

Measurement-Device-Independent Quantum Secure Direct Communication Based on Decoy States and Polarization--Spatial Hyperentanglement

Huayao Zhang

Shanghai Maritime University

Rigui Zhou

rgzhou@shmtu.edu.cn

Shanghai Maritime University

Research Article

Keywords: quantum secure direct communication, measurement-device-independent, polarization--spatial hyperentanglement, decoy-state

Posted Date: July 1st, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-10101864/v1>

License:   This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: No competing interests reported.

Version of Record: A version of this preprint was published at Quantum Information Processing on September 23rd, 2026. See the published version at <https://doi.org/10.1007/s11128-026-05340-9>.

Measurement-Device-Independent Quantum Secure Direct Communication Based on Decoy States and Polarization–Spatial Hyperentanglement

Huayao Zhang¹ and Rigui Zhou^{1*}

¹College of Information Engineering, Shanghai Maritime University,
Shanghai, 201306, China.

*Corresponding author(s). E-mail(s): rgzhou@shmtu.edu.cn;
Contributing authors: hyyozhang@163.com;

Abstract

Quantum secure direct communication (QSDC) can directly transmit confidential messages without pre-distributing secret keys. In practical applications, non-ideal light sources naturally contain multiphoton components, which can easily lead to photon-number-splitting attacks and constitute a core problem restricting secure practical implementation. Existing measurement-device-independent (MDI) QSDC protocols are mostly based on ideal source assumptions and lack strict security authentication for practical multiphoton risks. This paper proposes an MDI-QSDC protocol based on decoy states and polarization–spatial hyperentanglement. The protocol lower-bounds the contribution of the two-single-pair sector through an active three-intensity decoy-state mechanism and imposes a conservative bound on the potential information leakage caused by multiphoton events, while using polarization–spatial hyperentangled encoding to increase the payload of each valid HBSA event and relying on the MDI architecture to remove the need to trust the measurement device. Compared with similar schemes, this protocol significantly improves the secure message capacity in practical scenarios while maintaining detector-side security.

Keywords: quantum secure direct communication, measurement-device-independent, polarization–spatial hyperentanglement, decoy-state

1 Introduction

Quantum secure direct communication (QSDC) aims to transmit confidential messages directly through quantum carriers without first generating a shared secret key. Early deterministic secure communication and direct-communication protocols showed that classical confidential information can be embedded in quantum states [1, 2]. Deng et al. then proposed a two-step protocol based on Einstein–Podolsky–Rosen (EPR) pairs, separating channel security checking from message transmission [3]. This separation has become a common design principle in QSDC. Subsequent work extended QSDC to single photons, entangled systems, long-distance fiber links and multi-user networks [4–10]. These studies have moved QSDC from idealized protocol design toward practical quantum communication systems.

A central obstacle in practical QSDC is the non-ideal source. Weak coherent sources and spontaneous parametric down-conversion (SPDC) sources inevitably emit vacuum, single-photon or single-pair components, and multiphoton or multipair components. The latter may enable photon-number-splitting (PNS) attacks or quantum-storage attacks, which is especially serious for QSDC because the message itself, rather than a later-generated key, is carried by the transmitted quantum states. Decoy-state methods were first developed in quantum key distribution (QKD) to estimate the single-photon contribution under lossy practical sources [11–14]. The Gottesman–Lo–Lutkenhaus–Preskill (GLLP) tagged-component idea and decoy-state analysis with entangled photon sources further clarified how non-ideal source components can be handled in security proofs [15, 16]. In QSDC, practical active and passive decoy-state protocols have been used to estimate source statistics before message-bearing events are accepted [17–20]. These protocols strengthen source-side security, but most of them still use a single degree of freedom for information encoding.

Another route to higher secure message capacity is to enlarge the encoding alphabet. Hyperentanglement means simultaneous entanglement of the same photon pair in more than one degree of freedom (DoF). Polarization–spatial hyperentangled photon pairs can be produced by SPDC-based optical sources [21–23]. Hyperentangled Bell-state analysis (HBSA) can then distinguish a larger set of joint polarization and spatial-mode labels than ordinary single-DoF Bell-state analysis [24–26]. In the polarization–spatial case, the four polarization Bell states and four spatial-mode Bell states form 16 orthogonal hyperentangled Bell states. A successful HBSA event can therefore carry a four-bit label. Dense coding and hyperentanglement-based QSDC exploit this structure to increase the conclusive-event information content [27–29]. However, hyperentanglement-based protocols are often discussed under idealized source assumptions, leaving the multipair risk of practical SPDC sources insufficiently connected with the secure message capacity analysis.

Measurement devices introduce a different security boundary problem. Detector-efficiency mismatch, time-shift attacks and bright-light blinding attacks show that real detectors may deviate from the ideal measurement model [30, 31]. The measurement-device-independent (MDI) idea, introduced by Lo et al., moves the joint measurement to an untrusted relay while keeping state preparation and classical post-processing inside the trusted user stations [32, 33]. In QSDC, MDI protocols place Bell-state measurements at an untrusted Charlie, so detector-side imperfections are removed

from the trusted boundary [34]. High-capacity MDI-QSDC and one-photon-interference QSDC have further explored larger alphabets and multi-intensity parameter estimation [35–37]. Recent polarization–spatial hyperentangled MDI-QSDC has shown that a four-bit conclusive-event information content can be combined with an MDI topology [38]. Nevertheless, a complete practical framework should simultaneously address three issues: practical SPDC source statistics, detector-side untrusted measurements and high-dimensional message carrying.

Motivated by these limitations, we propose a dual-source decoy-state polarization–spatial hyperentangled MDI-QSDC protocol. Alice and Bob independently prepare active three-intensity SPDC hyperentangled sources and send travelling photons to an untrusted Charlie for HBSA. The first round uses delayed intensity-class disclosure and random Pauli-frame labels to support decoy-state estimation of the certified single-pair contribution. The second round uses the retained photons for four-bit message encoding and private Pauli masking. The masking idea follows the information-theoretic protection used in high-capacity QSDC and private dense-coding studies [39, 40]. Compared with decoy-state QSDC using a single DoF, the proposed protocol provides a four-bit conclusive-event information content. Compared with ideal-source hyperentangled MDI-QSDC, it explicitly treats vacuum and multipair components as tagged events in the secure message capacity bound.

The remainder of this paper is organized as follows. Section 2 introduces the hyperentangled Bell-state alphabet, the HBSA announcement model and the active three-intensity SPDC source. Section 3 presents the protocol steps. Section 4 derives the decoy-state constraints, tagged-event leakage and secure message capacity bound. Section 5 gives numerical comparisons and hardware-parameter scans. Section 6 concludes the paper.

2 Preliminaries

2.1 Hyperentangled Bell states

Polarization–spatial hyperentangled Bell states are the information carriers of the protocol and provide the physical basis for a four-bit conclusive-event information content. Hyperentanglement means that the same photon pair is entangled in more than one degree of freedom (DoF) [21, 22]. We use two DoFs. The polarization space is spanned by the horizontal state $|H\rangle$ and the vertical state $|V\rangle$. The spatial-mode space is spanned by Alice’s paths $|a_1\rangle, |a_2\rangle$ and Bob’s paths $|b_1\rangle, |b_2\rangle$.

The standard polarization Bell basis is defined as

$$|\phi^\pm\rangle_p = \frac{|H\rangle_A \otimes |H\rangle_B \pm |V\rangle_A \otimes |V\rangle_B}{\sqrt{2}}, \quad (1)$$

$$|\psi^\pm\rangle_p = \frac{|H\rangle_A \otimes |V\rangle_B \pm |V\rangle_A \otimes |H\rangle_B}{\sqrt{2}}. \quad (2)$$

The spatial-mode Bell basis is

$$|\phi^\pm\rangle_s = \frac{|a_1\rangle_A \otimes |b_1\rangle_B \pm |a_2\rangle_A \otimes |b_2\rangle_B}{\sqrt{2}}, \quad (3)$$

$$|\psi^\pm\rangle_s = \frac{|a_1\rangle_A \otimes |b_2\rangle_B \pm |a_2\rangle_A \otimes |b_1\rangle_B}{\sqrt{2}}. \quad (4)$$

A polarization–spatial hyperentangled Bell state is the tensor product of the two Bell states,

$$|\Xi_h\rangle = |\beta_{h_P}\rangle_P \otimes |\beta_{h_S}\rangle_s, \quad h = (h_P, h_S) \in \mathbb{Z}_2^2 \times \mathbb{Z}_2^2 \cong \mathbb{Z}_2^4. \quad (5)$$

Here $|\beta_{h_P}\rangle_P$ and $|\beta_{h_S}\rangle_s$ denote the four Bell states in the polarization and spatial-mode DoFs, respectively. The joint label $h \in \mathbb{Z}_2^4$ is a four-bit binary string and uniquely identifies one of the 16 orthogonal hyperentangled Bell states. Without loss of generality, the initial state before local encoding is chosen as $|\Xi_0\rangle = |\phi^+\rangle_P \otimes |\phi^+\rangle_s$.

For both DoFs we use the same two-bit label convention,

$$|\beta_{00}\rangle = |\phi^+\rangle, \quad |\beta_{01}\rangle = |\phi^-\rangle, \quad |\beta_{10}\rangle = |\psi^+\rangle, \quad |\beta_{11}\rangle = |\psi^-\rangle. \quad (6)$$

Thus $h = (h_P, h_S)$ specifies the polarization label h_P and the spatial-mode label h_S . This choice fixes the Bell-labeling convention used by Alice, Bob and Charlie when announced HBSA labels are processed in the protocol.

Local Pauli operations applied by Alice and Bob are mathematically equivalent to bitwise addition modulo 2 on the hyperentangled Bell label in $\mathbb{Z}_2^4$, while the underlying two-DoF entangled structure is preserved. Therefore, the 16 orthogonal states form a complete four-bit alphabet. All message labels m_i , Bob masks r_i and HBSA output labels h_i are processed in $\mathbb{Z}_2^4$, with addition understood componentwise modulo 2. The hyperentangled Bell labels defined above are used consistently to describe the first-round entanglement-swapping announcement, the second-round message-readout announcement, and the local Pauli-label transformations performed by Alice and Bob.

2.2 HBSA model and hyperentanglement-swapping relation

In the MDI architecture, Charlie and all measurement devices inside his station are outside the trusted boundary. The security analysis therefore does not require Charlie to honestly implement a fixed optical HBSA circuit, nor does it assume ideal internal detectors. Charlie is used only through a classical announcement interface

$$\mathcal{M}_C : \rho_{A_2 B_2} \longrightarrow h \in \Omega_{\text{HBSA}} \cup \{\perp\}. \quad (7)$$

Here A_2 and B_2 denote the travelling photons sent by Alice and Bob, $h = (h_P, h_S)$ is a joint polarization–spatial Bell label, $\Omega_{\text{HBSA}} \subseteq \mathbb{Z}_2^4$ is the set of labels that a given honest implementation can identify uniquely, and $\perp$ denotes loss, an invalid coincidence, a degenerate outcome or any other inconclusive announcement. Equation (7) is an input–output interface, not a trusted measurement assumption in the security proof.

The protocol nevertheless needs HBSA labels for two operational reasons. In the first round, HBSA on the travelling photons performs hyperentanglement swapping

and assigns a conditional Bell label to the photons retained by Alice and Bob. In the second round, HBSA reads out the label shift produced by Alice’s message operation and Bob’s private Pauli mask. For the first round, Alice and Bob prepare

$$|\Xi_0\rangle_{A_1 A_2}, \quad |\Xi_0\rangle_{B_1 B_2}, \quad (8)$$

where A_1 and B_1 are retained locally and A_2 and B_2 are sent to Charlie. Under the Bell-label convention of Section 2.1, the ideal swapping relation can be written in the compact form

$$|\Xi_0\rangle_{A_1 A_2} |\Xi_0\rangle_{B_1 B_2} = \frac{1}{4} \sum_{h \in \mathbb{Z}_2^4} \omega_h |\Xi_{f(h)}\rangle_{A_1 B_1} |\Xi_h\rangle_{A_2 B_2}. \quad (9)$$

The phase factor ω_h depends only on the Bell-state sign convention and has no effect on the classical label processing. The fixed map f gives the retained-photon label determined by Charlie’s travelling-photon HBSA label. We do not assume $f(h) = h$ without convention checking; instead, the mapping is absorbed into the corrected first-round label used in Section 3.

In an honest performance model, Charlie’s analyser is designed to distinguish the hyperentangled Bell basis

$$\mathcal{B}_{\text{HBSA}} = \{|\Xi_h\rangle = |\beta_{h_P}\rangle_P \otimes |\beta_{h_S}\rangle_S : h = (h_P, h_S) \in \mathbb{Z}_2^4\}. \quad (10)$$

Complete discrimination of all 16 polarization–spatial hyperentangled Bell states usually requires auxiliary entanglement, nonlinear interactions, cavity-assisted interactions, QND measurements or other enhanced measurement resources [24–26]. Only under such a complete-HBSA honest-device model do we set

$$\Omega_{\text{HBSA}}^{\text{full}} = \mathbb{Z}_2^4, \quad |\Omega_{\text{HBSA}}^{\text{full}}| = 16. \quad (11)$$

For a partial HBSA implementation, only labels that are uniquely identified enter Ω_{HBSA} ; unresolved labels, mode mismatch, photon loss and invalid coincidences are all assigned to $\perp$. This reduces the conclusive rate but does not change the definition of a successfully announced label.

For the honest-device performance model used in the numerical simulation, conclusive outcomes may be represented by the idealized POVM

$$E_h = p_{\text{HBSA}} |\Xi_h\rangle \langle \Xi_h| \quad (h \in \Omega_{\text{HBSA}}), \quad E_{\perp} = I - \sum_{h \in \Omega_{\text{HBSA}}} E_h. \quad (12)$$

This representation is not imposed on an adversarial Charlie in the MDI security analysis. The intrinsic HBSA success probability is defined as

$$p_{\text{HBSA}} = \Pr(h \in \Omega_{\text{HBSA}} \mid \text{valid hyperentangled two-photon input}). \quad (13)$$

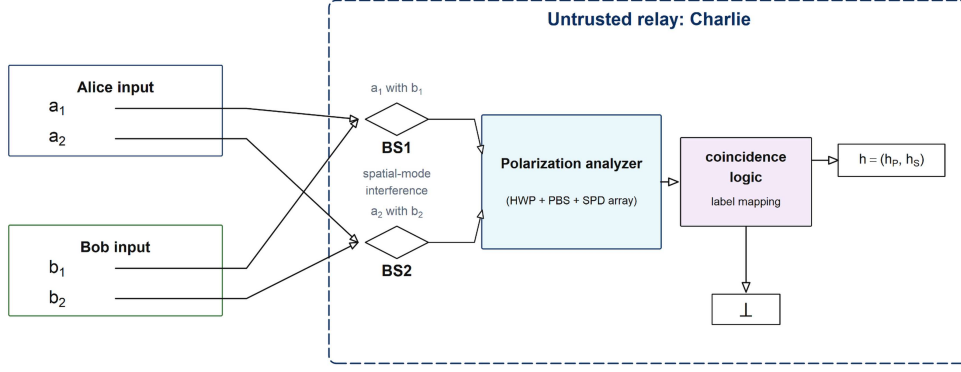


Fig. 1 Conceptual HBSA relay in Charlie's untrusted domain. Alice's travelling rails a_1, a_2 and Bob's travelling rails b_1, b_2 are processed to produce a public joint label $h = (h_P, h_S)$ or the failure symbol $\perp$.

Figure 1 summarizes only the functional flow of the untrusted relay. The two beam splitters BS1 and BS2 represent the spatial-interference branches for the mode pairs (a_1, b_1) and (a_2, b_2) , respectively. The polarization-analyzer block is a compact functional description of the polarization-measurement stage, while the coincidence-logic block converts detector-click patterns into the announced classical label $h = (h_P, h_S)$. Hence the figure should be read as an input–output model of Charlie's HBSA interface rather than as a complete deterministic optical implementation for resolving all 16 hyperentangled Bell states.

The parameter p_{HBSA} does not include the SPDC emission probability, the users' intensity-class probabilities, channel transmittance, quantum-memory efficiency or detector efficiency. If an implementation reports a total conclusive probability including detector and mode-matching losses, it must first be decomposed before being inserted into the simulations; schematically,

$$p_{\text{con}} = p_{\text{HBSA}} \eta_{\text{mode}} \eta_d^k, \quad (14)$$

where η_{mode} denotes mode-overlap and interferometric visibility losses and k is the implementation-dependent number of effective detector clicks required for a successful HBSA event.

Equation (7) is implemented operationally through the interface illustrated in Fig. 1. It should not be interpreted as two independent measurements on copied photons. The same travelling photons first carry the spatial-mode interference information and are then analysed in polarization, so the spatial label h_S and polarization label h_P are extracted from one joint detector-coincidence event inside Charlie's untrusted relay. In the protocol data flow, the first HBSA supplies $h_i^{(1)}$ for entanglement swapping and source testing, whereas the second HBSA supplies $h_i^{(2)}$ for message recovery.

2.3 Practical hyperentangled SPDC source and decoy-state statistics

A practical spontaneous parametric down-conversion (SPDC) source cannot deterministically emit exactly one photon pair in every pump slot. Instead, it contains vacuum, single-pair and multipair components. Multipair components may support photon-number-splitting (PNS) and quantum-storage attacks. This point is especially important in QSDC, because plaintext is transmitted directly and leaked information cannot be repaired afterwards by privacy amplification as in quantum key distribution (QKD). The role of the decoy-state method is therefore not to identify the photon-pair number of each individual slot. It is to bound, at the aggregate statistical level, the single-pair contribution that can be credited to the secure message capacity, so that uncertified events can be subtracted in the later security analysis under a worst-case rule.

We denote by μ the mean photon-pair number in one pump slot. For a phase-randomized SPDC source, the probability of emitting n photon pairs follows the thermal, or geometric, distribution

$$P_n(\mu) = \frac{\mu^n}{(1 + \mu)^{n+1}}, \quad n = 0, 1, 2, \dots \quad (15)$$

Alice and Bob randomly choose their intensity classes from the signal, weak decoy-state and near-vacuum classes, denoted by $x, y \in \{s, d, v\}$, with corresponding mean photon-pair numbers μ_x and μ_y . The symbol (x, y) denotes Alice's and Bob's joint intensity pair, not a new joint source. The physical premise of the decoy-state method is that, under the same channel and measurement conditions, the conditional yield Y_{nm} and error rate e_{nm} of a given photon-pair-number component (n, m) are independent of the selected intensities μ_x and μ_y .

The SPDC device is assumed to generate the spatial Bell component inside the interferometric source. For one user's source, writing ℓ and t for the retained and travelling photons, respectively, the ideal single-pair component may be represented as

$$|\Xi_0\rangle_{\ell t} = |\phi^+\rangle_{p, \ell t} \otimes \frac{|\ell_1\rangle_\ell \otimes |t_1\rangle_t + e^{i\phi_s} |\ell_2\rangle_\ell \otimes |t_2\rangle_t}{\sqrt{2}}. \quad (16)$$

The travelling modes $|t_1\rangle$ and $|t_2\rangle$ are later relabelled as $|a_1\rangle, |a_2\rangle$ for Alice's source and $|b_1\rangle, |b_2\rangle$ for Bob's source. Thus the two spatial rails are part of the pair-generation process, as in a Sagnac or dual-path SPDC source, rather than the output of a post-SPDC beamsplitter applied to a single photon.

Figure 2 gives the preparation module assumed at each trusted station in a compact form, rather than a full protocol-flow diagram. The classical control chain RNG/class *ightarrow* IM indicates that a random intensity class $x \in \{s, d, v\}$ is first selected and then used to set the mean photon-pair number μ_x . Here PR denotes phase randomization, IM denotes intensity modulation, and the PBS-based Sagnac HE-SPDC block represents the interferometric hyperentangled source. The label PPLN/BBO

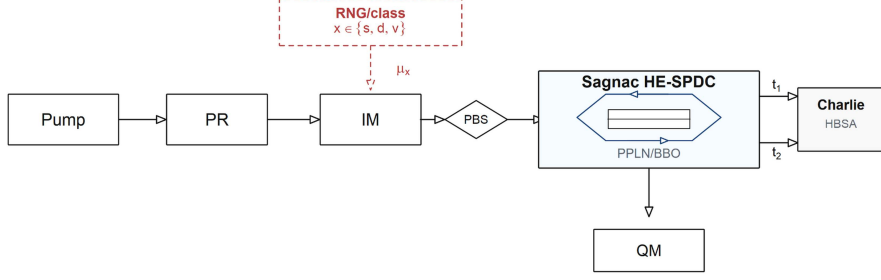


Fig. 2 Conceptual trusted source module with active intensity selection and HE-SPDC preparation. The pump is phase-randomized and intensity-modulated before entering the Sagnac HE-SPDC source; the travelling rails t_1, t_2 are sent to Charlie for HBSA and the retained photon is stored locally.

inside the source is used only to indicate a typical nonlinear medium for SPDC pair generation, not to restrict the protocol to a unique crystal choice.

The optical outputs t_1 and t_2 are the two travelling spatial rails emitted by the source and sent to Charlie, while the retained photon is stored in the local quantum memory QM for the second round. In the later protocol description, t_1, t_2 are relabelled as a_1, a_2 for Alice and as b_1, b_2 for Bob. This convention fixes the meaning of μ_x , a_1/a_2 , b_1/b_2 , and η_m used throughout the protocol and the secure-capacity analysis. The detailed step-by-step operations associated with these prepared states are given in Section 3.

The first-round checking statistic is defined only on protocol-specified checking samples, not by comparing every valid HBSA label with one fixed target label. In a conclusive checking slot, the retained-photon label inferred from Charlie's announcement and the local first-round Pauli frames is

$$\tilde{h}_i^{(1)} = f\left(h_i^{(1)}\right) \oplus t_i^A \oplus t_i^B. \quad (17)$$

The users then test whether the measured or otherwise opened checking data satisfy the correlation rule determined by $\tilde{h}_i^{(1)}$. This definition keeps the entanglement-swapping map, Alice's Pauli frame and Bob's Pauli frame in a single consistent label.

For a joint intensity pair (x, y) , let N_{xy} , C_{xy} and W_{xy} be the number of transmitted pump slots, the number of conclusive first-round HBSA announcements and the number of conclusive checking events that violate the protocol-defined correlation rule, respectively. The observed gain and error-weighted gain are

$$Q_{xy}^{\text{obs}} = \frac{C_{xy}}{N_{xy}}, \quad T_{xy}^{\text{obs}} = \frac{W_{xy}}{N_{xy}}. \quad (18)$$

The corresponding true gain and error-weighted gain satisfy

$$\begin{aligned} Q_{xy} &= \sum_{n,m \geq 0} P_n(\mu_x) P_m(\mu_y) Y_{nm}, \\ T_{xy} &= \sum_{n,m \geq 0} P_n(\mu_x) P_m(\mu_y) Z_{nm}. \end{aligned} \tag{19}$$

Here Y_{nm} is the conditional probability that Charlie announces a conclusive HBSA label $h \neq \perp$ when Alice sends n travelling photons and Bob sends m travelling photons in the same slot. The quantity Z_{nm} is the conditional probability of a conclusive checking-event violation, so that $Z_{nm} = e_{nm} Y_{nm}$ and $0 \leq Z_{nm} \leq Y_{nm}$. For $n \geq 2$ or $m \geq 2$, the HBSA device may produce multi-click patterns, wrong labels or inconclusive outcomes because it is designed for the two-photon hyperentangled Bell subspace. The decoy-state LP therefore estimates the single-pair sector $(n, m) = (1, 1)$ for secure-message credit, while the conclusive part of all uncertified multiphoton responses is treated as tagged events and subtracted in Section 4 under a worst-case leakage rule.

In finite data, the observed quantities are first converted into confidence intervals for the true expectation values by Chernoff or Hoeffding bounds,

$$Q_{xy}^- \leq Q_{xy} \leq Q_{xy}^+, \quad T_{xy}^- \leq T_{xy} \leq T_{xy}^+. \tag{20}$$

These macroscopic constraints are the inputs of the finite-statistical linear programme (LP) in Section 4, which yields the single-pair yield lower bound Y_{11}^L and the single-pair error-rate upper bound e_{11}^U . Because the SPDC distribution has a long tail, the probability mass above the cutoff n_{cut} is treated conservatively as worst-case uncertainty.

3 Protocol Description

The protocol involves trusted users Alice and Bob, and an untrusted relay Charlie. Let N be the total number of pump slots and let $S_{\text{raw}} = \{1, 2, \dots, N\}$ denote the set of all initial slots. After the first-round source authentication, the surviving signal-intensity slots form the message-candidate set S_{cand} . Alice and Bob then choose a hidden test subset $S_{\text{test}} \subset S_{\text{cand}}$ and use the remaining subset $S_{\text{msg}} = S_{\text{cand}} \setminus S_{\text{test}}$ for actual message transmission, so that $S_{\text{cand}} = S_{\text{test}} \cup S_{\text{msg}}$ and $S_{\text{test}} \cap S_{\text{msg}} = \emptyset$. All state preparation, storage and local Pauli operations are performed inside the trusted user stations, whereas Charlie only provides HBSA announcements through the untrusted interface of Eq. (7) over an authenticated classical channel.

Figure 3 separates the data flow into trusted Alice, untrusted Charlie and trusted Bob. The upper layer is Round 1, which authenticates the source statistics before plaintext is encoded. The lower layer is Round 2, which carries the masked message and supplies the final HBSA label for Bob's recovery.

Step 1. State Preparation and First-Round Transmission. In each slot $i \in S_{\text{raw}}$, Alice and Bob independently choose intensity classes $x_i, y_i \in \{s, d, v\}$ with corresponding intensities μ_{x_i} and μ_{y_i} , and independently sample random Pauli-frame

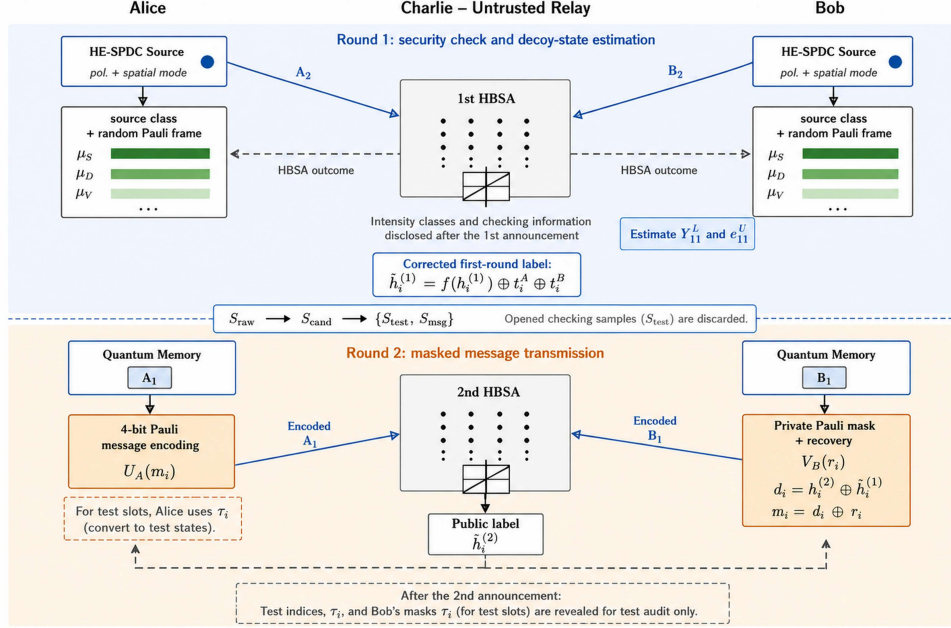


Fig. 3 Decoy-state hyperentangled MDI-QSDC protocol. In Round 1, Alice and Bob independently select private intensity classes and random first-round Pauli-frame labels, send travelling photons to Charlie for the first HBSA and store their local photons. Charlie announces the first label or the failure symbol before the users disclose the intensity classes and checking labels used for decoy-state estimation. In Round 2, Alice encodes a four-bit message, Bob applies a private four-bit Pauli mask, Charlie performs the second HBSA and Bob recovers the plaintext.

labels $t_i^A, t_i^B \in \mathbb{Z}_2^4$. Alice prepares $|\Xi_0\rangle_{A_1 A_2}$ and Bob prepares $|\Xi_0\rangle_{B_1 B_2}$. The travelling photons A_2 and B_2 are sent to Charlie, while the retained photons A_1 and B_1 are kept in local quantum memories. The local first-round Pauli frames t_i^A and t_i^B are applied within the trusted stations so that they act as Bell-label translations after the first-round swapping relation. If a near-vacuum class is chosen or no pair is emitted in a given slot, that side sends no travelling photon in that slot.

Step 2. First-Round HBSA and Delayed Disclosure. Charlie announces the first-round outcome $h_i^{(1)} \in \Omega_{\text{HBSA}} \cup \{\perp\}$ for each slot through the interface of Eq. (7). In the honest-device performance model this announcement is associated with the basis $\mathcal{B}_{\text{HBSA}}$ of Eq. (10), but the security analysis does not trust Charlie's internal measurement. Crucially, Alice and Bob keep (x_i, y_i, t_i^A, t_i^B) private until Charlie has completed his first-round announcement. Afterward, they disclose the intensity classes needed for decoy grouping and open the Pauli-frame information only for checking and candidate processing. For each conclusive slot, the corrected first-round label is

$$\tilde{h}_i^{(1)} = f(h_i^{(1)}) \oplus t_i^A \oplus t_i^B. \quad (21)$$

This delayed disclosure prevents Charlie from adapting his public outcome to the intensity class or the hidden Pauli twirling.

Step 3. Decoy-State Estimation and Set Partitioning. Alice and Bob group the first-round data by joint intensity pair (x, y) and by the checking information opened after Charlie's announcement. They record the slot numbers N_{xy} , conclusive counts C_{xy} and checking-error counts W_{xy} , where W_{xy} counts only conclusive checking events that violate the protocol-defined correlation rule associated with $\tilde{h}_i^{(1)}$. Operationally, a checking sample is opened by measuring or otherwise revealing the retained-photon correlation required for the test; such opened slots are not reused for plaintext transmission. Alice and Bob then solve the finite-statistical linear programme of Section 4 to obtain the single-pair yield lower bound Y_{11}^L and the single-pair error-rate upper bound e_{11}^U . If the security threshold is not met, the protocol aborts. Otherwise, the unopened slots with $x_i = y_i = s$ and $h_i^{(1)} \neq \perp$ form S_{cand} , and Alice and Bob randomly partition S_{cand} into the hidden test set S_{test} and the message set S_{msg} .

Step 4. Message Encoding and Private Masking. For each $i \in S_{\text{msg}}$, Alice applies the four-bit message operation $U_A(m_i)$ and Bob applies the private four-bit mask $V_B(r_i)$ to their retained photons. For each $i \in S_{\text{test}}$, Alice applies a random test operation $U_A(\tau_i)$, while Bob still applies his private mask $V_B(r_i)$. Both users then send the encoded photons to Charlie. By the hyperentangled Bell-label shift property in Section 2.1, the encoded state for a message slot evolves as

$$|\Psi_i\rangle = U_A(m_i) \otimes V_B(r_i) |\Xi_{\tilde{h}_i^{(1)}}\rangle = |\Xi_{\tilde{h}_i^{(1)} \oplus m_i \oplus r_i}\rangle. \quad (22)$$

For a hidden-test slot, m_i in Eq. (22) is replaced by τ_i .

Step 5. Second-Round HBSA and Auditing. Charlie performs the second HBSA and announces $h_i^{(2)} \in \Omega_{\text{HBSA}} \cup \{\perp\}$. The test-set indices remain hidden until this second-round announcement is complete. Alice and Bob then reveal the indices of S_{test} , the corresponding test labels τ_i , and Bob's masks for the test slots only. The check compares $h_i^{(2)}$ with the expected label shift generated from $\tilde{h}_i^{(1)}$, τ_i and the revealed test-slot mask. Bob's message-slot masks are never disclosed. If the hidden-test error exceeds the prescribed confidence interval, the protocol aborts. Otherwise, the message slots with $i \in S_{\text{msg}}$ and $h_i^{(2)} \neq \perp$ are accepted for final recovery.

Step 6. Message Recovery. For each accepted message slot, Bob calculates the two-round label difference

$$d_i = h_i^{(2)} \oplus \tilde{h}_i^{(1)}. \quad (23)$$

By the label-shift property of hyperentangled Bell states, a valid message slot satisfies

$$h_i^{(2)} = \tilde{h}_i^{(1)} \oplus m_i \oplus r_i, \quad (24)$$

and therefore $d_i = m_i \oplus r_i$. Bob recovers the plaintext through

$$m_i = d_i \oplus r_i. \quad (25)$$

The rigorous derivation of this recovery rule is given in Section 4.

4 Security Analysis and Secure Message Capacity Bound

4.1 Source authentication and tagged-event subtraction against PNS attacks

Practical SPDC sources inevitably contain multipair components, which may allow Eve to mount PNS or quantum-storage attacks. Unlike QKD, QSDC directly transmits plaintext and cannot rely on later privacy amplification to compress already leaked message information. The active three-intensity decoy-state statistics are therefore used to certify, in aggregate, the single-pair contribution that may be credited to the secure message capacity.

In the dual-source MDI architecture, the fluctuation analysis is performed on the joint intensity-pair statistics. The elementary random variable is therefore a pump slot conditioned on $(x, y) \in \mathcal{X}^2$ with $\mathcal{X} = \{s, d, v\}$, rather than two independent one-sided fluctuations for Alice and Bob. For a joint intensity pair (x, y) , define the observed gain and checking-label error gain as $\hat{Q}_{xy} = C_{xy}/N_{xy}$ and $\hat{T}_{xy} = W_{xy}/N_{xy}$. We allocate the linear-programme failure probability as $\varepsilon_{Q,xy} = \varepsilon_{T,xy} = \varepsilon_{\text{LP}}/(2|\mathcal{X}|^2) = \varepsilon_{\text{LP}}/18$. Using the additive Chernoff–Hoeffding confidence interval for Bernoulli observations [18, 33, 41–43],

$$\begin{aligned} Q_{xy}^{\pm} &= \left[\hat{Q}_{xy} \pm \sqrt{\frac{\ln(2/\varepsilon_{Q,xy})}{2N_{xy}}} \right]_0^1, \\ T_{xy}^{\pm} &= \left[\hat{T}_{xy} \pm \sqrt{\frac{\ln(2/\varepsilon_{T,xy})}{2N_{xy}}} \right]_0^1, \end{aligned} \quad (26)$$

where $[z]_0^1 = \min(1, \max(0, z))$. The multiplicative Chernoff form can also be used to obtain slightly tighter numerical intervals, but Eq. (26) is closed-form and conservative. A union bound gives simultaneous validity of all nine gain intervals and all nine error-gain intervals with probability at least $1 - \varepsilon_{\text{LP}}$. Hence the LP receives one joint confidence box for each intensity pair (x, y) , rather than separate independent fluctuation boxes for Alice and Bob.

The photon-pair-number cutoff is chosen before solving the LP. It is not a fitted simulation parameter. For a design tolerance ξ_{tail} satisfying $\xi_{\text{tail}} \ll \varepsilon_{\text{LP}}$, for example $\xi_{\text{tail}} \leq \varepsilon_{\text{LP}}/10$, we take

$$n_{\text{cut}} = \min \left\{ n : \max_{x,y \in \mathcal{X}} \left[1 - \left(\sum_{k=0}^n P_k(\mu_x) \right) \left(\sum_{\ell=0}^n P_{\ell}(\mu_y) \right) \right] \leq \xi_{\text{tail}} \right\}. \quad (27)$$

The residual tail mass

$$\tau_{xy}^{\text{tail}} = 1 - \left(\sum_{k=0}^{n_{\text{cut}}} P_k(\mu_x) \right) \left(\sum_{\ell=0}^{n_{\text{cut}}} P_{\ell}(\mu_y) \right) \quad (28)$$

is not ignored. It is inserted as worst-case uncertainty in the LP constraints. In numerical work, n_{cut} is increased until Eq. (27) is satisfied for all nine intensity pairs, and the same cutoff is then used for the gain and error-gain constraints,

$$\max(0, Q_{xy}^- - \tau_{xy}^{\text{tail}}) \leq \sum_{n,m \leq n_{\text{cut}}} P_n(\mu_x) P_m(\mu_y) Y_{nm} \leq Q_{xy}^+. \quad (29)$$

$$\max(0, T_{xy}^- - \tau_{xy}^{\text{tail}}) \leq \sum_{n,m \leq n_{\text{cut}}} P_n(\mu_x) P_m(\mu_y) Z_{nm} \leq T_{xy}^+, \quad (30)$$

with $0 \leq Z_{nm} \leq Y_{nm}$. The first-round random Pauli-frame labels and the swapping correction in Eq. (21) are essential in this step because the checking rule samples the HBSA label alphabet rather than comparing all conclusive outcomes with one fixed Bell label. The LP minimizes Y_{11} subject to Eq. (29) and maximizes Z_{11} subject to Eqs. (29) and (30). The resulting single-pair error-rate upper bound is

$$e_{11}^U = \min\left(1, \frac{Z_{11}^U}{Y_{11}^L}\right), \quad (31)$$

whenever $Y_{11}^L > 0$; otherwise the protocol aborts. The lower bound on the untagged single-pair message-acceptance gain is

$$Q_{\text{msg},11}^L = q_{\text{msg}} p_s^A p_s^B [P_1(\mu_s)]^2 Y_{11}^L \Gamma_2^L, \quad (32)$$

where Γ_2^L collects the independently calibrated lower bound for the second-round accepted-readout probability. In the simulations this factor is decomposed into the intrinsic HBSA term p_{HBSA} , the relevant channel transmittance, memory efficiency and detector-efficiency terms, following the separation in Eq. (14); p_{HBSA} itself is not used a second time to include detector loss. The core defence against PNS attacks is the worst-case subtraction of tagged events. Let Q_{msg}^+ be an upper bound on the total accepted message gain. The tagged-event gain is bounded by

$$Q_{\text{tag}}^U = \max(0, Q_{\text{msg}}^+ - Q_{\text{msg},11}^L). \quad (33)$$

In the worst case, Eve may obtain the full four-bit information content of every tagged event, including multipair emissions and vacuum mis-admissions. The eavesdropper information caused by PNS-type leakage is therefore upper bounded by

$$I(A:E)_{\text{PNS}} \leq 4Q_{\text{tag}}^U. \quad (34)$$

4.2 THA assumptions and blinding of the untrusted relay

The MDI architecture removes all detector-side attacks at Charlie, including time-shift and blinding attacks, from the trusted boundary. Alice's and Bob's source modulators and Pauli modulators, however, remain trusted local devices and must be protected against Trojan-horse attacks. We therefore assume calibrated optical isolators and narrowband wavelength filters at all optical ports, real-time monitoring taps that

abort anomalously strong injected pulses, and physical shielding that prevents different intensity classes or Pauli operations from producing distinguishable timing, spectral or modal side information. Any independently quantified residual side-channel leakage is included in the penalty Δ_{side} .

Charlie can observe both HBSA labels and the delayed intensity-class announcements, but Alice's plaintext m_i and Bob's message-slot mask r_i are never disclosed. Even if the first-round correction information is treated conservatively as public after Charlie's first announcement, a valid message slot satisfies $h_i^{(2)} = \tilde{h}_i^{(1)} \oplus m_i \oplus r_i$. Thus any two-round label difference available after the first-round correction has the form

$$d_i = h_i^{(2)} \oplus \tilde{h}_i^{(1)} = m_i \oplus r_i. \quad (35)$$

Unlike a computational pseudorandom-function mask, r_i is an information-theoretic one-time pad. Since r_i is independently and uniformly distributed over $\mathbb{Z}_2^4$, for any plaintext m_i and observation δ ,

$$\Pr(d_i = \delta \mid m_i) = \Pr(r_i = \delta \oplus m_i) = \frac{1}{16}. \quad (36)$$

Therefore, d_i and m_i are statistically independent, $I(m_i; d_i) = 0$. Together with delayed disclosure, the full public transcript T_C available to Charlie satisfies

$$I(m_i; T_C) = 0. \quad (37)$$

4.3 Secure message capacity lower bound

We now derive the capacity expression used in the numerical section, rather than introducing it without derivation. All information quantities are normalized per pump slot, so the unit is bit/pulse rather than bit/s. For a quantum adversary, $I(M; E)$ denotes the Holevo information between Alice's message variable M and Eve's quantum side information. Following the wiretap-channel treatment of secure direct communication [44–46], the secure message capacity is lower bounded by

$$C_s \geq [I(M; B) - I(M; E)]^+, \quad (38)$$

where B denotes Bob's final decoding data and E includes Eve's quantum system and Charlie's public transcript.

The legal information term is credited only to certified untagged single-pair events. Let U denote the event that a message slot belongs to the decoy-state-certified single-pair sector. The hyperentangled Bell label is a 16-symbol alphabet, so a noiseless conclusive event carries $\log_2 16 = 4$ bits. If the single-pair label error rate is e_{11} , Fano's inequality for a 16-ary alphabet gives

$$H(M \mid B, U) \leq h_2(e_{11}) + e_{11} \log_2 15 \equiv H_{16}(e_{11}), \quad (39)$$

where $h_2(\cdot)$ is the binary entropy. Therefore

$$I(M; B | U) = H(M | U) - H(M | B, U) \geq 4 - H_{16}(e_{11}). \quad (40)$$

Discarding any possible legal information from tagged events gives a conservative per-slot lower bound

$$I(M; B) \geq Q_{\text{msg},11}^L (4 - H_{16}(e_{11}^U)). \quad (41)$$

The eavesdropper-information term is bounded in the opposite direction. For untagged single-pair events, Charlie's public label difference is masked by Bob's uniform private Pauli label, and Eq. (37) gives zero mutual information between the plaintext and Charlie's transcript. Any residual leakage from imperfect trusted devices is not absorbed into this ideal statement and is accounted for by Δ_{side} . For tagged events, including multipair emissions and vacuum mis-admissions, the proof assigns Eve the full four-bit information content. Hence

$$I(M; E) \leq 4Q_{\text{tag}}^U + \Delta_{\text{side}} + \Delta_{\text{fin}}. \quad (42)$$

The total failure probability is allocated as

$$\varepsilon_{\text{sec}} = \varepsilon_{\text{LP}} + \varepsilon_{\text{test}} + \varepsilon_{\text{sm}} + \varepsilon_{\text{cor}} + \varepsilon_{\text{side}}, \quad (43)$$

where $\varepsilon_{\text{LP}} = \sum_{x,y} (\varepsilon_{Q,xy} + \varepsilon_{T,xy})$ is used by the confidence intervals in Eq. (26), $\varepsilon_{\text{test}}$ by the hidden-test sampling bound, ε_{sm} and ε_{cor} by the smooth-entropy secrecy and correctness terms, and $\varepsilon_{\text{side}}$ by any separately calibrated side-channel leakage model.

It remains to make Δ_{fin} explicit. Let $N_{\text{tot}} = \sum_{x,y} N_{xy}$ be the total number of pump slots used for normalization and define the finite accepted block lengths

$$n_{\text{msg},11}^L = N_{\text{tot}} Q_{\text{msg},11}^L, \quad n_{\text{tag}}^U = N_{\text{tot}} Q_{\text{tag}}^U. \quad (44)$$

In the second round, suppose that N_{test} accepted slots are opened as hidden tests and N_{msg} accepted slots remain for message recovery. Let $\hat{e}_{\text{test}}$ denote the observed hidden-test error rate. Since the hidden tests are sampled without replacement from the accepted candidate set, a conservative Serfling-type bound gives, except with probability $\varepsilon_{\text{test}}$,

$$e_{\text{msg}}^U = \min \left[1, \hat{e}_{\text{test}} + \sqrt{\frac{(N_{\text{test}} + N_{\text{msg}})(N_{\text{test}} + 1)}{2N_{\text{test}}^2 N_{\text{msg}}}} \ln \frac{1}{\varepsilon_{\text{test}}} \right]. \quad (45)$$

The finite-block penalty used in Eq. (42) is written in a smooth-min-entropy form. Following the standard leftover-hashing treatment against quantum side information

[33, 47–49], the finite confidential message length obeys

$$\begin{aligned} \ell_{\text{sec}}^L \geq & 4n_{\text{msg},11}^L - n_{\text{msg},11}^L H_{16}(e_{\text{msg}}^U) - 4n_{\text{tag}}^U \\ & - 6 \log_2 \frac{21}{\varepsilon_{\text{sm}}} - \log_2 \frac{2}{\varepsilon_{\text{cor}}} - N_{\text{tot}} \Delta_{\text{side}}. \end{aligned} \quad (46)$$

Dividing Eq. (46) by N_{tot} gives the explicit finite-size penalty

$$\begin{aligned} \Delta_{\text{fin}} = & Q_{\text{msg},11}^L [H_{16}(e_{\text{msg}}^U) - H_{16}(e_{11}^U)]_+ \\ & + \frac{1}{N_{\text{tot}}} \left[6 \log_2 \frac{21}{\varepsilon_{\text{sm}}} + \log_2 \frac{2}{\varepsilon_{\text{cor}}} \right], \end{aligned} \quad (47)$$

where $H_{16}(e) = h_2(e) + e \log_2 15$. The first term is the additional 16-ary entropy cost caused by finite hidden-test sampling. The second term is the explicit smooth-min-entropy secrecy and correctness overhead. The LP fluctuation itself is not added again in Δ_{fin} , because it has already entered the finite-data bounds Y_{11}^L and e_{11}^U through Eq. (26). Therefore the dependence of the finite-size penalty on the total number of pump slots N_{tot} , the hidden-test sample size, and the failure allocation ε_{sec} is explicit rather than symbolic. In the asymptotic simulations, $N_{\text{tot}} \rightarrow \infty$, $e_{\text{msg}}^U \rightarrow e_{11}^U$, and Δ_{fin} is set to zero.

Substituting Eqs. (41) and (42) into Eq. (38) gives the conservative secure message capacity lower bound

$$C_{\text{sec}}^L = [Q_{\text{msg},11}^L (4 - H_{16}(e_{11}^U)) - 4Q_{\text{tag}}^U - \Delta_{\text{fin}} - \Delta_{\text{side}}]_+. \quad (48)$$

The first term in Eq. (48) is therefore the legal mutual information certified by the decoy-state single-pair sector. The second term is not a fitted loss term, but the worst-case Holevo information assigned to all uncertified tagged events. In the asymptotic simulations, Δ_{fin} and Δ_{side} are set to zero, giving

$$C_{\text{sec,asy}}^L = [Q_{\text{msg},11}^L (4 - H_{16}(e_{11}^U)) - 4Q_{\text{tag}}^U]_+. \quad (49)$$

A positive value of C_{sec}^L means that the protocol has positive secure direct-communication capability under the stated physical model and trusted-station assumptions.

5 Numerical Simulation and Performance Comparison

This section presents numerical simulations for the proposed decoy-state hyperentangled MDI-QSDC protocol. The signal intensity is optimized at each channel attenuation to maximize the secure message capacity. The numerical comparison is organized in three parts. Section 5.1 compares the secure message capacity with representative decoy-state QSDC protocols. Section 5.2 compares the protocol resources with representative

MDI-QSDC protocols. Section 5.3 identifies the source and hardware conditions that give the highest secure message capacity in the proposed architecture.

The optical-loss, dark-count, detector-error and detector-efficiency values used below are adopted from the free-space QSDC experiment reported by Pan et al. [50]. The notation is adapted to the present dual-source model.

Table 1 Parameters used in the numerical simulation. The experimental parameter values are adopted from Pan et al. [50].

Parameter	Value
η_{BA}	0.21
η_{BAB}	0.088
P_d	8.0×10^{-8}
e_d^A	0.0131
e_d^B	0.0026
$\eta_{H(V)}$	0.70

5.1 Secure message capacity comparison with decoy-state QSDC protocols

Figure 4 compares the proposed protocol with three representative decoy-state QSDC schemes under the same channel-attenuation axis. The blue dashed curve denotes the practical active decoy-state QSDC model of Liu et al. [17], the green dashed curve denotes the heralded-source decoy-state QSDC model of Ying et al. [19], and the black dotted curve denotes the passive decoy-state QSDC trend of Ying et al. [20]. The horizontal axis is the channel attenuation in dB, and the vertical axis is the secure message capacity C_s in bit/pulse on a logarithmic scale.

The red curve remains above the three decoy-state QSDC references throughout the simulated attenuation range. Under the conclusive-event comparison used in Fig. 4, the secure message capacity improvement is about fourfold, corresponding to an approximate 300% increase over the best single-degree-of-freedom decoy-state baseline at the same attenuation. This gain comes from the 16-state polarization-spatial hyperentangled Bell alphabet: a conclusive single-degree-of-freedom event carries one message bit, whereas a conclusive hyperentangled Bell event carries four bits. The additional hardware factors of the full MDI implementation, especially HBSA success probability and quantum-memory efficiency, are evaluated separately in Section 5.3.

5.2 Comparison with representative MDI-QSDC protocols

The efficiency comparison in this subsection is a protocol-resource comparison, not the secure message capacity C_{sec}^L derived in Section 4. To avoid mixing concepts, we use

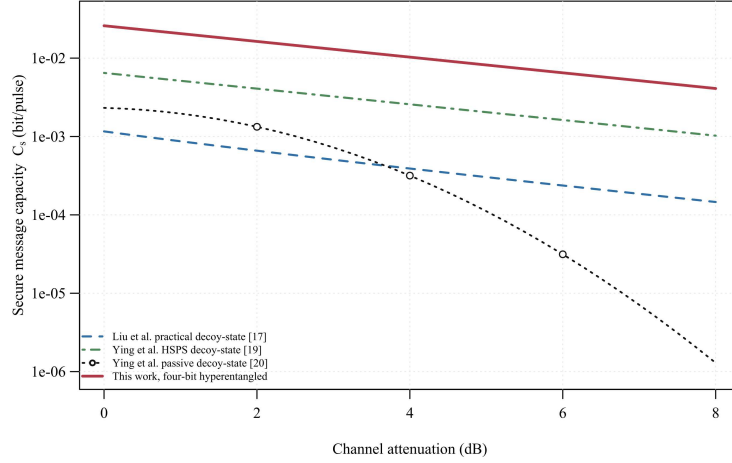


Fig. 4 Secure message capacity comparison with representative decoy-state QSDC protocols. The

Fig. 4 Secure message capacity comparison with representative decoy-state QSDC protocols. The blue dashed, green dashed and black dotted curves denote practical active decoy-state QSDC [17], heralded-source decoy-state QSDC [19] and passive decoy-state QSDC [20], respectively. The open black circles are the passive-decoy values reported in Ref. [20]. The red curve is the proposed four-bit hyperentangled conclusive-event information content under the same conclusive-event comparison basis.

three separate quantities. First, the logical payload per conclusive label is

$$b_{\log} = \log_2 |\Omega_{\text{msg}}|, \quad (50)$$

where Ω_{msg} is the message alphabet carried by one conclusive Bell-label event. This value is 4 bit for the polarization-spatial hyperentangled alphabet used here. Second, the BSM/HBSA success entry denotes the intrinsic Bell-analyser success probability for a valid input under the cited honest-device model. For the proposed protocol this quantity is treated as the simulation parameter p_{HBSA} in Eq. (13), not as an experimentally demonstrated fixed value and not as a product including source emission, channel loss, detector efficiency or memory efficiency. Third, the resource efficiency follows the common QSDC counting rule

$$\eta_{\text{res}} = \frac{B_{\text{msg}}}{Q_q + B_{\text{cl}}}, \quad (51)$$

where B_{msg} is the number of useful message bits, Q_q is the number of quantum carriers consumed and B_{cl} is the amount of classical information that the corresponding reference counts as necessary for decoding. If a cited efficiency is reported after an analyser-success probability p_M , Eq. (51) is equivalently written per attempted block as

$$\eta_{\text{res}}^{\text{eff}} = \frac{b_{\log} p_M}{q_q + b_{\text{cl}} p_M}, \quad (52)$$

with q_q and b_{cl} fixed by that reference’s resource-counting convention. Thus a resource-efficiency number is not a substitute for the bit/pulse secure-capacity bound in Eq. (48). In this paper, the decoy-state layer changes the certified accepted fraction through Y_{11}^L , e_{11}^U and tagged-event subtraction; it does not change the four-bit logical payload of a conclusive hyperentangled HBSA event.

Table 2 Protocol-resource comparison of representative MDI-QSDC protocols. The payload column is the logical message content per conclusive Bell-label event, whereas the resource-efficiency column follows the counting convention reported in the cited protocols and should not be confused with C_{sec}^L in bit/pulse.

Protocol	Payload	BSM/HBSA success	Resource efficiency	Key features
Zhou et al. MDI-QSDC [34]	2	$\sim 50\%$	$\sim 25\%$	Basic MDI-QSDC
Ying et al. MDI-QSDC [51]	2	$\sim 50\%$	$\sim 30\%$	One-step MDI-QSDC
Das et al. MDI-QSDC [52]	2	$\sim 50\%$	$\sim 33\%$	With authentication
Liu et al. MDI-QSDC [53]	4	$\sim 50\text{--}60\%$	$\sim 40\%$	High-dimensional
This work	4	65%	33.3%	Hyperentanglement + decoy-state

Table 2 gives a compact protocol-level comparison under the definitions above. For the proposed protocol, $|\Omega_{\text{msg}}| = 16$ gives a payload of 4 bit per conclusive HBSA label. To place the last row on the same numerical basis as the preceding schemes, the HBSA-success entry uses the baseline simulation setting $p_{\text{HBSA}} = 0.65$, namely 65%. Under Eq. (51), a four-bit message block uses four quantum carriers (A_1 , A_2 , B_1 and B_2), while the two four-bit HBSA announcements contribute eight classical bits. Hence $\eta_{\text{res}} = 4/(4 + 8) = 33.3\%$. These are the protocol-comparison values reported in Table 2. The end-to-end secure message capacity remains determined by Eq. (48), which additionally includes the decoy-certified single-pair gain, tagged-event subtraction, channel loss, detector efficiency and memory efficiency.

5.3 Source and hardware optimization

The signal mean photon-pair number μ_s controls the balance between the certified dual single-pair contribution and the tagged-event subtraction. If μ_s is too small, useful dual single-pair events are rare. If it is too large, multipair tagged events dominate the leakage term.

At $A = 6$ dB with the baseline settings $\eta_d = 0.70$, $p_{\text{HBSA}} = 0.65$ and $\eta_m = 0.85$, the optimized source brightness is $\mu_s^* = 0.0855$ and the simulated capacity is 1.96×10^{-5} bit/pulse. The optimum remains below the high-brightness regime because multipair emissions are counted as tagged events in the security bound.

Figure 6 scans the hardware parameters that are specific to the proposed hyper-entangled MDI architecture. The HBSA success probability p_{HBSA} controls the intrinsic

conclusiveness of the HBSA module for a valid hyperentangled two-photon input. It is scanned independently from the detector efficiency η_d , because η_d is not included in the definition of p_{HBSA} in Eq. (13). The memory efficiency η_m determines how much of the stored-photon part of the four-bit conclusive-event information content survives the two-round implementation.

Within the scanned range, the highest secure message capacity occurs when the detector efficiency, HBSA success probability and storage efficiency are all improved. For $\eta_d = 0.80$, $p_{\text{HBSA}} = 0.85$ and $\eta_m = 1.00$, the re-optimized brightness is $\mu_s^* = 0.0955$ and the secure message capacity reaches 9.34×10^{-5} bit/pulse at 6 dB. This is about 4.76 times the baseline value. This upper scan point is a sensitivity benchmark rather than a claim that the present optical implementation already realizes such a complete-HBSA performance. The result identifies the most direct route to a higher secure message capacity: improve HBSA conclusiveness, reduce detector loss and preserve the stored idler photons.

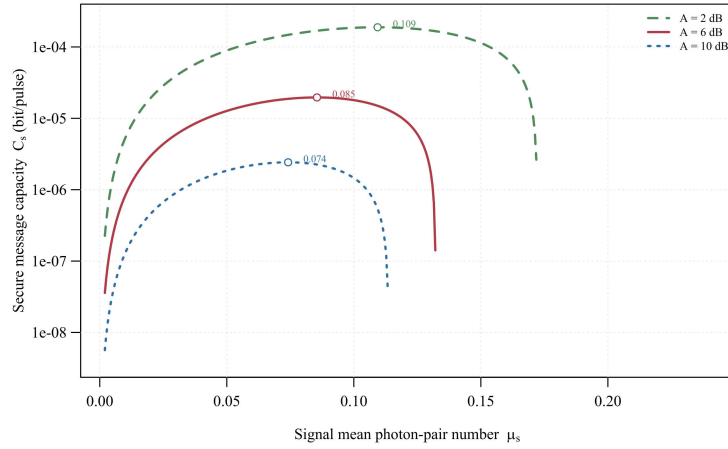


Fig. 5 Secure message capacity as a function of the signal mean photon-pair number μ_s . Markers indicate the pointwise optimum μ_s^* . The same symbol μ_s is used in the source model, protocol and simulation.

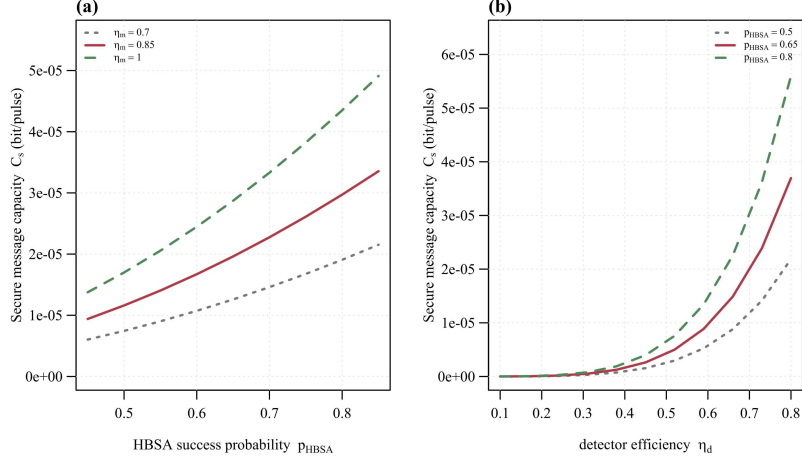


Fig. 6 Hardware robustness scan at $A = 6$ dB. (a) Secure message capacity versus HBSA success probability p_{HBSA} for different quantum-memory efficiencies. (b) Secure message capacity versus detector efficiency η_d for different HBSA success probabilities. The signal intensity μ_s is re-optimized at every point.

5.4 Numerical conclusion

The numerical results lead to two conclusions. First, relative to decoy-state QSDC protocols with a single-degree-of-freedom conclusive-event information content, the proposed hyperentangled Bell alphabet gives a fourfold secure message capacity gain under the same conclusive-event comparison basis. Second, the practical secure message capacity is controlled by HBSA success probability, detector efficiency, memory efficiency and the optimized SPDC brightness. Improving these quantities converts the four-bit conclusive-event advantage into a higher end-to-end secure message capacity.

6 Conclusion

We have proposed a decoy-state polarization-spatial hyperentangled MDI-QSDC protocol with independent state preparation. Alice and Bob each prepare active three-intensity SPDC hyperentangled photon pairs and send their signal photons to an untrusted Charlie for the first HBSA. After the security test, Alice encodes a four-bit message on her retained photon, Bob applies a private four-bit Pauli mask, and both users send the encoded photons to Charlie for the second HBSA. Decoy-state statistics estimate the dual single-pair contribution, while tagged-event subtraction handles vacuum and multipair risks. Bob's private mask makes Charlie's public labels statistically independent of Alice's plaintext.

The protocol has a clear cost. A strict dual-source MDI layout introduces the probability penalty of two independent SPDC sources and two HBSA rounds. It also requires stable quantum memories, matched modes and a high-quality HBSA module.

The benefit is a transparent security boundary: detectors and measurement optics are removed from the trusted part of the system, while the conclusive-event information content remains 4 bit. The framework therefore provides theoretical support for the practical design and performance evaluation of high-security, high-capacity MDI-QSDC systems with non-ideal SPDC sources.

Declarations

Funding. This work is supported by the National Natural Science Foundation of China under Grant No. 62572292.

Competing interests. The authors declare no competing interests.

Author contributions. H.Z. proposed the initial idea, performed the theoretical analysis and carried out the numerical calculations. R.-G.Z. designed and refined the protocol model, supervised the security analysis, and reviewed and revised the manuscript. Both authors discussed the results and contributed to the final manuscript.

Data availability. This work is theoretical and does not involve experimental data. The numerical data supporting the figures can be reproduced from the model in Section 4 and the parameter settings in Table 1. The numerical code is available from the corresponding author upon reasonable request.

References

- [1] Long, G.-L., Liu, X.-S.: Theoretically efficient high-capacity quantum-key-distribution scheme. *Phys. Rev. A* **65**, 032302 (2002) <https://doi.org/10.1103/PhysRevA.65.032302>
- [2] Boström, K., Felbinger, T.: Deterministic secure direct communication using entanglement. *Phys. Rev. Lett.* **89**, 187902 (2002) <https://doi.org/10.1103/PhysRevLett.89.187902>
- [3] Deng, F.-G., Long, G.-L., Liu, X.-S.: A two-step quantum direct communication protocol using the Einstein–Podolsky–Rosen pair block. *Phys. Rev. A* **68**, 042317 (2003) <https://doi.org/10.1103/PhysRevA.68.042317>
- [4] Deng, F.-G., Long, G.-L.: Secure direct communication with a quantum one-time pad. *Phys. Rev. A* **69**, 052319 (2004) <https://doi.org/10.1103/PhysRevA.69.052319>
- [5] Lucamarini, M., Mancini, S.: Secure deterministic communication without entanglement. *Phys. Rev. Lett.* **94**, 140501 (2005) <https://doi.org/10.1103/PhysRevLett.94.140501>
- [6] Hu, J., Yu, B., Jing, M., *et al.*: Experimental quantum secure direct communication with single photons. *Light Sci. Appl.* **5**, 16144 (2016) <https://doi.org/10.1038/lsa.2016.144>

- [7] Qi, R., Sun, Z., Lin, Z., *et al.*: Implementation and security analysis of practical quantum secure direct communication. *Light Sci. Appl.* **8**, 22 (2019) <https://doi.org/10.1038/s41377-019-0132-3>
- [8] Zhang, H., Sun, Z., Qi, R., Yin, L., Long, G.-L., Lu, J.: Realization of quantum secure direct communication over 100 km fiber with time-bin and phase quantum states. *Light Sci. Appl.* **11**, 83 (2022) <https://doi.org/10.1038/s41377-022-00769-w>
- [9] Qi, Z., Li, Y., Huang, Y.-W., *et al.*: A 15-user quantum secure direct communication network. *Light Sci. Appl.* **10**, 183 (2021) <https://doi.org/10.1038/s41377-021-00634-2>
- [10] Pan, D., Long, G.-L., Yin, L.-G., *et al.*: The evolution of quantum secure direct communication: On the road to the Qinternet. *IEEE Commun. Surv. Tutor.* **26**, 1898–1949 (2024)
- [11] Hwang, W.-Y.: Quantum key distribution with high loss: toward global secure communication. *Phys. Rev. Lett.* **91**, 057901 (2003) <https://doi.org/10.1103/PhysRevLett.91.057901>
- [12] Lo, H.-K., Ma, X., Chen, K.: Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005) <https://doi.org/10.1103/PhysRevLett.94.230504>
- [13] Wang, X.-B.: Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94**, 230503 (2005) <https://doi.org/10.1103/PhysRevLett.94.230503>
- [14] Ma, X., Qi, B., Zhao, Y., Lo, H.-K.: Practical decoy state for quantum key distribution. *Phys. Rev. A* **72**, 012326 (2005) <https://doi.org/10.1103/PhysRevA.72.012326>
- [15] Gottesman, D., Lo, H.-K., Lütkenhaus, N., Preskill, J.: Security of quantum key distribution with imperfect devices. *Quantum Inf. Comput.* **4**, 325–360 (2004)
- [16] Ma, X., Fung, C.-H.F., Lo, H.-K.: Quantum key distribution with entangled photon sources. *Phys. Rev. A* **76**, 012307 (2007) <https://doi.org/10.1103/PhysRevA.76.012307>
- [17] Liu, X., Li, Z.-J., Luo, D., *et al.*: Practical decoy-state quantum secure direct communication. *Sci. China Phys. Mech. Astron.* **64**, 120311 (2021) <https://doi.org/10.1007/s11433-021-1775-4>
- [18] Park, J., Kim, B., Heo, J.: Statistical fluctuation analysis for decoy-state quantum secure direct communication. *Quantum Inf. Process.* **22**, 112 (2023) <https://doi.org/10.1007/s11128-023-03845-1>
- [19] Ying, J.-W., Zhao, P., Zhong, W., *et al.*: Passive decoy-state quantum secure

- direct communication with a heralded single-photon source. *Phys. Rev. Applied* **22**, 024040 (2024) <https://doi.org/10.1103/PhysRevApplied.22.024040>
- [20] Ying, J.-W., Wang, J.-Y., Xiao, Y.-X., *et al.*: Passive decoy-state quantum secure direct communication. *Fundam. Res* (2026) <https://doi.org/10.1016/j.fmre.2025.12.008>
 - [21] Barreiro, J.T., Langford, N.K., Peters, N.A., Kwiat, P.G.: Generation of hyper-entangled photon pairs. *Phys. Rev. Lett.* **95**, 260501 (2005) <https://doi.org/10.1103/PhysRevLett.95.260501>
 - [22] Kwiat, P.G., Mattle, K., Weinfurter, H., Zeilinger, A., Sergienko, A.V., Shih, Y.: New high-intensity source of polarization-entangled photon pairs. *Phys. Rev. Lett.* **75**, 4337–4341 (1995) <https://doi.org/10.1103/PhysRevLett.75.4337>
 - [23] Kwiat, P.G., Waks, E., White, A.G., Appelbaum, I., Eberhard, P.H.: Ultrabright source of polarization-entangled photons. *Phys. Rev. A* **60**, 773–776 (1999) <https://doi.org/10.1103/PhysRevA.60.R773>
 - [24] Sheng, Y.-B., Deng, F.-G., Long, G.-L.: Complete hyperentangled-Bell-state analysis for quantum communication. *Phys. Rev. A* **82**, 032318 (2010) <https://doi.org/10.1103/PhysRevA.82.032318>
 - [25] Wang, T.-J., Wang, C.: Complete hyperentangled Bell-state analysis for photonic qubits assisted by a three-level Λ system. *Sci. Rep.* **6**, 19497 (2016) <https://doi.org/10.1038/srep19497>
 - [26] Walborn, S.P., Pádua, S., Monken, C.H.: Hyperentanglement-assisted Bell-state analysis. *Phys. Rev. A* **68**, 042313 (2003) <https://doi.org/10.1103/PhysRevA.68.042313>
 - [27] Wang, T.-J., Li, T., Du, F.-F., Deng, F.-G.: High-capacity quantum secure direct communication based on quantum hyperdense coding with hyperentanglement. *Chin. Phys. Lett.* **28**, 040305 (2011) <https://doi.org/10.1088/0256-307X/28/4/040305>
 - [28] Bennett, C.H., Wiesner, S.J.: Communication via one- and two-particle operators on Einstein–Podolsky–Rosen states. *Phys. Rev. Lett.* **69**, 2881–2884 (1992) <https://doi.org/10.1103/PhysRevLett.69.2881>
 - [29] Cozzolino, D., Da Lio, B., Bacco, D., Oxenløwe, L.K.: High-dimensional quantum communication: benefits, progress, and future challenges. *Quantum Technol.* **2**, 1900038 (2019) <https://doi.org/10.1002/qute.201900038>
 - [30] Zhao, Y., Fung, C.-H.F., Qi, B., Chen, C., Lo, H.-K.: Quantum hacking: experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A* **78**, 042333 (2008) <https://doi.org/10.1103/PhysRevA.78.042333>

- [31] Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J., Makarov, V.: Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photonics* **4**, 686–689 (2010) <https://doi.org/10.1038/nphoton.2010.214>
- [32] Lo, H.-K., Curty, M., Qi, B.: Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012) <https://doi.org/10.1103/PhysRevLett.108.130503>
- [33] Curty, M., Xu, F., Cui, W., Lim, C.C.W., Tamaki, K., Lo, H.-K.: Finite-key analysis for measurement-device-independent quantum key distribution. *Nat. Commun.* **5**, 3732 (2014) <https://doi.org/10.1038/ncomms4732>
- [34] Zhou, Z.-R., Sheng, Y.-B., Niu, P.-H., Yin, L.-G., Long, G.-L., Hanzo, L.: Measurement-device-independent quantum secure direct communication. *Sci. China Phys. Mech. Astron.* **63**, 230362 (2020) <https://doi.org/10.1007/s11433-019-1450-8>
- [35] Wu, X., Zhou, L., Zhong, W., Sheng, Y.-B.: High-capacity measurement-device-independent quantum secure direct communication. *Quantum Inf. Process.* **19**, 354 (2020) <https://doi.org/10.1007/s11128-020-02864-6>
- [36] Li, X.-J., Wang, M., Pan, X.-B., Zhang, Y.-R., Long, G.-L.: One-photon-interference quantum secure direct communication. *Entropy* **26**, 811 (2024) <https://doi.org/10.3390/e26090811>
- [37] Lei, Y.-T., Li, X.-J., Pan, X.-B., Zhang, Y.-R., Long, G.-L.: High-dimensional and multi-intensity one-photon-interference quantum secure direct communication. *Entropy* **27**, 332 (2025) <https://doi.org/10.3390/e27040332>
- [38] Song, D.-B., Zhou, R.-G., Du, L.-T.: Measurement-device-independent quantum secure direct communication using polarization–spatial hyperentanglement and PRF encoding. *Quantum Inf. Process.* **25**, 143 (2026) <https://doi.org/10.1007/s11128-026-05153-w>
- [39] Long, G.-L., Zhang, H.: Drastic increase of channel capacity in quantum secure direct communication using masking. *Sci. Bull.* **66**, 1267–1269 (2021) <https://doi.org/10.1016/j.scib.2021.04.016>
- [40] Wu, J., Long, G.-L., Hayashi, M.: Quantum secure direct communication with private dense coding using a general preshared quantum state. *Phys. Rev. Applied* **17**, 064011 (2022) <https://doi.org/10.1103/PhysRevApplied.17.064011>
- [41] Lim, C.C.W., Curty, M., Walenta, N., Xu, F., Zbinden, H.: Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A* **89**, 022307 (2014) <https://doi.org/10.1103/PhysRevA.89.022307>

- [42] Hoeffding, W.: Probability inequalities for sums of bounded random variables. *J. Am. Stat. Assoc.* **58**, 13–30 (1963) <https://doi.org/10.1080/01621459.1963.10500830>
- [43] Chernoff, H.: A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. *Ann. Math. Stat.* **23**, 493–507 (1952) <https://doi.org/10.1214/aoms/1177729330>
- [44] Wyner, A.D.: The wire-tap channel. *Bell Syst. Tech. J.* **54**, 1355–1387 (1975) <https://doi.org/10.1002/j.1538-7305.1975.tb02040.x>
- [45] Csiszár, I., Körner, J.: Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory* **24**, 339–348 (1978) <https://doi.org/10.1109/TIT.1978.1055892>
- [46] Wu, J., Lin, Z., Yin, L., Long, G.-L.: Security of quantum secure direct communication based on Wyner’s wiretap channel theory. *Quantum Eng.* **1**, 26 (2019) <https://doi.org/10.1002/que2.26>
- [47] Tomamichel, M., Lim, C.C.W., Gisin, N., Renner, R.: Tight finite-key analysis for quantum cryptography. *Nat. Commun.* **3**, 634 (2012) <https://doi.org/10.1038/ncomms1631>
- [48] Tomamichel, M., Colbeck, R., Renner, R.: A fully quantum asymptotic equipartition property. *IEEE Trans. Inf. Theory* **55**, 5840–5847 (2009) <https://doi.org/10.1109/TIT.2009.2032797>
- [49] Tomamichel, M., Schaffner, C., Smith, A., Renner, R.: Leftover hashing against quantum side information. *IEEE Trans. Inf. Theory* **57**, 5524–5535 (2011) <https://doi.org/10.1109/TIT.2011.2158473>
- [50] Pan, D., Lin, Z.-S., Wu, J.-W., Zhang, H.-R., Sun, Z., Ruan, D., Yin, L.-G., Long, G.-L.: Experimental free-space quantum secure direct communication and its security analysis. *Photon. Res.* **8**(9), 1522–1531 (2020) <https://doi.org/10.1364/PRJ.388790>
- [51] Ying, J.-W., Zhou, L., Zhong, W., Sheng, Y.-B.: Measurement-device-independent one-step quantum secure direct communication. *Chin. Phys. B* **31**, 120303 (2022) <https://doi.org/10.1088/1674-1056/ac8f37>
- [52] Das, N., Paul, G.: Measurement-device-independent quantum secure direct communication with user authentication. *Quantum Inf. Process.* **21**, 260 (2022) <https://doi.org/10.1007/s11128-022-03572-z>
- [53] Liu, L., Niu, J.-L., Fan, C.-R., Feng, X.-T., Wang, C.: High-dimensional measurement-device-independent quantum secure direct communication. *Quantum Inf. Process.* **19**, 404 (2020) <https://doi.org/10.1007/s11128-020-02908-x>