rangle$ states are decoherence-free subspace under collective rotation noise. As a result, these states serve as optimal decoy qubits for channels experiencing collective rotation, making them the best choice for ensuring security in such environments. In our proposed protocols, Alice and Bob use $|\psi^{+}\rangle_{d_1d_2}$ and $|\psi^{+}\rangle_{d_3d_4}$ states, respectively, as decoy Bell qubits, which are decoherence-free [42]. Since the security of our protocols relies heavily on these decoherence-free decoy Bell qubits, it is critical to protect them from a noisy environment. If collective noise is detected in the communication channel, we can proactively prepare appropriate decoy qubits (that are decoherence-free) for creating the verification string necessary for implementing QSB MDI-QSDC and QSB MDI-QD protocols. In some cases, specific types of noise might even be intentionally introduced to enhance security, leveraging the known behavior of these states in noisy environments.

MDI-QSDC protocols are designed to address security vulnerabilities stemming from imperfections in measurement devices used in quantum communication, such as side-channel attacks that exploit detector flaws. By employing Bell state measurements and entanglement swapping, the protocol shifts the security focus away from the measurement devices, ensuring that an eavesdropper (Eve) cannot exploit them. Additionally, MDI-QSDC enhances communication range by leveraging entanglement swapping, effectively doubling the distance for secure direct message transmission compared to traditional methods, without compromising security.

The paper is organized as follows. In Section 1, we have introduced MDI QSDC with contemporary state-of-research and stated the motivation for OSB MDI-QSDC and MDI-QD protocols. Further in Section 2, we described our OSB MDI-QSDC protocol step by step, which is followed by our OSB MDI-QD protocol in Section 3. Subsequently, we analyzed the security of our protocols in Section 4 against most relevant attacks. Furthermore, in Section 5, we computed the efficiency based on resource consumption for both of our proposed protocols and the pioneering MDI-QSDC protocols [31, 32], and carried out a detailed comparison. Additionally, we also discussed the system complexity of our OSB MDI-QSDC protocol and compared it with MDI-QSDC protocol. Finally, we concluded in Section 6.

2 OSB MDI-QSDC protocol

There are three parties in the OSB MDI-QSDC protocol, say Alice, Bob, and Charlie, where Alice (sender) who wants to send her secret messages to Bob (receiver), and Charlie is an untrusted quantum measurement device performs Bell measurements and could be fully controlled by an adversary, Eve. Alice and Bob use one of the following Bell states:

$$
\begin{aligned}
|\psi^{+}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\\
|\psi^{-}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)\\
|\phi^{+}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)\\
|\phi^{-}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)
\end{aligned}
\tag{1}
$$

The following are the steps involved in the protocol.

Step 1: Preparation: Alice prepares n number of a Bell state, i.e., $|\psi^{+}\rangle_{12}^{\otimes n}$. She prepares the two ordered sequences of all the first qubits as sequence A_M (on which she is supposed to encode her secret message later) and of all the second qubits as sequence A_E (which is to be used for entanglement swapping with Bob's B_E). Further, she prepares n number of decoy Bell states $|\psi^{+}\rangle_{d_1d_2}^{\otimes n}$, where d stands for the verification qubits as decoy Bell pairs. She takes $|\psi^{+}\rangle_{d_1d_2}^{\otimes n/2}$ decoy pairs, keeps all d_1 decoys with herself, and inserts d_2 partner decoys randomly in A_E sequence to obtain an extended A'_E sequence. Similarly, Bob also prepares n number of the Bell states randomly in $|\psi^{+}\rangle_{34}$ or $|\psi^{-}\rangle_{34}$. He prepares the two ordered sequences of all the first qubits as sequence B_M and of all the second qubits as sequence B_E. Subsequently, he prepares n number of decoy Bell states $|\psi^+\rangle_{d_3d_4}^{\otimes n}$, he takes $|\psi^+\rangle_{d_3d_4}^{\otimes n/2}$ decoy pairs, keeps all d_3 decoys with himself, and inserts d_4 partner decoys randomly in B_E sequence to obtain an extended B'_E sequence. Alice and Bob keep their rest of the decoy Bell pairs $|\psi^+\rangle_{d_1d_2}^{\otimes n/2}, |\psi^+\rangle_{d_3d_4}^{\otimes n/2}$ separately for the security of the communication of A_M and B_M sequences to Charlie. It is to be noted that all decoys d_2 and d_4 have been randomly inserted in the communication channel, i.e., each partner particle of a decoy Bell pair has random position in extended sequences A'_E and B'_E and the actual sequence is known to Alice and Bob, respectively.

Here, Alice and Bob can prepare the decoy Bell pairs randomly in any one (or a random series of all) of the Bell states $\{|\psi^{\pm}\rangle_{dd'}, |\phi^{\pm}\rangle_{dd'}\}$ to keep the decoy state secret, which does not allow Charlie to announce any particular fake decoy Bell measurement outcome.

Step 2: Transmission of A'_E and B'_E sequences: Alice and Bob keep the sequence A_M and B_M and their respective decoys d_1 and d_3 with themselves and send the extended A'_E and B'_E sequences to Charlie to allow him to perform the Bell measurement as shown in Fig 1. Without having any knowledge to distinguish between entangled (E) or decoy (d_2, d_4) partner particles in the received sequences A'_E and B'_E from Alice and Bob, respectively, Charlie performs the joint Bell measurement on both the sequences A'_E and B'_E and announces the Bell measurement outcome (BMO) which leads to 4 cases as shown below in Table 1.

As can be followed in Fig. 1, Charlie's Bell measurement on the sequences A'_E and B'_E leads to entanglement swapping, and Alice's and Bob's corresponding home sequences A_M, B_M, along with their decoys d_1, d_3; E, d_3; d_1, E become pairwise entangled between Alice and Bob.

Step 3: Eavesdropping check: After Charlie's BMO announcement, Alice and Bob announce the positions of decoys d_2 and d_4 in their A'_E and B'_E sequences, respectively. They also announce their initially prepared decoy Bell pair state. For case I, both Alice and Bob measure their home decoy qubits d_1 and d_3 in computational basis $\{|0\rangle, |1\rangle\}$ and check the correlation according to the Bell measurement outcome of Charlie's announcement. This is because Alice's and Bob's home decoy qubits d_1 and d_3 are Bell entangled

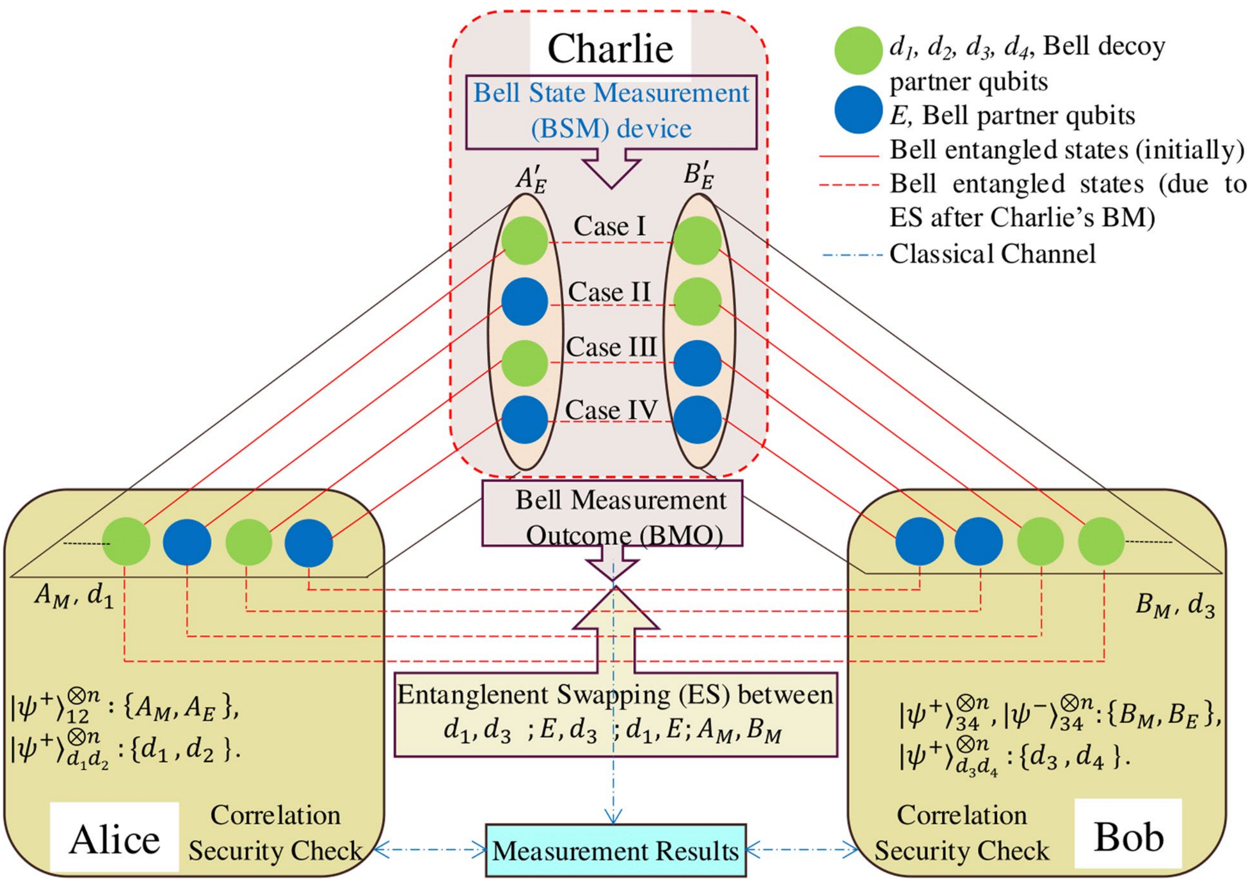

Fig. 1 (Color online) A schematic illustrating the establishment of secure entanglement channel between Alice and Bob via Charlie's Bell measurement assistance in our OSB MDI-QSDC protocol

Table 1 4 cases of Bell measurement performed by Charlie and their corresponding actions in the protocol

4 cases	A'_E	B'_E	Actions
Case I	d_2	d_4	Correlation security check from Eve/Charlie's fake BMO announcement
Case II	E	d_4	Correlation security check from Eve/Charlie's fake BMO announcement
Case III	d_2	E	Correlation security check from Eve/Charlie's fake BMO announcement
Case IV	E	E	Entanglement swapping (ES) for message transmission

E indicates the entangled partner qubit from an entangled pair in A'_E and B'_E sequences. d_2 and d_4 are partners of Bell decoys in A'_E and B'_E, respectively

(due to entanglement swapping) after Charlie performs Bell measurement on decoys d_2 and d_4 received from Alice and Bob, let us consider if Charlie's announces $|\psi^+\rangle_{d_2d_4}$ as his BMO then Alice and Bob home decoys will be $|\psi^+\rangle_{d_1d_3}$ so if Alice's measurement (in computational basis) outcome on d_1 is $|0\rangle(|1\rangle)$ then Bob's outcome on d_3 will be correlated and should be $|0\rangle(|1\rangle)$. Further for case II, Alice measures her corresponding entangled qubit and Bob measures his home decoy qubits d_3 in $\{|0\rangle, |1\rangle\}$ and check for correlation according to the BMO of Charlie's announcement. Similarly, for case III, Alice measures her home decoy qubits d_1 and Bob measures his corresponding entangled qubit in $\{|0\rangle, |1\rangle\}$ and check for correlation according to the BMO of Charlie's announcement (here Bob also has to announce his initial Bell state $|\psi^+\rangle_{34}$ or $|\psi^-\rangle_{34}$ to help Alice for correlation check). These three cases ensure the security against an eavesdropper "Eve" and any fake transmission or announcements (without actually making) Bell measurement by Charlie, because any eavesdropping/mischievous will disturb the correlation check that Alice and Bob can easily identify. For example, if Eve performs an intercept-and-resend attack, she would be exposed when Alice and Bob calculate the error rate on correlation check and if they find this error rate below the threshold value then they continue to the next step, otherwise they discard the protocol and starts afresh.

It is reasonable to think that case I is enough to ensure the security against Eve/Charlie, then cases II and III can also be used for message encoding just as case IV and that would make the OSB MDI-QSDC more efficient. In such a case, Alice just need to announce the initial Bell decoy state in case III she prepared initially, although in case II, initial Bell state $|\psi^+\rangle_{12}$ is already known.

Step 4: Entanglement swapping: Now for case VI, due to Charlie's Bell measurement on each pair of A_E and B_E sequences (i.e., the qubits 2, 4) leads to quantum entanglement swapping, resulting the corresponding A_M and B_M sequences become pair-wise entangled as Bell states (i.e., the qubits 1, 3) as shown below in Eq. 2.

It is to be noted that Bell-state analysis is crucial in entanglement-based QSDC, as it allows the sender and receiver to distinguish between different Bell states to extract secure information. However, in standard linear optics, fully complete Bell-state analysis is not achievable with linear optics alone, i.e., Bell state discrimination is limited to only two Bell states. This problem has been addressed via advanced techniques such as hyperentanglement [49, 50], kerr nonlinearity [51], or ancillary photons [52] enable full discrimination. For example, non-destructive discrimination of all four Bell states has been successfully demonstrated with the aid of ancillary qubits, which can be reused in subsequent measurement iterations [53, 54]. These methods are essential for entanglement-based QSDC to ensure secure and reliable quantum communication.

Step 5: Message encoding by Alice: After the eavesdropping check is confirmed that there is no eavesdropping or no fake announcements from Charlie, Alice (Bob) discarded all the corresponding partner entangled (E) qubits from $A_M(B_M)$ which contributed to cases II (III) and will start message coding process (on case IV) as shown in Fig. 2. Alice holds A_M sequence initially prepared in $|\psi^+\rangle_{12}$ state whereas Bob holds B_M sequence randomly prepared in $|\psi^+\rangle_{34}$ and $|\psi^-\rangle_{34}$ states initially. Both the ordered sequences A_M and B_M are now Bell entangled (i.e., (A_M, B_M) pairwise entangled) due to the entanglement swapping in the last step. Therefore, (A_M, B_M) states are only known to Bob based on his initial preparation of $|\psi^+\rangle_{34}$ or $|\psi^-\rangle_{34}$. Now, Alice applies the unitary (Pauli) operations $U_0 = I$, $U_1 = X$, $U_2 = iY$, and $U_3 = Z$ on the qubits of A_M sequence to encode her 2-bits of classical information 00, 01, 10, and 11, respectively. After encoding her secret messages on A_M sequence, Alice finds an encoded sequence A'_M, in which she inserts rest of the decoy Bell pairs $|\psi^+\rangle_{d_1d_2}^{\otimes n/2}$ randomly (to follow the GV subroutine [40] for security check in next step) and sends

$$
\begin{aligned}
|\psi^+\rangle_{12} \otimes |\psi^+\rangle_{34} &= \frac{1}{2}\left(|\psi^+\rangle_{13}|\psi^+\rangle_{24} + |\phi^+\rangle_{13}|\phi^+\rangle_{24} + |\phi^-\rangle_{13}|\phi^-\rangle_{24} + |\psi^-\rangle_{13}|\psi^-\rangle_{24}\right),\\
|\psi^+\rangle_{12} \otimes |\psi^-\rangle_{34} &= \frac{1}{2}\left(|\psi^+\rangle_{13}|\psi^-\rangle_{24} - |\phi^+\rangle_{13}|\phi^-\rangle_{24} - |\phi^-\rangle_{13}|\phi^+\rangle_{24} + |\psi^-\rangle_{13}|\psi^+\rangle_{24}\right).
\end{aligned} \tag{2}
$$

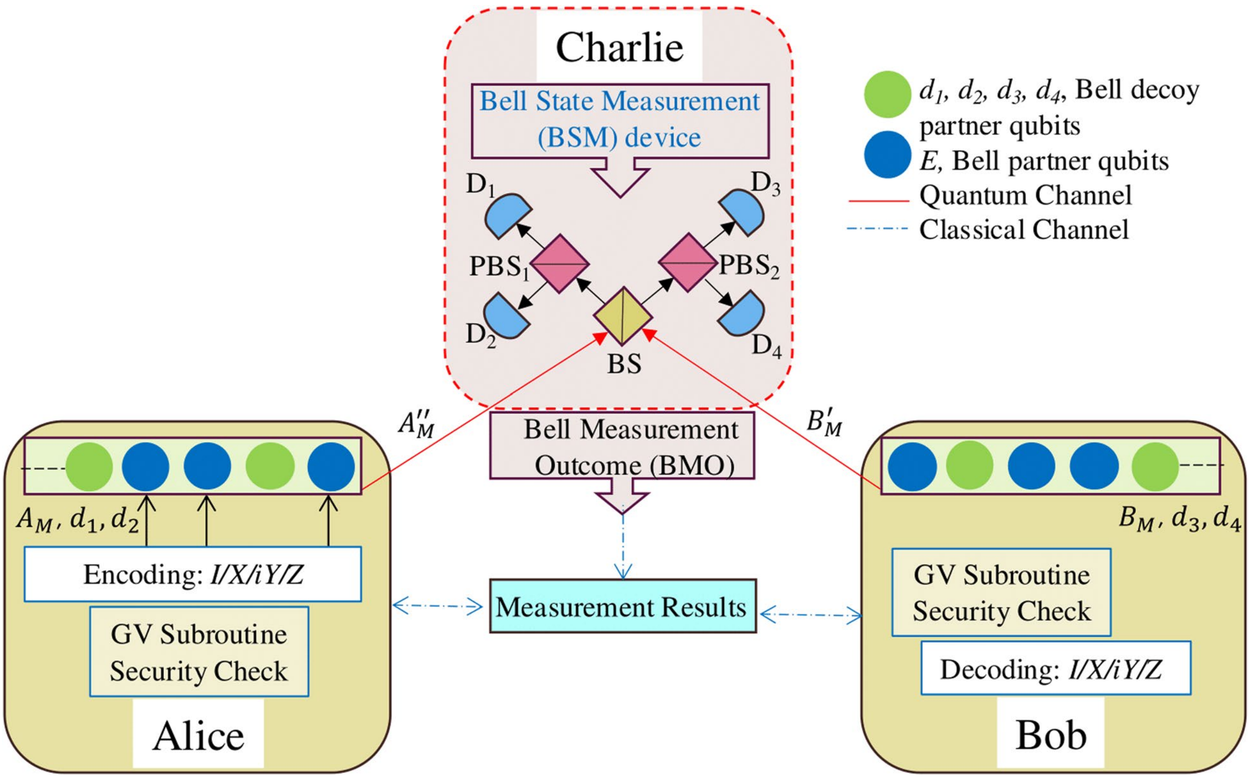

Fig. 2 (Color online) Basic set-up of Alice and Bob illustrating their cryptographic process (encoding, decoding, and eavesdropping checking by GV subroutine [40, 42]) along with experimental design of Charlie's Bell measurement device crucial in our OSB MDI-QSDC protocol. BS: beam splitter; PBS_1, PBS_2: polarizing beam splitter; D_1, D_2, D_3, and D_4 detectors

an extended message encoded sequence A''_M to Charlie. At the same time, Bob randomly applies I or X from the set of cover operations $\{I, X\}$ on the qubits of B_M. The cover operations help against information leakage as mentioned in Refs. [33, 35]. He also inserts rest of the decoy Bell pairs $|\psi^+\rangle_{d_3d_4}^{\otimes n/2}$ randomly (to follow the GV subroutine [40] for security check in next step) in B_M sequence and sends an extended sequence B'_M to Charlie.

Alice can choose to leave (does not encode) some random qubits of A_M sequence as it is for the correlation check in the next step. This will ensure the security of the message against Charlie. Alternatively, Alice can divide the decoy Bell qubits into two parts to check the security by GV subroutine using one part and by a correlation check using another part. This strategy would be helpful to trace any bit flip attack as discussed in Section 4.5.

Step 6: Eavesdropping check: After receiving the authenticated acknowledgement of the receipt of all the qubits of A''_M and B'_M sequences by Charlie, Alice and Bob announce the positions of their decoy Bell pairs in their sequences A''_M and B'_M, respectively. Charlie then measures the decoy Bell pairs in each sequence A''_M and B'_M separately and announces the corresponding BMO. In the absence of an eavesdropping, Charlie should get each decoy Bell pair in the same state ($|\psi^+\rangle_{dd'}$) as his Bell measurement outcome as was initially prepared by Alice and Bob, respectively. In between if Eve tries to eavesdrop and measures the qubits in any of the sequences A''_M and B'_M, being unknown of decoys and message qubits, the decoys Bell pairs will get entanglement swapped with wrong partner particles and any other Bell measurement outcome ($|\psi^-\rangle_{dd'}, |\phi^+\rangle_{dd'}$ or $|\phi^-\rangle_{dd'}$) is the signature of eavesdropping, leading to the detection probability 75%. Alice and Bob compare the decoy Bell measurement outcomes with that of their initial decoy Bell pair preparation and calculate the error rate, they also check the correlation security check on unencoded qubits by Alice, if the error rate is below the threshold value then they continue to the next step, otherwise they discard the protocol and starts afresh.

Step 7: Decoding of message by Bob: After being confirmed there is no eavesdropping, Charlie obtains A'_M and B_M sequences and performs the Bell measurement on A'_M and B_M sequences and announces his Bell measurement outcomes, using which Bob can decode the secret message encoded by Alice. This is so because, only Bob knows which initial Bell state (qubits 1, 3 of column

Table 2 Alice prepares her initial Bell state $|\psi^+\rangle_{12}$ and Bob randomly prepares $|\psi^+\rangle_{34}$ or $|\psi^-\rangle_{34}$

Alice and Bob initial product Bell states (1, 2) and (3, 4)	Charlie's Bell measurement result on qubits 2, 4 (A_E,B_E)	Alice and Bob initially shared Bell state after entanglement swapping (only known to Bob) (A_M, B_M)	Bob's cover operations {*I*, *X*} on B_M	Charlie's Bell measurement result on message encoded qubits 1, 3 (A'_M, B_M)	Bob's decoding of Alice's encoded unitary operation $U_j \epsilon \{I, X, iY, Z\}$ where $j \epsilon \{0, 1, 2, 3\}$
$|\psi^+\rangle_{12} \otimes |\psi^+\rangle_{34}$	$|\psi^+\rangle_{24}$	$|\psi^+\rangle_{13}$	*I*	$|\psi^+\rangle_{13}/|\phi^+\rangle_{13}/|\phi^-\rangle_{13}/|\psi^-\rangle_{13}$	*I/X/iY/Z*
			X	$|\phi^+\rangle_{13}/|\psi^+\rangle_{13}/|\psi^-\rangle_{13}/|\phi^-\rangle_{13}$	*X/I/Z/iY*
	$|\phi^+\rangle_{24}$	$|\phi^+\rangle_{13}$	*I*	$|\phi^+\rangle_{13}/|\psi^+\rangle_{13}/|\psi^-\rangle_{13}/|\phi^-\rangle_{13}$	*I/X/iY/Z*
			X	$|\psi^+\rangle_{13}/|\phi^+\rangle_{13}/|\phi^-\rangle_{13}/|\psi^-\rangle_{13}$	*X/I/Z/iY*
	$|\phi^-\rangle_{24}$	$|\phi^-\rangle_{13}$	*I*	$|\phi^-\rangle_{13}/|\psi^-\rangle_{13}/|\psi^+\rangle_{13}/|\phi^+\rangle_{13}$	*I/X/iY/Z*
			X	$|\psi^-\rangle_{13}/|\phi^-\rangle_{13}/|\phi^+\rangle_{13}/|\psi^+\rangle_{13}$	*X/I/Z/iY*
	$|\psi^-\rangle_{24}$	$|\psi^-\rangle_{13}$	*I*	$|\psi^-\rangle_{13}/|\phi^-\rangle_{13}/|\phi^+\rangle_{13}/|\psi^+\rangle_{13}$	*I/X/iY/Z*
			X	$|\phi^-\rangle_{13}/|\psi^-\rangle_{13}/|\psi^+\rangle_{13}/|\phi^+\rangle_{13}$	*X/I/Z/iY*
$|\psi^+\rangle_{12} \otimes |\psi^-\rangle_{34}$	$|\psi^-\rangle_{24}$	$|\psi^+\rangle_{13}$	*I*	$|\psi^+\rangle_{13}/|\phi^+\rangle_{13}/|\phi^-\rangle_{13}/|\psi^-\rangle_{13}$	*I/X/iY/Z*
			X	$|\phi^+\rangle_{13}/|\psi^+\rangle_{13}/|\psi^-\rangle_{13}/|\phi^-\rangle_{13}$	*X/I/Z/iY*
	$|\phi^-\rangle_{24}$	$|\phi^+\rangle_{13}$	*I*	$|\phi^+\rangle_{13}/|\psi^+\rangle_{13}/|\psi^-\rangle_{13}/|\phi^-\rangle_{13}$	*I/X/iY/Z*
			X	$|\psi^+\rangle_{13}/|\phi^+\rangle_{13}/|\phi^-\rangle_{13}/|\psi^-\rangle_{13}$	*X/I/Z/iY*
	$|\phi^+\rangle_{24}$	$|\phi^-\rangle_{13}$	*I*	$|\phi^-\rangle_{13}/|\psi^-\rangle_{13}/|\psi^+\rangle_{13}/|\phi^+\rangle_{13}$	*I/X/iY/Z*
			X	$|\psi^-\rangle_{13}/|\phi^-\rangle_{13}/|\phi^+\rangle_{13}/|\psi^+\rangle_{13}$	*X/I/Z/iY*
	$|\psi^+\rangle_{24}$	$|\psi^-\rangle_{13}$	*I*	$|\psi^-\rangle_{13}/|\phi^-\rangle_{13}/|\phi^+\rangle_{13}/|\psi^+\rangle_{13}$	*I/X/iY/Z*
			X	$|\phi^-\rangle_{13}/|\psi^-\rangle_{13}/|\psi^+\rangle_{13}/|\phi^+\rangle_{13}$	*X/I/Z/iY*

Accordingly, column *I* shows the two possible product states of Alice and Bob, column *II* corresponds to the possible BMO on qubits (2, 4) by Charlie, and as a result column *III* shows the Bell state qubits (1, 3) after entanglement swapping (only known to Bob). Column *IV* shows the cover operation applied by Bob. Columns *V* and *VI* show the relationship between Charlie's BMO on Alice's message encoded qubits and Bob's decoding of unitary operation applied by Alice

III of Table 2) has been shared between Alice and Bob after entanglement swapping being performed by Charlie in step 4, which is in accordance to Bob's initial Bell state preparation of $|\psi^+\rangle_{34}$ or $|\psi^-\rangle_{34}$ (column *I* of Table 2).

This is how Alice sends her secret message to Bob via the help of an untrusted measurement device Charlie, without any information leakage.

Beyond the primary function of securely transmitting messages, which is the fundamental purpose of any QSDC protocol, our OSB MDI-QSDC scheme can, like other MDI-QSDC protocols [31, 32], be adapted to perform additional cryptographic tasks. Specifically, it can be reduced to a key negotiation protocol when Alice encodes randomly generated numbers into quantum states and follows our OSB MDI-QSDC procedure. In this mode, instead of conveying meaningful information, the protocol establishes a shared random key between Alice and Bob. Moreover, our OSB MDI-QSDC protocol can also be reduced to a true key distribution scheme by enabling the transmission of a pre-determined key. In this case, Alice selects a specific key in advance, encodes it into quantum states, and transmits it to Bob via Charlie using our OSB MDI-QSDC procedure. This allows for the secure distribution of a fixed, pre-determined key, distinguishing it from conventional key negotiation. In summary, our OSB MDI-QSDC protocol effectively supports all three functions: secure direct message transmission, quantum key negotiation, and predetermined key distribution. However, converting the reverse—OSB MDI-QKD back into OSB MDI-QSDC—is not possible.

Further, our OSB MDI-QSDC protocol is a unidirectional communication in which the information flows in one direction of communication (i.e., from Alice to Bob). It may be interesting to visualize it in bidirectional communication such that the information flows in both the direction of communication (i.e., from Alice to Bob and Bob to Alice) simultaneously using the same quantum channel as happens in the original QD [12].

Before we introduce an OSB MDI-QD protocol, it is to be noticed that the authors introduced an MDI quantum direct dialogue in section 2.3 of [31], where Alice encodes her secret message on her own travel qubits sequence M_A^1 (for Alice to Bob communication) but Bob does not encode his secret on the corresponding M_B^1. Similarly, Bob encodes his secret message on his own travel qubits sequence M_B^2 (for Bob to Alice communication) but Alice does not encode her secret on the corresponding M_A^2. The nonavailability of simultaneous encodings of both Alice and Bob on the corresponding Bell pairs (i.e., on M_A^1, M_B^1 and M_A^2, M_B^2) while Charlie performs the Bell measurement seems to be different than the original framework of QD protocols [12]. Thus, their MDI quantum direct dialogue rather can be more appropriately described equivalent to the two QSDCs, first QSDC from Alice to Bob using M_A^1, M_B^1 and second QSDC form Bob to Alice using M_A^2, M_B^2. Because, when Charlie measures M_A^1, M_B^1 (M_A^2, M_B^2), it only contains the encoding of Alice (Bob) but not of Bob (Alice). So when Charlie measures M_A^1, M_B^1 (M_A^2, M_B^2), both the encodings from Alice and Bob are not available simultaneously on the same quantum channel, which may not fully align with the requirements of the original QD framework [12].

In principle, in a original QD protocols [12], which refers to the situation, where Alice and Bob send their secret messages to each other simultaneously on the same quantum channel in which they both encode their secret messages on the same travel qubit entangled with another kept as home qubit with Bob. However, we consider a protocol as QD, when the two different travel qubits which became entangled (due to entanglement swapping) being encoded by Alice and Bob, respectively. We emphasize that we can consider such protocols as QD (within original framework of QD [12]) even if the two different travel qubits entangled with each other and each travel qubit carries the encoding information. The logic behind is that when the two qubits are entangled then they behave in the same manner regardless of $U_B U_A$ being encoded only on the second qubit of $|\psi^+\rangle_{12} = \frac{|00\rangle_{12}+|11\rangle_{12}}{\sqrt{2}}$ respectively, or U_A and U_B are separately encoded on first and second qubit respectively of $|\psi^+\rangle_{12} = \frac{|00\rangle_{12}+|11\rangle_{12}}{\sqrt{2}}$. Following the latter trick, we introduce an OSB MDI-QD protocol in Section 3. The only criteria to be within QD is that the combined Bell state should be measured by Charlie only after Alice and Bob apply the operations U_A and U_B respectively on their travel qubits. Hence, both the encodings U_A and U_B are available simultaneously on the same quantum channel. It is to be noted that in a two-party QD protocol [12], it is preferred to apply $U_B U_A$ only on the second travel qubit because there are only two parties and one party Bob starts the protocol and receives the travel qubit back himself encoded by Alice. But here in OSB MDI-QD, there are three parties where two authorized parties Alice and Bob separately sending their encoded travel qubits (which become entangled after entanglement swapping in step 4) in step 5 to an unauthorized party Charlie for Bell measurement. Here, the encoded sequences have been measured by Charlie only after Alice and Bob send their sequences A_M and B_M to Charlie after encoding their secret messages. With this motivation, now we introduce our OSB MDI-QD protocol in the next section.

3 OSB MDI-QD protocol

QD protocol is a two-way communication scheme that allows both parties, Alice and Bob, to simultaneously exchange the secret messages on the same quantum channel utilizing a Bell pair [12, 13]. The key advantage of QD is its ability to achieve secure bidirectional communication in a single session. The proposed OSB MDI-QD protocol steps could be outlined as follows:

Step 1: Preparation: Alice prepares n number of the Bell states, i.e., $|\psi^+\rangle_{12}^{\otimes n}$. She prepares the two ordered sequences of all the first qubits as sequence A_M (on which she is supposed to encode her secret message later) and of all the second qubits as sequence A_E (which is to be used for entanglement swapping with Bob's B_E). Further, she prepares n number of decoy Bell states $|\psi^+\rangle_{d_1 d_2}^{\otimes n}$, where d stands for the verification qubits as decoy Bell pairs. She takes $|\psi^+\rangle_{d_1 d_2}^{\otimes n/2}$ decoy pairs, keeps all d_1 decoys with herself, and inserts d_2 partner decoys randomly in A_E sequence to obtain an extended A'_E sequence. Similarly, Bob also prepares n number of the Bell states randomly in $|\psi^+\rangle_{34}$ or $|\psi^-\rangle_{34}$. Further, he performs OSB MDI-QSDC protocol as shown in Section 2 to securely share the exact information of the prepared Bell state. However, Alice does not have to do so because her initial Bell state is fixed as $|\psi^+\rangle_{12}$ and is a public knowledge. Now, he prepares the two ordered sequences of all the first qubits as sequence B_M and of all the second qubits as sequence B_E. Subsequently, he prepares n number of decoy Bell states $|\psi^+\rangle_{d_3 d_4}^{\otimes n}$, he takes $|\psi^+\rangle_{d_3 d_4}^{\otimes n/2}$ decoy pairs, keeps all d_3 decoys with himself, and inserts d_4 partner decoys randomly in B_E sequence to obtain an extended B'_E sequence. Alice and Bob keep their rest of the decoy Bell pairs $|\psi^+\rangle_{d_1 d_2}^{\otimes n/2}$, $|\psi^+\rangle_{d_3 d_4}^{\otimes n/2}$ separately for the security of the communication of A_M and B_M sequences to Charlie. It is to be noted that all decoys d_2 and d_4 have been randomly inserted in the communication channel, i.e., each partner particle of a decoy Bell pair has random position in extended sequences A'_E and B'_E and the actual sequence is known to Alice and Bob, respectively.

Similar to step 1 of OSB MDI-QSDC, Alice and Bob can randomly prepare the decoy Bell pairs in any of the Bell states $\{|\psi^\pm\rangle_{dd'}, |\phi^\pm\rangle_{dd'}\}$, keeping the decoy state secret and preventing Charlie from announcing a fake Bell measurement outcome.

Step 2: Transmission of A'_E and B'_E sequences: Alice and Bob keep the sequence A_M and B_M with themselves and send the extended A'_E and B'_E sequences to Charlie to allow him to perform the Bell measurement that leads to 4 cases as shown in Table 1.

Step 3: Eavesdropping check: Same as step 3 of OSB MDI-QSDC described in Section 2.

Step 4: Entanglement swapping: Same as step 4 of OSB MDI-QSDC described in Section 2.

Step 5: Message encoding by Alice and Bob: Once it is confirmed that there is no eavesdropping or no fake announcements from Charlie, Alice (Bob) discards all the corresponding partner entangled (E) qubits from $A_M(B_M)$ which contributed to cases II (III) (they do not discard if they decide to use these cases for message coding). After that Alice and Bob start message coding process (on case IV) where Alice holds A_M sequence initially prepared in $|\psi^+\rangle_{12}$ state whereas Bob holds B_M sequence randomly prepared in $|\psi^+\rangle_{34}$ or $|\psi^-\rangle_{34}$ state initially. Both the ordered sequences A_M and B_M are now Bell entangled (i.e., (A_M, B_M) pairwise entangled) due to the entanglement swapping in the last step. Hence, after the Bell measurement announcement of (A_E, B_E) from Charlie as shown in column *II* of Table 2, Alice and Bob both know the initial Bell state A_M, B_M they share as shown in *III* column of Table 2 according to Eq. 2. Unlike OSB MDI-QSDC, here Alice also know initial Bell state A_M, B_M because Bob has already executed OSB MDI-QSDC in step 1 to securely share the exact information of the prepared Bell state ($|\psi^+\rangle_{34}$ or $|\psi^-\rangle_{34}$). Now, Alice applies one of the unitary operations $U_0 = I$, $U_1 = X$, $U_2 = iY$, and $U_3 = Z$ on the qubits of A_M sequence to encode her 2-bits of classical information 00, 01, 10, and 11, respectively. After encoding her secret messages on A_M sequence, Alice finds an encoded sequence A'_M, in which she inserts rest of the decoy Bell pairs $|\psi^+\rangle_{d_1d_2}^{\otimes n/2}$ randomly and sends an extended message encoded sequence A''_M to Charlie. At the same time, Bob also randomly applies one of the unitary operations $U_0 = I$, $U_1 = X$, $U_2 = iY$, and $U_3 = Z$ on the qubits of B_M sequence according to his secret message to encode his 2-bits of classical information and gets his encoded sequence B'_M, then he also inserts rest of the decoy Bell pairs $|\psi^+\rangle_{d_3d_4}^{\otimes n/2}$ randomly in B'_M sequence and sends an extended sequence B''_M to Charlie. It should be noted that here, Alice or Bob do not require applying the cover operations $\{I, X\}$ [33, 35].

Step 6: Eavesdropping check: This step is the same as step 6 of OSB MDI-QSDC described in Section 2, with the only difference being that in this case, the sequences A''_M and B''_M, obtained from the previous step, will now be checked.

Step 7: Decoding of message by Alice and Bob: After being confirmed there is no eavesdropping, Charlie performs the Bell measurement on A'_M, B'_M message encoded sequences and announces his final Bell measurement outcomes, using which Alice and Bob can decode the secret messages encoded by Bob and Alice, respectively. This is so because Alice (Bob) knows Bob's (Alice's) initial Bell state prepared in step 1 for which Bob executed OSB MDI-QSDC as shown in Section 2 to securely share the information about which Bell state ($|\psi^+\rangle_{34}$ or $|\psi^-\rangle_{34}$) that he has prepared initially. However, Alice's initial Bell state ($|\psi^+\rangle_{12}$) is the public knowledge so Bob knows it. Hence, after Bell measurement is performed on qubits 2, 4, resulting in entanglement swapping on qubits 1, 3 and 2, 4 in Eq. 2, Alice and Bob also know the initial Bell state (qubits 1, 3) shared between them in step 4, on which they have encoded their secret messages. Further, they know Charlie's final Bell measurement result announcement and their own encoding unitary operation. Therefore, they can successfully decode each others secret information and complete the quantum dialogue protocol between them via the help of an untrusted measurement device, Charlie.

Now, we would like to note that there is a special reason why we have selected that Alice prepares $|\psi^+\rangle_{12}$ and Bob prepares randomly in $|\psi^+\rangle_{34}$ or $|\psi^-\rangle_{34}$ as initial Bell state in step 1. Specifically, in Section 4.4, we will show how the number of initial Bell state selection will allow Alice and Bob to reduce the information leakage by 1-bit of classical information in comparison to the standard quantum dialogue protocol [12], where the information leaks by 2-bits on the Bell measurement announcement. Further, we will also show that if Alice also chooses to prepare any two Bell states randomly in $|\psi^+\rangle_{12}$ or $|\psi^-\rangle_{12}$ like Bob chooses to prepare randomly in $|\psi^+\rangle_{34}$ or $|\psi^-\rangle_{34}$ as initial Bell state in step 1, then the leakage problem can be completely solved, but in such a case, Alice also have to securely share with Bob the exact information of the initial Bell state $|\psi^+\rangle_{12}$ or $|\psi^-\rangle_{12}$ prepared in step 1, as was done by Bob, executing the OSB QSDC protocol as shown in Section 2.

Interestingly, in this way, Alice and Bob can ensure that the ignorance of Eve should be equal to the total classical information (4-bits secret messages, i.e., 2-bits by Alice and 2-bits by Bob) transmitted between them simultaneously on the same quantum channel. Basically, as Eve's ignorance increases, the c-bits information leakage decreases. Therefore, the random preparation of initial Bell states by Alice and Bob in step 1 provides a tradeoff to avoid the conventional information leakage problem in QD protocols. We have shown the details in Section 4.4. However, it is useless for Alice and or Bob to prepare more than any two Bell states randomly, for example, suppose they prepare $|\psi^+\rangle_{12}$ or $|\psi^-\rangle_{12}$ and $|\psi^+\rangle_{34}, |\psi^-\rangle_{34}$ or $|\phi^+\rangle_{34}$ respectively because in this case, Eve's ignorance would exceed the maximum requirements of 4-bits in our OSB MDI-QD protocol, so we restrict ourselves to the above two cases, however, such a case might be useful where the Eve's ignorance requirements are higher than 4-bits.

In the original two-party QD protocols [12], initial and final Bell states are public knowledge, and Alice and Bob know their own encoding so they can deduce each other's encoding information. However, there exists a partial information leakage problem of 2-bits due to the final Bell measurement announcement, i.e., Eve can extract 2-bits information about the product of unitary operations $U_B U_A$ applied by Alice (U_A) and Bob (U_B), respectively. Hence, information leakage is an inherent problem in QD protocols. To avoid such a leakage, we used the tricks mentioned and utilized in [46], such that in the first step of our OSB MDI-QD protocol, Bob can use OSB QSDC protocol for sharing information about his initial Bell state (which he randomly prepared in $|\psi^+\rangle_{34}$ or $|\psi^-\rangle_{34}$). This strategy of random preparation of Bell states by Bob would help to increase the ignorance of Eve, thereby reducing the information leakage.

4 Security analysis

In this section, we have analyzed the security of the two proposed protocols under the following possible eavesdropping attacks.

4.1 Security of OSB MDI-QSDC protocol

Since Charlie is an untrusted third party responsible for measurement, he effectively plays the role of Eve in the security analysis. To decode the secret message of Alice, Charlie or Eve must have to know the initial Bell state shared between Alice and Bob (on which Alice is supposed to encode her secret messages) which is obtained by them after the entanglement swapping. Basically, if the initial Bell states prepared by both Alice and Bob are known to Charlie/Eve, then after the entanglement swapping performed by Charlie, he/she can get the knowledge of new born Bell states (qubits 1, 3) and can decode the secret message at the end. However, Eve's attempt to try knowing that new born initial Bell state (1, 3) fails because Bob has prepared his initial Bell state randomly in one of the two $|\psi^+\rangle_{34}$ or $|\psi^-\rangle_{34}$ Bell states (unknown to Charlie/Eve). As soon as Charlie has performed the Bell measurement on qubits (2, 4), which results into entanglement swapping on qubits (1, 3) as shown in Eq. 2. After that Charlie/Eve can never verify the exact initial Bell state shared between Alice and Bob and they end up with the two possible product state equally probable due to the random preparation of the initial Bell state by Bob as shown in Eq. 2. Further, any attempts of eavesdropping by Charlie/Eve will disturb the maximal entanglement correlation between Alice and Bob, and will be traced out by Alice and Bob, where the security would arise from monogamy of entanglement [43]. All kinds of fake particle attacks or entangle-and-measure attack will be detected during the correlation security and eavesdropping checks performed in steps 3 and 6 in Section 2.

4.2 Intercept-and-resend attack

If Eve applies an intercept-and-resend attack to our OSB MDI-QSDC, she prepares her own Bell state, intercepts Bob's qubit from the extended B'_E sequence during its transmission to Charlie (in step 2), and sends one qubit of her fake Bell state to Charlie. Eve aims for her fake Bell state to undergo entanglement swapping (in step 4) with Alice's qubit sequence A_M, on which Alice will later apply her secret encoding operation (in step 5). Since Alice's initial Bell state $|\psi^+\rangle_{12}$ is publicly known, Eve plans to deduce Alice's secret information once Charlie announces his Bell measurement results in step 7. However, this attack can be detected as early as step 3 under case I, when Alice and Bob perform correlation checks based on Charlie's Bell measurement outcomes. Any attempted intercept-resend attack by Eve will break the correlation, which ensures security against both Eve and Charlie. After entanglement swapping in step 4, the initial Bell state shared between Alice and Bob is unknown to Eve, hence it is meaningless for Eve to apply this attack in step 5, as she cannot decode the message without the knowledge of initial Bell state being shared. The same eavesdropping detection strategy works for our OSB MDI-QD protocol.

4.3 Entangle-and-measure attack

In the entangle-and-measure attack, Eve prepares one or more ancilla qubits, either in a pure state like $|0\rangle$ or a superposition state $|p\rangle = \alpha|0\rangle_e + \beta|1\rangle_e$. She then entangles this ancilla qubit with the travel qubit being transmitted from Alice (or Bob separately) to Charlie via a unitary operation, typically a controlled-*NOT* (*CNOT*) gate. The goal of this attack is to allow Eve to extract information about Alice's qubits (or Bob's qubits) by measuring her entangled ancilla qubit at a later stage, without directly interfering with the main communication process. In step 1 of the proposed protocols, as Alice (and Bob separately) prepares a decoy Bell state $|\psi^+\rangle_{dd'} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{ht}$, $(d\epsilon 1, 3;\, d'\epsilon 2, 4)$ keeping the home qubit (h) and sending the travel qubit (t) in her extended A'_E sequence (Bob's B'_E sequence) to the Charlie. Eve, with her ancilla qubit, say $|p\rangle = \alpha|0\rangle_e + \beta|1\rangle_e$, applies a CNOT gate, with target on the t qubit and control on her ancilla qubit $|p\rangle$. After this operation, the resulting composite state becomes:

$$\begin{aligned} CNOT_{e\to t} &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{ht} \otimes (\alpha|0\rangle_e + \beta|1\rangle_e), \\ &= \frac{1}{\sqrt{2}}[\alpha|00\rangle_{ht}|0\rangle_e + \alpha|11\rangle_{ht}|0\rangle_e + \beta|01\rangle_{ht}|1\rangle_e + \beta|10\rangle_{ht}|1\rangle_e], \\ &= \frac{1}{\sqrt{2}}[\alpha|0\rangle_e(|00\rangle + |11\rangle)_{ht} + \beta|1\rangle_e(|01\rangle + |10\rangle)_{ht}], \end{aligned} \tag{3}$$

Eve now measures her entangled ancillary qubit in the standard basis $\{|0\rangle, |1\rangle\}$. There are two possible outcomes.

Case 1: If her measurement outcome is $|0\rangle_e$ with probability $|\alpha|^2$ then the remaining state collapses to $|\psi^+\rangle_{dd'} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{ht}$, i.e., original decoy Bell state initially prepared by Alice (Bob) which means no disturbance, so Alice or Bob cannot detect Eve in step 3. Case 2: However, if Eve gets the measurement outcome $|1\rangle_e$ with probability $|\beta|^2$ then the remaining state collapses to $|\phi^+\rangle_{dd'} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{ht}$, i.e., orthogonal to the original decoy Bell state. This is an error from Alice's (Bob's) perspective, and it will show up as a disturbance when Bell state measurements and correlation security checks will be performed. Eve's strategy will be failed and detected by Alice and Bob in the correlation security check in step 3.

Let us suppose Eve applies entangle-and-measure attack on Bob's decoy Bell state $|\psi^+\rangle_{d_3d_4} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{ht}$ in $B_E^{'}$ sequence traveling to Charlie and with her measurement outcome $|1\rangle_e$ in case 2, the remaining decoy Bell state collapses to $|\phi^+\rangle_{d_3d_4}$ as shown above, which would then be entanglement swapped by Charlie (step 2) with Alice's decoy Bell state $|\psi^+\rangle_{d_1d_2}$ in $A_E^{'}$ sequence (received by Charlie from Alice). This will be a product of two decoy Bell states (in analogy with Eq. 2), which can be expressed after entanglement swapping as

$$|\psi^+\rangle_{d_1d_2} \otimes |\phi^+\rangle_{d_3d_4} = \frac{1}{2}\big(|\psi^+\rangle_{d_1d_3}|\phi^+\rangle_{d_2d_4} + |\psi^-\rangle_{d_1d_3}|\phi^-\rangle_{d_2d_4} + |\phi^+\rangle_{d_1d_3}|\psi^+\rangle_{d_2d_4} + |\phi^-\rangle_{d_1d_3}|\psi^-\rangle_{d_2d_4}\big). \quad (4)$$

However, in an ideal scenario when there is no eavesdropping (in absence of Eve) the above product of two decoy Bell states should have been

$$|\psi^+\rangle_{d_1d_2} \otimes |\psi^+\rangle_{d_3d_4} = \frac{1}{2}\big(|\psi^+\rangle_{d_1d_3}|\psi^+\rangle_{d_2d_4} + |\phi^+\rangle_{d_1d_3}|\phi^+\rangle_{d_2d_4} + |\phi^-\rangle_{d_1d_3}|\phi^-\rangle_{d_2d_4} + |\psi^-\rangle_{d_1d_3}|\psi^-\rangle_{d_2d_4}\big). \quad (5)$$

In Eq. 4, Chalie performs Bell measurement on decoy travel qubits d_2, d_4 from Alice and Bob, respectively. Let us suppose he gets his Bell measurement outcome $|\phi^+\rangle_{d_2d_4}$ in Eq. 4 and he announces it then the correlated decoy Bell state with home qubits d_1, d_3 will be $|\psi^+\rangle_{d_1d_3}$ which is different than expected, i.e., $|\phi^+\rangle_{d_1d_3}$ ideally (without Eve) shown in Eq. 5. Further, the corresponding home qubits d_1, d_3 in the correlated decoy Bell state $|\psi^+\rangle_{d_1d_3}$ at Alice and Bob's end will fail upon correlation security check performed by Alice and Bob, respectively. Hence, Eve can never pass or escape the correlations security check without being detected in step 3. The same eavesdropping detection strategy works for our OSB MDI-QD protocol.

4.4 Security of OSB MDI-QD protocol against information leakage

Information leakage is an inherent aspect of QD protocols [13], quantifiable as the discrepancy between the total information transmitted by legitimate users and the minimum amount of information Eve requires to infer that data (i.e., Eve's ignorance). This limitation similarly applies to the proposed OSB MDI-QD protocol, where Eve may gain some information about Alice's and Bob's encoding once Charlie announces the Bell measurement results. We calculate the average information Eve may gain [46] which can be expressed as,

$$I(AB:E) = H_{apriori} - H_{aposteriori}, \quad (6)$$

where $H_{apriori}$ represents the total classical information exchanged between Alice and Bob, which is 4 bits in our OSB MDI-QD. Now, we calculate the Eve's ignorance, i.e., $H_{aposteriori}$ after Charlie announces his Bell measurement outcome on qubits 1, 3 in step 7. Let us say Charlie's Bell measurement outcome in step 4 is $|\psi^+\rangle_{24}$ and in step 7 also is $|\psi^+\rangle_{13}$. This arrises two cases for Charlie/Eve considering the two random choices of initial Bell states $|\psi^+\rangle_{34}$ or $|\psi^-\rangle_{34}$ prepared by Bob given Alice always prepares $|\psi^+\rangle_{12}$:

Case (i) When Alice and Bob have chosen to prepare $|\psi^+\rangle_{12} \otimes |\psi^+\rangle_{34}$ as initial Bell states as shown in I row and I column of Table 2. After the entanglement swapping on qubits 2, 4 in step 4 and encodings by Alice and Bob on qubits 1, 3 in step 5 the state can be expressed as

$$\begin{aligned} &|\psi^+\rangle_{12} \otimes |\psi^+\rangle_{34} = \frac{1}{2}\big(|\psi^+\rangle_{13}|\psi^+\rangle_{24} + |\phi^+\rangle_{13}|\phi^+\rangle_{24} + |\phi^-\rangle_{13}|\phi^-\rangle_{24} + |\psi^-\rangle_{13}|\psi^-\rangle_{24}\big), \\ &P(II, |\psi^+\rangle_{13}||\psi^+\rangle_{13}) = P(XX, |\psi^+\rangle_{13}||\psi^+\rangle_{13}) = P(iYiY, |\psi^+\rangle_{13}||\psi^+\rangle_{13}) = P(ZZ, |\psi^+\rangle_{13}||\psi^+\rangle_{13}) \end{aligned} \quad (7)$$

Case (ii) When Alice and Bob have chosen to prepare $|\psi^+\rangle_{12} \otimes |\psi^-\rangle_{34}$ as initial Bell states as shown in II row and I column of Table 2. After the entanglement swapping on qubits 2, 4 in step 4 and encodings by Alice and Bob on qubits 1, 3 in step 5 the state can be expressed as

$$|\psi^+\rangle_{12} \otimes |\psi^-\rangle_{34} = \frac{1}{2}\left(|\psi^+\rangle_{13}|\psi^-\rangle_{24} - |\phi^+\rangle_{13}|\phi^-\rangle_{24} - |\phi^-\rangle_{13}|\phi^+\rangle_{24} + |\psi^-\rangle_{13}|\psi^+\rangle_{24}\right),$$
$$P(IZ, |\psi^-\rangle_{13}||\psi^+\rangle_{13}) = P(ZI, |\psi^-\rangle_{13}||\psi^+\rangle_{13}) = P(XiY, |\psi^-\rangle_{13}||\psi^+\rangle_{13}) = P(iYX, |\psi^-\rangle_{13}||\psi^+\rangle_{13}) \quad (8)$$

In both the cases above, Charlie/Eve never know that which case was chosen by Alice and Bob. Consequently, Charlie as never been sure about his Bell measurement outcome on qubits 2, 4 in step 4 is coming from case (i) or case (ii). So, he is also not certain which initial Bell states of qubits 1, 3 were being shared between Alice and Bob before encoding. Hence, all the above 8 possibilities (encoding by Alice and Bob) as shown together in Eqs. 7 and 8 are equally probable for Charlie/Eve with an unknown initial Bell state of qubits 1, 3 of case (i) and case (ii). Now, we can calculate $H_{aposteriori} = -8(\frac{1}{8})log_2(\frac{1}{8}) = 3$ bits. Further, $I(AB:E) = 4 - 3 = 1$ bit. This is an advantage that we have reduced Eve's ignorance by 1 bit in comparison with the leakage (2 bits) in the standard QD protocol [12].

We can also consider case (iii) $|\psi^+\rangle_{12} \otimes |\phi^+\rangle_{34}$ and case (iv) $|\psi^+\rangle_{12} \otimes |\phi^-\rangle_{34}$ to maximize Eve's ignorance by 4 bits and can obtain Eve's gain $I(AB:E) = 0$, which means that Eve cannot obtain any information through the public announcements of BMO by Charlie because the total classical information exchanged between Alice and Bob is equal to the Eve's ignorance.

4.5 Flip attack

Flip attack is a kind of disturbance attack where Eve applies X operation on all the travel qubits in order to misguide authorized parties while she cannot learn any meaningful information. As we know that GV subroutine [40] fails (e.g., $X \otimes X|\psi^+\rangle_{dd'} = |\psi^+\rangle_{dd'}$) when Eve tries to apply the flip attack on all the traveling qubits. To avoid such attack in general, Alice can prepare the n number of decoy Bell pairs say in $|\psi^+\rangle_{dd'}$, but she concatenates $n-m$ Bell pairs $|\psi^+\rangle_{dd'}$, and only partner particles of the m ($m < n$) Bell pair $|\psi^+\rangle_{dd'}$ in the message sequence. Specifically, $n-m$ Bell pairs will take care of the GV subroutine to check eavesdropping and partner particles of m Bell pairs will be used for correlation check between Alice and Bob to check flip attack. Specifically, Alice keeps the first qubits of the m Bell pairs as home qubit and sends the corresponding second qubits to Charlie along with the message sequence in step 5 of OSB MDI-QSDC and OSB MDI-QD in Section 2 and in Section 3, respectively. After Charlie announces the receipt of all the qubits, Alice will announce the positions of the partner particles of the m Bell pairs, then Charlie measures in $\{0, 1\}$ basis and announces the results for correlation check for Alice where Alice also measure the corresponding home qubits in $\{0, 1\}$ basis and check for the perfect correlations (if Charlie gets 0 (1) then Alice should also get 0 (1)). If Eve really attacks all the qubits by flip attack in the extended sequence, then the correlation must be mismatched (i.e., if Charlie gets 0 (1) then Alice should get 1 (0). Similarly, Bob will also check for the perfect correlation with Charlie. Therefore, if Eve is applying flip attack on all of the travel qubits of (both) the sequence(s) coming from Alice (and Bob) to Charlie then she would be traced by Alice (and Bob) in correlation check of Bell states as mentioned above. If the errors are below the certain threshold value then Alice and Bob are safe enough to correctly decode each-others encoding in step 7 of OSB MDI-QD, because Eve cannot differentiate between message and decoy qubits so she will flip all the travel qubits (messages and decoys), and applies flip operation $X \otimes X$ on A'_M, B'_M which will never change the actual encodings of Alice and Bob as $X \otimes X = I$, hence no disturbance in the secret information. Similarly, Bob correctly decodes Alice's encoding in step 7 of OSB MDI-QSDC, as if Eve applies flip operation $X \otimes X$ on A'_M, B_M does not change the actual encoding of Alice. Now, if Eve is applying flip attack on few of the qubits in any of the sequences coming from Alice or Bob to Charlie then she would be traced by them with the usual GV subroutine. So, Eve has no way to escape without being detected.

4.6 Disturbance attack [55] or modification attack [56]

This attack is a specific type of denial-of-service (DoS) attack, where Eve aims to mislead Alice and Bob by altering the message content—such as changing the qubit order or applying unitary transformations to some qubits—during the transmission of the sequence A''_M from Alice to Charlie in step 5 of the OSB MDI-QSDC protocol, and the transmission of sequences A''_M and B''_M from Alice and Bob, respectively, to Charlie in step 5 of the OSB MDI-QD protocol. Importantly, Eve's goal in this attack is not to extract any meaningful information [55], but merely to disrupt communication. However, any such manipulation will be detectable. Since Eve cannot selectively alter only the message qubits without affecting the decoy Bell pairs $|\psi^+\rangle_{dd'}$, her interference will introduce detectable errors. These errors can be identified in step 6 of both protocols, ensuring the integrity of the communication.

5 Efficiency analysis

A widely used metric for evaluating the efficiency of secure quantum communication protocols is qubit efficiency [57], defined as

$$\eta = \frac{c}{q+b}, \tag{9}$$

where c represents the total number of transmitted classical bits (i.e., message bits), q denotes the total number of qubits used, and b is the number of classical bits exchanged to decode the message. It is important to note that classical communication used solely for eavesdropping checks is not included in b. This efficiency measure was first introduced by Cabello [57] in 2000 and has since become a standard tool for comparing various protocols for secure direct communication. For our proposed OSB MDI-QSDC protocol, Alice transmits $2n$ bits of classical information to Bob, thus $c = 2n$. To accomplish this, Alice uses n qubits from the A_M sequence and an equal number (i.e., n) of decoy qubits. Similarly, Bob uses n qubits from the B_M sequence and n decoy qubits, all of which are sent to Charlie. Therefore, the total number of qubits used is $q = 2n + 2n$. In addition, Charlie announces the outcomes of his Bell state measurements, which amount to $2n$ bits of classical information needed by Bob to decode Alice's message. Hence, $b = 2n$. Therefore, the qubit efficiency of our OSB MDI-QSDC protocol is $\eta = \frac{2n}{2n+2n+2n} = \frac{1}{3} = 33.33\%$. In a standard QSDC protocol, the efficiency $\eta = 50\%$ [10] without requiring the parameter b. However, due to the MDI nature of our OSB MDI-QSDC protocol, where b is essential for message decoding, the efficiency is reduced to 33.33%. Notably, this reduction is offset by a practical advantage, i.e., our OSB MDI-QSDC protocol effectively doubles the communication distance between Alice and Bob compared to a conventional QSDC protocol.

For our proposed OSB MDI-QD protocol, Alice and Bob each transmit $2n$ bits of classical information to each other, thus $c = 2n + 2n = 4n$. To accomplish this, Alice uses n qubits from the A_M sequence and an equal number (i.e., n) of decoy qubits. Similarly, Bob uses n qubits from the B_M sequence and n decoy qubits, all of which are sent to Charlie. In addition, Bob uses a Bell state to perform OSB MDI-QSDC to convey the information regarding the initial state to Alice. ($|\psi^+\rangle_{34}$ or $|\psi^-\rangle_{34}$) through an OSB MDI-QSDC scheme, which requires 4 extra qubits (two qubits for the channel and two qubits for eavesdropping checking) and 2 bits for Charlie's Bell measurement announcements. Therefore, the total number of qubits used is $q = 2n + 2n + 4$, similar to [46]. Now, Charlie announces the outcomes of his Bell state measurements, which amount to $2n$ bits of classical information needed by Alice and Bob to decode each other's messages in the main part of OSB MDI-QD and we also add 2 bits of classical announcement by Charlie for OSB MDI-QSDC. Hence, $b = 2n + 2$. Thus, in the $n \to \infty$ limit the efficiency would become the same as that in the QD scheme without QSDC [46]. This is so because in this particular case, $\eta = lim_{n\to\infty} \frac{4n}{(2n+2n+4)+2n+2} = lim_{n\to\infty} \frac{4n}{6n(1+\frac{1}{n})} = \frac{2}{3} = 66.67\%$. Therefore, the qubit efficiency of our OSB MDI-QD protocol is $\eta = 66.67\%$. Thus, our OSB MDI-QD protocol can double the communication distance without incurring any additional overhead, while maintaining the same efficiency bound as a standard QD protocol [13, 46].

Now, to compare our efficiency values, we compute the efficiencies of the pioneering MDI-QSDC protocols [31, 32]. In Ref. [31], Alice transmits $2n$ bits of classical information to Bob, thus $c = 2n$. Alice uses n qubits from the S_A sequence and Bob also uses n qubits from the S_B sequence, they both send to Charlie. Therefore, the total number of qubits used is $q = 2n$. Now, Charlie announces the outcomes of his Bell state measurements, which amount to $2n$ bits of classical information needed by Bob to decode Alice's message. Further, to ensure the integrity of the message, Alice also encodes some random check numbers on some of the photons (say, δn) in M_A at random positions. Alice announces the positions (δn) and values (δn) of the random check numbers, and Bob compares them with Alice to check the integrity of messages. Hence, total $b = 2n + 2\delta n$. Therefore, the qubit efficiency of Ref. [31] MDI-QSDC protocol is, $\eta = \frac{2n}{2n+2n+2\delta n} = \frac{2n}{4n+2\delta n}$. Since the choice of δn is subjective, so we focus only on the limiting case. A small value of δn may compromise the integrity check, whereas the most robust integrity verification is achieved when $\delta n = n$, i.e., when the number of check qubits equals the number of message qubits, which in this case is n. Therefore, in the limiting case $lim_{\delta n\to n} \frac{2n}{4n+2\delta n} = \frac{2n}{4n+2n} = \frac{1}{3} = 33.33\%$. In Ref. [32], Alice transmits n bits of classical information to Bob, so $c = n$. Now, Alice uses $n + t_0$ qubits from the S_{Ah} sequence and Bob also uses $n + t_0$ qubits to send Charlie, so $q = 2n + 2t_0$. Further, Charlie announces $2(n + t_0)$ bits to disclose his Bell measurement outcome (related to teleportation), as well as announces n bits of his σ_Z basis measurements (in step 5). In addition, Bob announces $n + t_0$ bits for his basis preparation (in step 4). Alice announces $2t_0$ bits corresponding to the positions and values of the random check numbers for integrity of messages (in step 6). Hence, the total $b = 2(n + t_0) + n + (n + t_0) + 2t_0 = 4n + 5t_0$. Therefore, $\eta = \frac{n}{2n+2t_0+4n+5t_0} = \frac{n}{6n+7t_0}$. However, in the limiting case, $lim_{t_0\to n} \frac{n}{n(6+\frac{7t_0}{n})} = \frac{n}{6+7} = \frac{1}{13} = 7.69\%$. For the purpose of a fair comparison, it would be apt to consider $c = 2n$, which will eventually correspond to dense coding. In this limiting case for Ref. [32], $\eta = \frac{2}{13} = 15.38\%$. This reduced efficiency is due to the fact that protocol in Ref. [32] uses classical communication for the announcements of outcomes during teleportation and other involved subroutines for message decoding as mentioned above. It is evident from the above calculation that the efficiency of our OSB MDI-QSDC protocol is same, i.e., 33.33% as that for the conventional MDI-QSDC protocol in Ref. [31]. However, the efficiency of our protocol outperforms the efficiency of another conventional MDI-QSDC protocol in Ref. [32], the efficiency of the latter one comes out to be 15.38%. Here, we compare the efficiency of our OSB MDI-QSDC protocol only with the two most relevant and pioneering MDI-QSDC protocols, but with the description provided above, it would be straightforward to compare the efficiency of our protocol with any other relevant MDI-QSDC protocol.

In the following, we briefly describe experimental elements responsible for system complexity in light of the requirement of OSB MDI-QSDC protocol and compare it with that of MDI-QSDC protocols. We also point out this comparison from view of operational complexity. We briefly visit relavant portion of the protocol to mark the difference. The difference between our OSB MDI-QSDC protocol and MDI-QSDC is that in the former case, the decoy states is prepared in the Bell basis, and in the latter case, the decoy states are prepared in the single-qubit states, requiring account of complexity analysis, while in both protocols, message qubits were prepared in the Bell basis. The preparation of Bell decoy states can be done using the same hardware resources that are used for the preparation of Bell states used for message encoding. As the Bell state preparation, maintenance, and measurement are the essential parts of both protocols and so the requirement of all experimental elements, i.e., Entangled Photon Source, BBO Crystal, Phase Stabilization, Interferometers, Coincidence Detection, Polarization, Controllers, Delay Lines, Synchronization Clock for Bell state preparation and Single Photon Source, Polarizer or Waveplates, Fiber Coupler, Detector for single qubit state preparation. Irrespective of whether Bell states are used only for message qubit states or for both message qubit states and for the decoy qubit states, the system complexity due to hardware resources remains the same in both protocols. However, the preparation of extra Bell states used as decoys in OSB MDI-QSDC protocol essentially increases the operational complexity in the form of energy and time resources.

6 Conclusion

MDI-QSDC protocols are designed to eliminate security vulnerabilities tied to imperfections in the measurement devices used in quantum communication protocols. These vulnerabilities, such as side-channel attacks, are common in traditional setups, where the eavesdropper can exploit weaknesses in detectors or measurement systems. Technically, MDI-QSDC achieves this by utilizing Bell state measurements and entanglement swapping. Our innovative protocols utilize the unique resources to effectively eliminate security vulnerabilities associated with Charlie's measurement devices. Additionally, they significantly enhance the range of secure direct message transmission, achieving double the distance for secure direct message transmission compared to conventional quantum communication methods. We proposed two OSB protocols of MDI-QSDC and MDI-QD protocols that are fundamentally distinct from conventional conjugate-coding methods, offering unconditional security derived from the monogamy of entanglement [40, 43]. Further, we conducted security analysis of our protocols, evaluating their robustness against key quantum attacks like intercept-and-resend, entangle-and-measure, flip, and disturbance or denial-of-service attacks. We also demonstrated the resilience of the proposed OSB MDI-QD protocol, particularly in mitigating information leakage and ensuring the integrity of quantum communication channels. This intrinsic security feature arises because the correlations shared by legitimate parties exclude any potential eavesdropper, making OSB protocols highly robust against various quantum attacks [43]. Specifically, the proposed OSB MDI-QSDC and OSB MDI-QD protocols contribute to the growing body of work in MDI-QSDC by exploring alternative quantum mechanical resources beyond HUP for ensuring unconditional security. These protocols establish that HUP is not the only mechanism capable of providing unconditional security in quantum communication, opening the door for further research into different foundational principles. The main advantages of our proposed protocols are as follows: Firstly, OSB protocols represent a distinct class in quantum cryptography where orthogonal quantum states are used securely by exploiting deep quantum properties beyond uncertainty, offering alternative routes to quantum security that can be more resilient in realistic or device-imperfect scenarios. Secondly, conventional MDI QSDC protocols use single-qubit decoys randomly prepared in $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ bases, which underperform in comparison to the Bell decoys states in the collective noisy environment [42]. In such a practical noisy environment, the conventional MDI QSDC protocols face double challenges dealing with two separate noisy communication channels, i.e., Alice-Charlie and Bob-Charlie. However, in this noisy environment, our OSB MDI QSDC protocol uses Bell decoy states, leveraging their advantage of the decoherence-free subspace, and outperforms the single-qubit decoys used in conventional MDI protocols. This would apparently reduce the effective noise (or noise impact) on the two noisy communication channels compared with conventional MDI QSDC protocols while doubling the communication distance. Thirdly, decoy Bell states retain a significant advantage over single-qubit decoys in noisy environments. Their inherent quantum correlations allow for entanglement-based verification techniques—such as Bell inequality tests, parity checks and fidelity checks—that can differentiate natural decoherence from eavesdropping-induced disturbances. Moreover, certain Bell states may form decoherence-free subspaces under symmetric noise models, further enhancing robustness. In contrast, single-qubit decoys lack such structure, making them more vulnerable to indistinguishable effects of noise and attack. Fourthly, other than noise resiliency, another major advantage of OSB MDI-QSDC protocol is the higher detection probability of eavesdropping, i.e., 75%, compared to 50% in the standard MDI-QSDC protocol, as reported in [31, 32]. The 75% detection probability in our protocol is due to the fact that we use a single Bell state as a decoy state, and any variation in the measurement outcomes of Charlie from this expected state leads to an error. As there are three possibilities for causing error corresponding to the remaining three Bell states out of four, an error detection probability of 75% can be realized.

Subsequently, we calculate the efficiency of our OSB MDI-QSDC and QD protocols and compare them with standard versions of MDI-QSDC protocols. Further, we discuss system and operational complexity of our OSB MDI-QSDC protocol in light of experimental elements and the processes. Another significant motivation is that the OSB secure quantum communication protocols outperform under certain noisy environment in comparison to the conjugate-coding-based secure quantum communication protocols [42]. It remains the future prospects of our research direction that is to investigate the scope of decoherence free subspace for the variety of noises including non-Markovian noise aligning with the recent work [27]. Moreover, it would be of wider interest to investigate and compare the effect of various noisy channels on our OSB MDI-QSDC and OSB MDI-QD protocol and MDI-QSDC and MDI-QD protocols given [31, 32], which is under the scope of upcoming work.

Acknowledgements
We gratefully acknowledge Dr. Kishore Thapliyal for his valuable feedback. We also extend our heartfelt thanks to Prof. Radhakrishna Srikanth for his early encouragement, which inspired C.S. to undertake and continue this research. CS also acknowledges QuISTechAI for the support provided during her employment with QuISTechAI from Feb.-April 2025.

Auhthors' contributions
C.S. conceptualized the idea. C.S. and A.S. are leading authors contributed in developing the methodology, writing and polishing the manuscript. All the authors read and reviewed the final manuscript.

Funding
C.S. and S.C. gratefully acknowledge support in part by the project Lux4QCI under Grant GA 101091508 funded by the Digital Europe Program and in part by the project LUQCIA funded by the Government of Luxembourg/SMC. A.S. and M.N. acknowledge the support from project BeQCI (cofounded by EU and Belspo) and SBO BeQuNet project (funded by the FWO).

Data availability
Not applicable.

Declarations

Competing interests
The authors declare that they have no competing interests.

Author details
[1]Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, Luxembourg 1855, Luxembourg. [2]IMO-IMOMEC, Hasselt University, Wetenschapspark 1, B-3590 Diepenbeek, Belgium. [3]QuISTechAI Private Limited, Rajni Khand, Sharda Nagar, 226002, Uttar Pradesh, Lucknow, India.

Received: 21 April 2025 Accepted: 10 July 2025
Published online: 30 July 2025

References

1. U. Vazirani, T. Vidick, Fully device independent quantum key distribution. Phys. Rev. Lett. **113**, 140501 (2014)
2. A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, V. Scarani, Device-independent security of quantum cryptography against collective attacks. Phys. Rev. Lett. **98**(23), 230501 (2007)
3. H.K. Lo, M. Curty, B. Qi, Measurement-device-independent quantum key distribution. Phys. Rev. Lett. **108**(13), 130503 (2012)
4. Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, H.K. Lo, Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. Phys. Rev. Lett. **112**(19), 190503 (2014)
5. C.H. Bennet, in *Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore, India, Dec. 10-12, 1984* (IEEE, Bangalore, 1984)
6. L. Goldenberg, L. Vaidman, Quantum cryptography based on orthogonal states. Phys. Rev. Lett. **75**, 1239–1243 (1995)
7. M. Hillery, V. Bužek, A. Berthiaume, Quantum secret sharing. Phys. Rev. A **59**(3), 1829 (1999)
8. G.L. Long, X.S. Liu, Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A **65**(3), 032302 (2002)
9. F.G. Deng, G.L. Long, Controlled order rearrangement encryption for quantum key distribution. Phys. Rev. A **68**(4), 042315 (2003)
10. C. Shukla, A. Pathak, R. Srikanth, Beyond the Goldenberg-Vaidman protocol: secure and efficient quantum communication using arbitrary, orthogonal, multi-particle quantum states. Int. J. Quantum Inf. **10**(08), 1241009 (2012)
11. A. Banerjee, K. Thapliyal, C. Shukla, A. Pathak, Quantum conference. Quantum Inf. Process. **17**, 1–22 (2018)
12. B.A. Nguyen, Quantum dialogue. Phys. Lett. A **328**(1), 6–10 (2004)
13. C. Shukla, V. Kothari, A. Banerjee, A. Pathak, On the group-theoretic structure of a class of quantum dialogue protocols. Phys. Lett. A **377**(7), 518–527 (2013)
14. H. Zhang, Z. Sun, R. Qi, L. Yin, G.L. Long, J. Lu, Realization of quantum secure direct communication over 100 km fiber with time-bin and phase quantum states. Light Sci. Appl. **11**(1), 83 (2022)
15. G.L. Long, D. Pan, Y.B. Sheng, Q. Xue, J. Lu, L. Hanzo, An evolutionary pathway for the quantum internet relying on secure classical repeaters. IEEE Netw. **36**(3), 82–88 (2022)
16. D. Pan, Z. Lin, J. Wu, H. Zhang, Z. Sun, D. Ruan et al., Experimental free-space quantum secure direct communication and its security analysis. Photon. Res. **8**(9), 1522–1531 (2020)
17. Y.B. Sheng, L. Zhou, G.L. Long, One-step quantum secure direct communication. Sci. Bull. **67**(4), 367–374 (2022)
18. C.W. Ding, W.Y. Wang, W.D. Zhang, L. Zhou, Y.B. Sheng, Quantum secure direct communication based on quantum error correction code. Appl. Phys. Lett. **126**(2), (2025) 024002

19. J.W. Ying, P. Zhao, W. Zhong, M.M. Du, X.Y. Li, S.T. Shen et al., Passive decoy-state quantum secure direct communication with a heralded single-photon source. Phys. Rev. Appl. **22**(2), 024040 (2024)
20. M. Wang, G.L. Long, Lattice-based access authentication scheme for quantum communication networks. Sci. China Inf. Sci. **67**(12), 222501 (2024)
21. Z. Sun, L. Song, Q. Huang, L. Yin, G. Long, J. Lu, L. Hanzo, Toward practical quantum secure direct communication: a quantum-memory-free protocol and code design. IEEE Trans. Commun. **68**(9), 5778–5792 (2020)
22. W. Zhang, D.S. Ding, Y.B. Sheng, L. Zhou, B.S. Shi, G.C. Guo, Quantum secure direct communication with quantum memory. Phys. Rev. Lett. **118**(22), 220501 (2017)
23. X.J. Li, D. Pan, G.L. Long, L. Hanzo, Single-photon-memory measurement-device-independent quantum secure direct communication—part I: its fundamentals and evolution. IEEE Commun. Lett. **27**(4), 1055–1059 (2023)
24. L. Zhou, Y.B. Sheng, One-step device-independent quantum secure direct communication. Sci. China Phys. Mech. Astron. **65**(5), 250311 (2022)
25. L. Zhou, B.W. Xu, W. Zhong, Y.B. Sheng, Device-independent quantum secure direct communication with single-photon sources. Phys. Rev. Appl. **19**(1), 014036 (2023)
26. C. Liu, C. Zhang, S.P. Gu, X.F. Wang, L. Zhou, Y.B. Sheng, Receiver-device-independent quantum secure direct communication. Sci. China Phys. Mech. Astron. **68**(5), 250311 (2025)
27. P. Roy, S. Bera, S. Gupta, A.S. Majumdar, Device-independent quantum secure direct communication under non-Markovian quantum channels. Quantum Inf. Process **23**(5), 170 (2024)
28. F. Xu, Y.Z. Zhang, Q. Zhang, J. Pan, Device-independent quantum key distribution with random post selection. Phys. Rev. Lett. **128**, 110506 (2022)
29. D. Pan, G.L. Long, L. Yin, Y.B. Sheng, D. Ruan, S.X. Ng et al., The evolution of quantum secure direct communication: on the road to the qinternet. IEEE Commun. Surv. Tutorials. 26(3), 1898–1949
30. D. Pan, Y.C. Liu, P. Niu, H. Zhang, F. Zhang, M. Wang et al., Simultaneous transmission of information and key exchange using the same photonic quantum states. Sci. Adv. **11**(8), eadt4627 (2025)
31. P.H. Niu, Z.R. Zhou, Z.S. Lin, Y.B. Sheng, L.G. Yin, G.L. Long, Measurement-device-independent quantum communication without encryption. Sci. Bull. **63**(20), 1345–1350 (2018)
32. Z. Zhou, Y. Sheng, P. Niu, L. Yin, G. Long, L. Hanzo, Measurement-device-independent quantum secure direct communication. Sci. China Phys. Mech. Astron. **63**(3), 230362 (2020)
33. P.H. Niu, J.W. Wu, L.G. Yin, G.L. Long, Security analysis of measurement-device-independent quantum secure direct communication. Quantum Inf. Process **19**(10), 356 (2020)
34. Z. Z. Sun, Y. B. Cheng, D. Ruan, D. Pan, Single-photon measurement-device-independent quantum secure direct communication. Opt. Commun. 130745;569, (2024)
35. N. Das, G. Paul, Improving the security of measurement-device-independent quantum communication without encryption. Sci. Bull. **65**(24), 2048–2049 (2020)
36. N. Das, G. Paul, Measurement device-independent quantum secure direct communication with user authentication. Quantum Inf. Process **21**(7), 260 (2022)
37. R. Guo, R.G. Zhou, X.X. Zhang, Measurement-device-independent multi-party quantum secure direct communication. Quantum Inf. Process **23**(9), 1–17 (2024)
38. X.D. Wu, L. Zhou, W. Zhong, Y.B. Sheng, High-capacity measurement-device-independent quantum secure direct communication. Quantum Inf. Process **19**, 1–14 (2020)
39. T.J. Pan, R.G. Zhou, X.X. Zhang, Measurement-device-independent quantum secure direct communication based on quantum cover channel and multiple degrees of freedom of hyperentanglement. Phys. Scr. **100**(2), 025114 (2025)
40. C. Shukla, A. Banerjee, A. Pathak, R. Srikanth, Secure quantum communication with orthogonal states. Int. J. Quantum Inf. **14**(06), 1640021 (2016)
41. A. Avella, G. Brida, I.P. Degiovanni, M. Genovese, M. Gramegna, P. Traina, Experimental quantum-cryptography scheme based on orthogonal states. Phys. Rev. A At. Mol. Opt. Phys. **82**(6), 062309 (2010)
42. R.D. Sharma, K. Thapliyal, A. Pathak, A.K. Pan, A. De, Which verification qubits perform best for secure communication in noisy channel? Quantum Inf. Process **15**, 1703–1718 (2016)
43. P. Yadav, R. Srikanth, A. Pathak, Two-step orthogonal-state-based protocol of quantum secure direct communication with the help of order-rearrangement technique. Quantum Inf. Process **13**, 2731–2743 (2014)
44. C. Shukla, N. Alam, A. Pathak, Protocols of quantum key agreement solely using Bell states and Bell measurement. Quantum Inf. Process **13**(11), 2391–2405 (2014)
45. C. Shukla, A. Pathak, Orthogonal-state-based deterministic secure quantum communication without actual transmission of the message qubits. Quantum Inf. Process **13**, 2099–2113 (2014)
46. A. Banerjee, C. Shukla, K. Thapliyal, A. Pathak, P.K. Panigrahi, Asymmetric quantum dialogue in noisy environment. Quantum Inf. Process **16**, 1–23 (2017)
47. C. Shukla, K. Thapliyal, A. Pathak, Semi-quantum communication: protocols for key agreement, controlled secure direct communication and dialogue. Quantum Inf. Process **16**, 1–19 (2017)
48. X.H. Li, F.G. Deng, H.Y. Zhou, Efficient quantum key distribution over a collective noise channel. Phys. Rev. A **78**, 022321 (2008)
49. Y.B. Sheng, F.G. Deng, G.L. Long, Complete hyperentangled-Bell-state analysis for quantum communication. Phys. Rev. A At. Mol. Opt. Phys. **82**(3), 032318 (2010)
50. X.H. Li, S. Ghose, Complete hyperentangled Bell state analysis for polarization and time-bin hyperentanglement. Opt. Express **24**(16), 18388–18398 (2016)
51. Q. Liu, G.Y. Wang, Q. Ai, M. Zhang, F.G. Deng, Complete nondestructive analysis of two-photon six-qubit hyperentangled Bell states assisted by cross-Kerr nonlinearity. Sci. Rep. **6**(1), 22016 (2016)
52. W.P. Grice, Arbitrarily complete Bell-state measurement using only linear optical elements. Phys. Rev. A At. Mol. Opt. Phys. **84**(4), 042331 (2011)
53. M. Sisodia, A. Shukla, A. Pathak, Experimental realization of nondestructive discrimination of Bell states using a five-qubit quantum computer. Phys. Lett. A **381**(46), 3860–3874 (2017)
54. J.R. Samal, M. Gupta, P.K. Panigrahi, A. Kumar, Non-destructive discrimination of Bell states by NMR using a single ancilla qubit. J. Phys. B At. Mol. Opt. Phys. **43**(9), 095508 (2010)
55. N.B. An, Secure dialogue without a prior key distribution. J.-Korean Phys. Soc. **47**(4), 562 (2005)
56. C.Y. Lin, C.W. Yang, T. Hwang, Authenticated quantum dialogue based on Bell states. Int. J. Theor. Phys. **54**, 780–786 (2015)
57. A. Cabello, Quantum key distribution in the Holevo limit. Phys. Rev. Lett. **85**(26), 5635 (2000)

Publisher's Note