Differential phase encoded measurement-device-independent quantum key distribution

Shashank Kumar Ranu[1,2] · **Anil Prabhakar**[1] · **Prabha Mandayam**[2]

Abstract

We present a measurement-device-independent quantum key distribution (MDI-QKD) using single photons in a linear superposition of three orthogonal *time-bin* states, for generating the key. The orthogonal states correspond to three distinct paths in the delay line interferometers used by two (trusted) sources. The key information is decoded based on the measurement outcomes obtained by an untrusted third party Charles, who uses a beamsplitter to measure the phase difference between pulses traveling through different paths of the two delay lines. The proposed scheme combines the best of both differential-phase-shift (DPS) QKD and MDI-QKD. It is more robust against phase fluctuations, and also ensures protection against detector side-channel attacks. We prove unconditional security by demonstrating an equivalent protocol involving shared entanglement between the two trusted parties. We show that the secure key rate for our protocol compares well to existing protocols in the asymptotic regime. For the decoy-state variant of our protocol, we evaluate the secure key rate by using a phase-post-selection technique. Finally, we estimate the bit error rate and the phase error rate, in the finite key regime.

Keywords MDI-QKD · DPS-QKD · Finite-key

1 Introduction

Quantum key distribution (QKD) is proven to be unconditionally secure in theory [1–5]. However, QKD protocols may be rendered insecure in practice, because of the difference in the behavior of practical devices and the respective theoretical mod-

---

✉ Shashank Kumar Ranu
ee16s300@ee.iitm.ac.in

[1] Department of Electrical Engineering, Indian Institute of Technology Madras, Chennai, India

[2] Department of Physics, Indian Institute of Technology Madras, Chennai, India

els used in security proofs. For example, the standard protocols and their security proofs fail to take into account side-channel attacks on the detectors [6–15], thereby compromising security.

Various solutions have been proposed to counteract side-channel attacks. One solution is to develop precise mathematical models of devices used in the QKD experiments and incorporate these models into new security proofs [16–18]. However, the complex nature of devices makes this approach very challenging to realize in practice. The other solution is to develop counter measures against known side-channel attacks [19,20], but the QKD system still remains vulnerable to unanticipated attacks. Device independent QKD (DI-QKD) [21,22] is another viable candidate against side-channel attacks. The security of DI-QKD relies on the violations of Bell inequality. However, the requirement of a loophole-free Bell test, and an extremely low key rate at long distances, makes this unfeasible with current technology [23,24]. Measurement-device-independent QKD (MDI-QKD) [25,26] was introduced as a practical solution to side-channel attacks on the measurement unit.

In an MDI-QKD protocol, Alice and Bob encode their respective classical key bits into quantum states and send it to a potentially untrusted party, Charles. It is assumed that the measurement unit is under complete control of Charles, who carries out the measurement and announces the results. This is followed by sifting, error correction and privacy amplification, as carried out in standard QKD protocols. The first MDI-QKD scheme was designed for a polarization-based implementation of BB84 [25]. Various variants of the original polarization-based MDI protocol exist in the literature [27–29]. MDI protocols employing time-bin [30,31] and phase-based encodings [32–36] also exist in the literature—see [37] for a recent review. However, random phase and polarization fluctuations are a major hindrance in long distance implementations of polarization and phase-based MDI-QKD schemes.

Here, we propose a differential-phase-shifted MDI-QKD (DPS MDI-QKD) scheme, as a potential candidate for alleviating random phase fluctuations. Random polarization fluctuations that occur over milli-second timescales do not affect such a differential phase-based protocol. In a differential phase-encoded QKD protocol, the classical key is encoded in the phase difference between successive optical pulses which are a few nano-seconds apart, thus making the protocol resilient to the effects of environmental phase fluctuations. There are a few variants of differential-phase-shifted keying proposed in the literature [38]. For example, the sender Alice could use a phase modulator in combination with a random number generator to apply a phase of either 0 or π, randomly, on a sequence of successive pulses generated by a weak coherent source (WCS) [39]. Alternately, the phase modulation may be done on a single photon pulse converted into a superposition of three orthogonal states corresponding to three different time-bins, via a delay line interferometer [40].

Here, we make use of the 3-pulse protocol, whose security is based on the fact that the eavesdropper has to distinguish between a set of four non-orthogonal quantum states. While the coherent-state DPS protocol is provably secure against individual attacks [41], the single-photon based 3-pulse protocol is shown to be unconditionally secure [42]. However, this security proof assumes infinitely long keys, whereas experimental implementations are constrained by the finite computational power of Alice and Bob, resulting in keys of finite length.
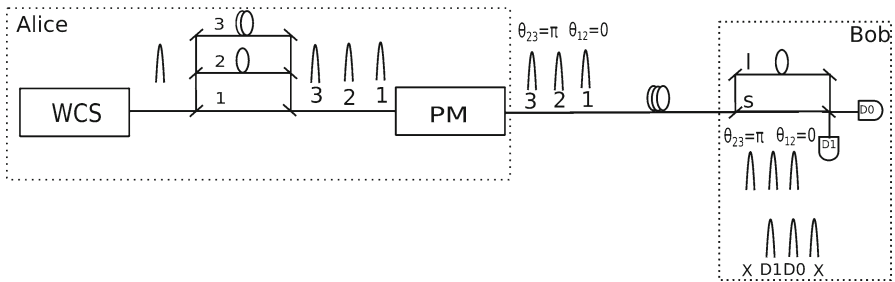
Fig. 1 Schematic of 3-pulse differential-phase-shift QKD. WCS = Weak Coherent Source, PM = Phase Modulator, $D0$, $D1$ = Single-photon Detectors

Effect of the finiteness of the key size on security parameters was first studied in [43]. Subsequently, the security of BB84 [44] and decoy state protocols [45–47] against collective attacks in the finite-key regime was established. Techniques used for the finite-key analysis of conventional QKD have also been applied to MDI-QKD, but for specific attacks [48]. More recently, a rigorous security proof of MDI-QKD against general attacks for a finite key length was demonstrated [49].

In this paper, we present a MDI-QKD scheme which incorporates the advantages of differential phase encoding. We show unconditional security of our protocol by mapping it to an equivalent entanglement-based protocol. An upper bound for the phase error rate of our scheme, in terms of the bit error rate, is then used to carry out the asymptotic and finite-key analysis of our scheme. We demonstrate that our protocol generates secure keys over reasonable distances, even under system imperfections. We also propose a decoy-state variant of our protocol and use phase-post-selection technique to show that our scheme offers reasonable security, thereby making it an attractive choice for practical implementations that use a weak coherent source (WCS).

In Sect. 2, we briefly review the 3-pulse DPS-QKD protocol and its security aspects. We discuss our DPS-MDI protocol in Sect. 3 and show that it maps to an entanglement-based protocol. We obtain the secure key rate using an ideal single-photon source as well as a WCS for the protocol. Finally, we present the finite-key analysis of our scheme in Sect. 4. The details of the calculation of the secure key rates for our scheme, and the mapping of our protocol to an equivalent entanglement-based protocol are presented in "Appendix A and B", respectively. We explicitly calculate the phase error rate for our protocol in terms of the bit error rate in "Appendix C", and finally, calculate the parameters involved in the asymptotic key analysis in "Appendix D".

2 Preliminaries

Starting with the original proposal to implement the B92 protocol [50], differential phase or distributed-phase protocols have been well-studied in the QKD literature [38]. Such protocols are popular because they are relatively easy to implement (compared to polarization-based protocols) and are robust against phase fluctuations. Most phase-based schemes use weak coherent pulses for encoding the key. However, in this paper,

we use the single-photon scheme proposed in [40]. We shall henceforth refer to this scheme as the 3-pulse DPS-QKD protocol and provide a brief description below.

2.1 3-pulse differential-phase-shift keying

In a 3-pulse DPS-QKD protocol, the sender (Alice) throws a single photon into a superposition of three time-bins, corresponding to the three distinct paths of a delay line interferometer, and then uses a phase modulator to introduce a relative phase between successive time-bins, as shown schematically in Fig. 1. Alice encodes her random key bit {0, 1} as a random phase {0, π} between successive pulses. The receiver (Bob) thus gets one of the four non-orthogonal quantum states given below, corresponding to the four possible phase-differences, i.e.,

$$|\psi(\pm, \pm)\rangle = \frac{1}{\sqrt{3}} \left(|100\rangle_a \pm |010\rangle_a \pm |001\rangle_a \right). \tag{1}$$

Here, $|100\rangle_a$, $|010\rangle_a$ or $|001\rangle_a$ indicate that the photon travelled with equal probability via paths 1, 2 or 3, respectively, in Alice's set-up.

Bob's decoding setup comprises of a delay line interferometer (DLI) and two single-photon detectors. The path lengths are chosen such that the longer arm of Bob's DLI introduces a time delay Δt which is exactly equal to the difference in time taken by the photon to traverse two successive arms of Alice's 3-path delay line. Thus, Bob can detect the incoming photon in one of the four possible time-bins, which we label as t_1, t_2, t_3, t_4, each separated from its previous bin by a time of Δt. Detections at times t_1 and t_4 do not provide any phase information, whereas detections at times t_2 and t_3 provide information about the relative phases θ_{12} and θ_{23} respectively (see Fig. 1). Specifically, Bob decodes the key bit associated with a given time-slot as a 0, or 1, if detector $D0$, or $D1$, clicks. By publicly announcing his detection times, Bob performs key-reconciliation with Alice and it is easy to see that the sifted key rate for this 3-pulse protocol is 1/2.

An alternate form of phase-encoded QKD is the pulse-train DPS-QKD [39], which is a variant of the original B92 protocol [50]. In the pulse-train protocol, Alice generates a train of coherent pulses and applies a phase of 0 or π to the pulses randomly, to encode the key bits 0 or 1, respectively. These phase modulated pulse trains are sent to Bob, who passes the incoming pulses through a DLI. Depending upon the phase difference between two successive pulses, constructive or destructive interference happens. An MDI-QKD protocol based on the coherent-state pulse-train DPS protocol was also proposed in [33].

We refer to [51] for a detailed analysis of the secure key rate for the 3-pulse DPS protocol, assuming individual attacks. A simple comparison with the pulse-train DPS protocol [52] shows that the 3-pulse variant offers better security against individual attacks, in the following sense: an eavesdropper introduces a higher error rate and also has a lower learning rate in the 3-pulse protocol [51].

Finally, we note that the 3-pulse DPS-QKD protocol can be extended to an n-pulse protocol by increasing the number of possible paths that the single photon can take

at the sender's set-up. In fact, the single-photon DPS protocol using n such paths has been shown to be unconditionally secure against general attacks for any $n \geq 3$ [42]. Experimental realization of n path DPS protocol would involve generating a photon in a superposition of n paths/time-bins using passive beam splitters (or beam combiners). As we increase the number of paths/time-bins, the insertion loss of passive beam splitters reduces the sifted key rate by a factor of n. Scaling of n in an experimental realization thus reduces the sifted key rate, in fact, the $n = 3$ protocol is shown to achieve the optimal secure key rate per pulse [42,53]. Note that $n = 3$ is the smallest n that allows Alice and Bob to encode the key information in a non-orthogonal set of states using only two phase values, 0 and π.

3 DPS-MDI-QKD

We now describe our MDI-QKD protocol based on the 3-pulse phase encoding scheme, using an ideal single-photon source. Apart from the fact that this scheme offers better security against individual attacks, compared to other DPS protocols, there are other practical considerations that motivate our use of the 3-path superposition in our protocol.

1. When Alice and Bob both use an ideal-single-photon source to implement a pulse-train protocol using two phase values (0 and π) for encoding key bits, the phase-independent nature of Hong—Ou-Mandel interference [54] makes the key extraction difficult.
2. Using only two phase values (0 and π) makes the states in a two-pulse protocol orthogonal, making them perfectly distinguishable [42].

Hence, we need at least 3-paths in the superposition to implement an MDI protocol using only a pair of phases $(0, \pi)$ for the encoding. An MDI protocol based on a two-path superposition, and four phase values $(0, \frac{\pi}{2}, \pi, \frac{3\pi}{2})$ was proposed in [34]. This scheme yields a phase-encoded version of BB84, with a sifted key rate of 1/2, but it needs four different voltage levels for driving the phase modulator in order to encode the key information. Now, increasing the number of voltage levels in a high-speed phase modulator driver circuit leads to an increase in amplitude fluctuations, consequently increasing the quantum bit error rate [55]. Our proposed DPS MDI protocol reduces the complexity of the key encoding process by using only two phase values $(0, \pi)$, with a sifted key rate of 4/9, explained in Sect. 3.1 below.

A simple schematic is shown in Fig. 2. As before, Alice and Bob generate single-photon pulses that pass through their respective DLIs, each creating the superposition state described in Eq. (1). Alice and Bob then encode the random key bits {0, 1} by assigning a relative phase difference of {0, π} between two successive pulses, and send their encoded signal states to the measurement unit (Charles). Charles' measurement set-up comprises of a beamsplitter and two single-photon detectors, labeled D_c and D_d as indicated in Fig. 2. For every photon detected by his setup, he notes which detector clicked (D_c or D_d or both), and the corresponding time-bin (t_1, t_2 or t_3) at which the click was observed. Based on this information, which is made public by Charles, Alice and Bob extract a sifted key.
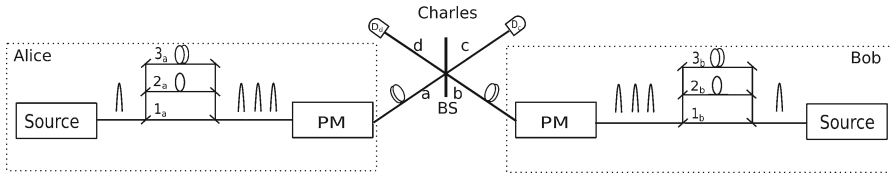
Fig. 2 Schematic of differential phase encoded MDI-QKD. Here, PM = Phase Modulator, D_c, D_d = Single-photon detectors

3.1 Sifting and reconciliation

We may use the form of the encoded 3-pulse state in Eq. (1) to represent the input to the Charles' measurement module as,

$$|\psi(\phi_{a_1}, \phi_{a_2}, \phi_{b_1}, \phi_{b_2})\rangle_{\text{in}} = \frac{1}{\sqrt{3}} \left(|100\rangle_a + e^{i\phi_{a_1}} |010\rangle_a + e^{i\phi_{a_2}} |001\rangle_a \right)$$
$$\otimes \frac{1}{\sqrt{3}} \left(|100\rangle_b + e^{i\phi_{b_1}} |010\rangle_b + e^{i\phi_{b_2}} |001\rangle_b \right). \quad (2)$$

As before, 1 and 0 indicate the presence or absence of a photon in a particular path. Similarly, $|100\rangle_a$ is the 3-pulse superposition state corresponding to the photon traversing path 1_a in Alice's set-up, $|010\rangle_b$ is a 3-pulse state corresponding to photon traversing path 2_b in Bob's set-up, and likewise for other terms in Eq. (2). For the sake of brevity, we represent tensor products of the form $|100\rangle_a \otimes |100\rangle_b$ as $|100, 100\rangle_{ab}$ in the rest of the paper. In DPS-MDI, Alice and Bob encode classical information as phase differences between first and second time-bins, and second and third time-bins. In our analysis, we assume the phase of the first time-bin as the reference phase, and apply a suitable phase (0 or π relative to the reference phase) on the second and third time-bins to encode the key information.

Corresponding to every pair of photons generated by the sources, there are three distinct time-bins (t_1, t_2, t_3) at which Charles' detectors click, corresponding to paths $1_a, 2_a, 3_a$ and $1_b, 2_b, 3_b$ in Alice's and Bob's set-up respectively. We first rewrite Charles' input state by grouping pairs of pulses that arrive in the same time-bin:

$$|\psi\rangle_{\text{in}} = \frac{1}{3} \Big[|100, 100\rangle_{ab} + e^{i\phi_{a_1}} |010, 100\rangle_{ab} + e^{i\phi_{a_2}} |001, 100\rangle_{ab}$$
$$+ e^{i\phi_{b_1}} |100, 010\rangle_{ab} + e^{i\phi_{b_2}} |100, 001\rangle_{ab} + e^{i(\phi_{a_1}+\phi_{b_1})} |010, 010\rangle_{ab}$$
$$+ e^{i(\phi_{a_1}+\phi_{b_2})} |010, 001\rangle_{ab} + e^{i(\phi_{a_2}+\phi_{b_1})} |001, 010\rangle_{ab}$$
$$+ e^{i(\phi_{a_2}+\phi_{b_2})} |001, 001\rangle_{ab} \Big]. \quad (3)$$

Note that the pairs of photons that traverse through identical paths in Alice's and Bob's interferometer (such as (1_a, 1_b) or (2_a, 2_b) or (3_a, 3_b)) do not contribute to the sifted key. Such a pair of photons would bunch together due to Hong–Ou–Mandel interference [54] and come out at the same port of the beamsplitter.

Table 1 Key reconciliation scheme for the proposed protocol

Measurement outcome of Charles	Action of Alice and Bob	Requirement of bit flip	Shared EPR pair
Det c clicks at both t_1 and t_2	Extract key using $\Delta\phi_1$	No	$\frac{1}{\sqrt{2}}[\lvert 00\rangle_{A_1 B_1} - \lvert 11\rangle_{A_1 B_1}]$
Det d clicks at both t_1 and t_2	Extract key using $\Delta\phi_1$	No	$\frac{1}{\sqrt{2}}[\lvert 00\rangle_{A_1 B_1} - \lvert 11\rangle_{A_1 B_1}]$
Det c clicks at both t_1 and t_3	Extract key using $\Delta\phi_2$	No	$\frac{1}{\sqrt{2}}[\lvert 00\rangle_{A_2 B_2} - \lvert 11\rangle_{A_2 B_2}]$
Det d clicks at both t_1 and t_3	Extract key using $\Delta\phi_2$	No	$\frac{1}{\sqrt{2}}[\lvert 00\rangle_{A_2 B_2} - \lvert 11\rangle_{A_2 B_2}]$
Det c clicks at t_1 and det d at t_2	Extract key using $\Delta\phi_1$	Yes	$\frac{1}{\sqrt{2}}[\lvert 01\rangle_{A_1 B_1} - \lvert 10\rangle_{A_1 B_1}]$
Det c clicks at t_2 and det d at t_1	Extract key using $\Delta\phi_1$	Yes	$\frac{1}{\sqrt{2}}[\lvert 01\rangle_{A_1 B_1} - \lvert 10\rangle_{A_1 B_1}]$
Det c clicks at t_1 and det d at t_3	Extract key using $\Delta\phi_2$	Yes	$\frac{1}{\sqrt{2}}[\lvert 01\rangle_{A_2 B_2} - \lvert 10\rangle_{A_2 B_2}]$
Det c clicks at t_3 and det d at t_1	Extract key using $\Delta\phi_2$	Yes	$\frac{1}{\sqrt{2}}[\lvert 01\rangle_{A_2 B_2} - \lvert 10\rangle_{A_2 B_2}]$
Det c clicks at both t_2 and t_3	Discard the bits	–	–
Det d clicks at both t_2 and t_3	Discard the bits	–	–
Det c clicks at t_2 and det d at t_3	Discard the bits	–	–
Det c clicks at t_3 and det d at t_2	Discard the bits	–	–

We write $\frac{1}{\sqrt{2}}[\lvert 0\rangle_{A_1}\lvert 0\rangle_{B_1} - \lvert 1\rangle_{A_1}\lvert 1\rangle_{B_1}]$ as $\frac{1}{\sqrt{2}}[\lvert 00\rangle_{A_1 B_1} - \lvert 11\rangle_{A_1 B_1}]$, and similarly for other terms

Using a beamsplitter transformation, we can write down the final two-photon state after the action of Charles' beamsplitter. We refer to "Appendix A" for the details of the calculation, with the form of the final state after Charles' measurement given in Eq. (28). We observe that depending on the values of the relative phases $\Delta\phi_1 = \phi_{a_1} - \phi_{b_1}$ and $\Delta\phi_2 = \phi_{a_2} - \phi_{b_2}$, and the path traversed by Alice's and Bob's photons, Charles may have the same or different detectors click at two different time-bins.

Finally, Alice and Bob perform key reconciliation once Charles announces his measurement outcomes. Based on which detector (D_c or D_d) clicks and the time-bins (t_1, t_2 and t_3) corresponding to the clicks for each pair of signal states, Alice and Bob can generate the sifted key using either $\Delta\phi_1$ or $\Delta\phi_2$ as listed in Table 1.

It follows immediately that the the sifted key rate of our protocol is,

$$R_{\text{sift}} = \frac{2}{3} \times \frac{2}{3} = \frac{4}{9}. \tag{4}$$

We discard the clicks that occur when photons from Alice and Bob fall on the beam splitter in the same time-bin. The terms $\lvert 100, 100\rangle_{ab}$, $\lvert 010, 010\rangle_{ab}$ and $\lvert 001, 001\rangle_{ab}$ in Eq. (3) correspond to such a scenario. Photons arriving at the same time-bin causes Hong–Ou–Mandel interference which leads to two photons falling on the same detector in the same time-bin, thereby making key extraction difficult. Comparing Eqs. (3) and (24), we see that one-third of the incoming photons have to be discarded due to Hong–Ou–Mandel interference. This leads to the first factor of $\frac{2}{3}$. Next, we observe from the key reconciliation table that two-thirds of Charles' measurements contribute to the raw key, thus leading to a sifted key rate of $\frac{4}{9}$. We note that the MDI protocol based

on 3-pulse encoding offers a lower key rate compared to the one based on coherent-state pulse-train encoding [33]. However, the use of single-photon sources in our protocol allows us to carry out a finite key analysis using the framework presented in [56]. Our protocol is also immune against eavesdropping attacks which target multi-photon pulses.

3.2 An equivalent entanglement-based protocol

To analyze the security of DPS-MDI, we first map it to a protocol that involves shared entangled pairs between Alice and Bob. Such a mapping of a phase-encoded protocol to an entanglement-based protocol has been shown earlier [42]. Following a similar approach, we now show there exists an equivalent, entanglement-based protocol to our proposed DPS-MDI-QKD protocol. The equivalent description of DPS-MDI, in terms of entangled states, allows us to demonstrate the unconditional security of our protocol and also perform the key rate analyses.

We first represent Alice's single-photon pulse in a linear superposition of three orthogonal states,

$$|\psi\rangle_a = \frac{1}{\sqrt{3}} \sum_{k=1}^{3} a_k^\dagger |0\rangle . \tag{5}$$

Here, $a_k^\dagger$ denotes the creation operator for the photon in the kth time-bin. Alice uses a quantum random number generator to generate a random 2-bit integer j, written in binary notation as $(j_1 j_2)_2$. She encodes this random integer in the single-photon pulse, such that the encoded state is written as,

$$|\psi_{j_1 j_2}\rangle_a = \frac{1}{\sqrt{3}} \left(a_1^\dagger |0\rangle + (-1)^{j_1} a_2^\dagger |0\rangle + (-1)^{j_2} a_3^\dagger |0\rangle \right) . \tag{6}$$

Alice prepares and stores 2 qubits corresponding to each encoded block in her quantum memory. She prepares $|j_1\rangle$ in $|0\rangle$ ($|1\rangle$) state when she applies a phase of 0 (π) to her second time-bin. Similarly, she prepares $|j_2\rangle$ in $|0\rangle$ ($|1\rangle$) state when she applies a phase of 0 (π) to her third time-bin. In this way, she entangles her two qubits to the encoded single-photon state as

$$|\psi\rangle_{\text{Alice}} = \frac{1}{2} \sum_{j_1, j_2 \in \{0,1\}} |j_1 j_2\rangle_{A_1 A_2} \otimes |\psi_{j_1 j_2}\rangle_a . \tag{7}$$

Bob also carries out a similar encoding procedure to get his own register of qubits entangled with his encoding blocks. Along the lines of Eqs. (6) and (7), Bob's state is written as,

$$|\psi\rangle_{\text{Bob}} = \frac{1}{2} \sum_{\tilde{j}_1, \tilde{j}_2 \in \{0,1\}} |\tilde{j}_1 \tilde{j}_2\rangle_{B_1 B_2} \otimes |\psi_{\tilde{j}_1 \tilde{j}_2}\rangle_b , \tag{8}$$

where $\tilde{j}_1$ or $\tilde{j}_1$ are the random integers used by Bob to encode his single-photon pulse.

Alice and Bob send their encoded states across to Charles. He first applies a quantum non-demolition (QND) measurement to find the number of photons in a given state and throws away the ones which have more than one photon in the same time-bin. He sends the rest through his beamsplitter. He then publicly announces the time-bin (say $k = 1, 2,$ or 3), as well as the detector (D_c or D_d), at which the photon was detected. As explained in Table 1, based upon Charles' measurement outcome, Alice and Bob use either $\Delta\phi_1$ or $\Delta\phi_2$ to extract the key.

When their shared key is established using $\Delta\phi_i$, Alice and Bob retain their corresponding ancilla qubits (A_i and B_i, respectively) and discard the other ancilla qubit. As shown in "Appendix B", for those time slots when they do not need to carry-out a bit flip operation, they share a perfectly correlated entangled state $\frac{1}{\sqrt{2}}[|00\rangle_{A_i B_i} - |11\rangle_{A_i B_i}]$. On the other hand, corresponding to those time slots when they execute a bit-flip to extract the shared key, they share the anti-correlated Bell state $\frac{1}{\sqrt{2}}[|01\rangle_{A_i B_i} - |10\rangle_{A_i B_i}]$. Thus, Charles measurement and filtering effectively implements a Bell state measurement, thereby entangling Alice's and Bob's ancilla qubits. A detailed discussion of the joint state after Charles' measurement and key-reconciliation can be found in "Appendix B".

3.3 Asymptotic secure key rate

Alice and Bob perform classical post-processing on the sifted key to extract the final secure key from it. The first step of this post-processing is to estimate the error rate in the sifted key, which involves Alice and Bob exposing a fraction of their sifted key bits to calculate the error rate. They abort the protocol and start again from the beginning (i.e., signal transmission to Charles) if their calculated error rate exceeds a pre-defined threshold. They define this threshold error rate by taking into account the error introduced in the key, both due to the system imperfections as well as any potential eavesdropping.

When the estimated error rate lies below the threshold error rate, they carry out the second step of post-processing, i.e., error correction. Alice and Bob apply a suitable error correction scheme on their sifted key to correct all the erroneous bits. The error estimation and correction happens over a classical channel, and we must assume that Eve is privy to all the information exchanged between Alice and Bob. Therefore, the final step of post-processing is privacy amplification, which aims to reduce Eve's knowledge about the key well below an acceptable level. This is done by discarding a fraction of the error-free key. Alice and Bob typically use a hash function to carry out privacy amplification.

Using the sifted key rate obtained in Eq. (4) and following the analysis in [3,25], we obtain the following asymptotic secure key rate for our MDI-DPS protocol,

$$R \geq Y_{11}[1 - fh(e_b) - h(e_p)]. \tag{9}$$

Here, Y_{11} is the probability of a successful Bell state measurement (BSM) when Alice and Bob transmit single photons. As per our mapping of DPS-MDI to an equivalent entangled-based protocol, a successful BSM corresponds to the cases tabulated in
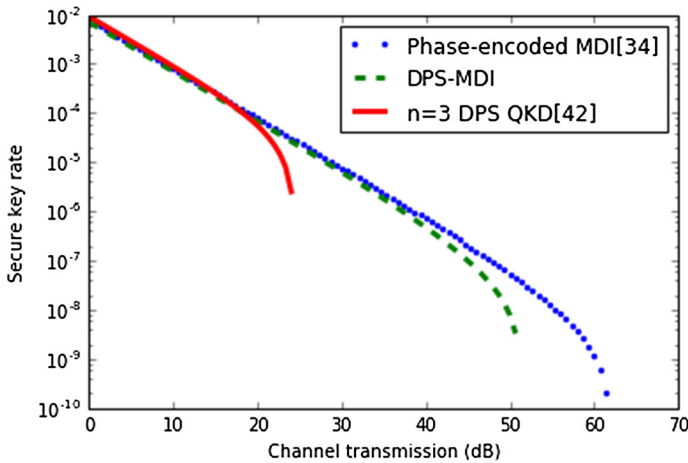
Fig. 3 Key rates for ideal, single-photon based protocols

Table 1 where Charles' measurement outcomes contribute to the sifted key. e_b is the quantum bit-error rate (QBER), e_p is the phase error rate, f represents the inefficiency of the error correction scheme employed by Alice and Bob, and $h(x)$ is the binary entropy function.

We bound the phase error rate of our protocol in terms of the bit error rate in "Appendix C" as,

$$e_p \leq e_b, \tag{10}$$

and use this bound for all of the simulation results. We also explicitly calculate the parameters given in Eq. (9) for our protocol in "Appendix D". We have taken phase misalignment, dark counts and different channel losses for the two channels into consideration while obtaining these parameters.

We compare the asymptotic key rate of DPS-MDI with two other protocols - phase-encoded MDI protocol [34] and DPS QKD [42]. From Fig. 3, we observe that DPS-MDI offers a secure channel length which is nearly twice of the channel length of DPS QKD—a trademark of MDI protocols when compared with non-MDI protocols. We also see that our DPS-MDI protocol offers performance comparable to an existing phase-encoded MDI protocol in terms of secure channel length and key rate. The slightly higher key rate in [34] is attributed to its higher sifted key rate of $\frac{1}{2}$ compared to DPS-MDI's rate of $\frac{4}{9}$.

We have obtained the non-MDI DPS QKD plot in Fig. 3 by using the key rate equation derived in [42]. We would like to point out the difference in the secure channel length for n=3 DPS QKD obtained in [42] and our simulation. The difference arises because we have used 3×10^{-6} as the dark count probability in our simulation, which is 1000 times higher than the dark count probability used in [42]. Also, [42] assumes an ideal error correction step in their classical post-processing, while our simulations assume a non-ideal error correction step. We capture the inefficiency of error correction in our protocol using the parameter f (Eq. 9).

In experimental implementations, weak coherent sources (WCS) are typically used to generate pulses with mean photon number (μ) of less than one so that the probability of generation of multi-photon pulses is significantly less than that of single-photon pulses. However, a WCS could still generate multi-photon pulses, and leak information to Eve. Hence, we use the decoy-state method to establish the security of our DPS-MDI protocol. The original decoy-state based QKD protocols have been proposed for BB84 schemes and secure key rates obtained in [57,58]. Decoy state analysis for MDI-BB84 was done in [25]. In our case, we follow the approach in [25] along with the improved phase-post-selection technique employed in [34] to obtain the key rate as,

$$R \geq Q_{11}[1 - h(e_\mathrm{p})] + Q'_{0\mu_b} - I_\mathrm{ec}. \tag{11}$$

Here, I_ec is the cost of error correction written as

$$I_\mathrm{ec} = Q_{\mu_a\mu_b} f h(E_{\mu_a\mu_b}), \tag{12}$$

where $Q_{\mu_a\mu_b}(E_{\mu_a\mu_b})$ is the overall gain (QBER) when Alice and Bob use a WCS with mean photon numbers μ_a and μ_b, respectively. $Q_{11}(e_\mathrm{p})$ is the gain (phase error rate) when both the sources generate single-photon states, and $Q'_{0\mu_b} = e^{-\mu_a} Q_{0\mu_b}$ is the probability that there is no photon from Alice's side and a successful BSM occurs. We refer to "Appendix D" for formal definitions and a detailed evaluation of these parameters.

Our decoy-state analysis assumes a fully phase-randomized coherent source. The intrinsic QBER shoots up due to phase randomization of the coherent source. The overall phase of $[0, 2\pi)$ can be sliced into N distinct slices as,

$$\left[\frac{m\pi}{N}, \frac{(m+1)\pi}{N} \right) \cup \left[\frac{(m+N)\pi}{N}, \frac{(m+N+1)\pi}{N} \right), \tag{13}$$

where m ranges from 0 to $N - 1$. Instead of carrying out phase randomization over the entire interval $[0, 2\pi)$, Alice and Bob randomly select one slice out of N, and then randomize the phase. Hence, an additional step of revealing the selected slice gets added in the decoy state version of our protocol. Alice and Bob keep the bits when both of them have selected the same phase slice. Figure 4 shows that dividing the interval $[0, 2\pi)$ into slices reduces the intrinsic QBER from 34% to around 1% for $N = 16$.

However, this phase-post-selection technique also changes the cost of error correction mentioned in Eq. (12) to

$$I_\mathrm{ec} = \sum_m Q^m_{\mu_a\mu_b} f h(E^m_{\mu_a\mu_b}). \tag{14}$$

From our numerical simulations, we observe that the key rate becomes negative upon using Eq. (14) in conjugation with Eq. (11). Hence, we assume that the gain and error rate of the single-photon states are evenly distributed over all the slices, thereby modifying the decoy MDI key rate equation to
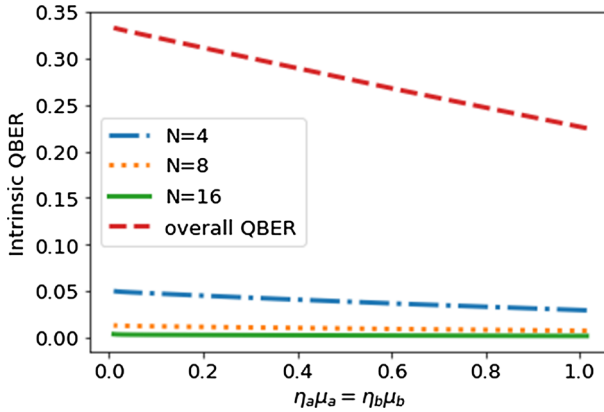
Fig. 4 QBER comparison when phase randomization is **a** carried out over entire range (**b**) carried out in one of the N slices. We have used Eq. (94) for numerically evaluating the QBER
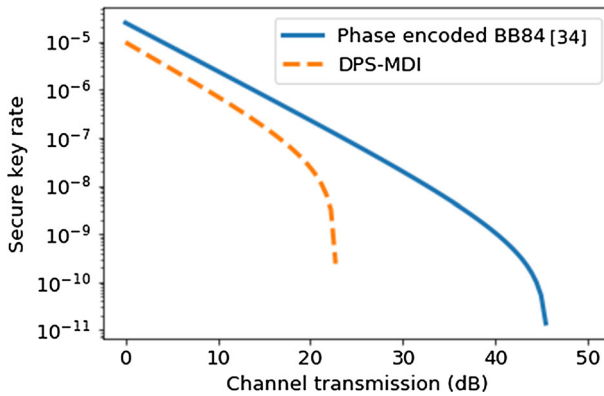

Fig. 5 Key rate comparison for decoy-state MDI schemes

$$R \geq \frac{1}{N} Q_{11}[1 - h(e_{\mathrm{p}})] + Q'_{0\mu_b} - Q^m f h(E^m)|_{m=0}. \tag{15}$$

We refer to "Appendix D" for a detailed analysis of the effect of this phase-post-selection technique on the overall gain and QBER. We compare the key rate of our decoy-state DPS-MDI with [34] (see Fig. 5), where we used the parameters from [25] for our simulations. The quantum efficiency of the detectors was taken to be 14.5% with a misalignment error of 1.5%. N and f are taken to be 16 and 1.16 respectively. We assume a dark count rate of 3×10^{-6} for the detector and an attenuation of 0.2 dB/km in the fiber channel.

3.4 Practical implementation

As described above, Alice and Bob can share a secure key using the setup shown in Fig. 2. However, a practical implementation of the proposed scheme requires certain modifications to the set-up (see Fig. 6).
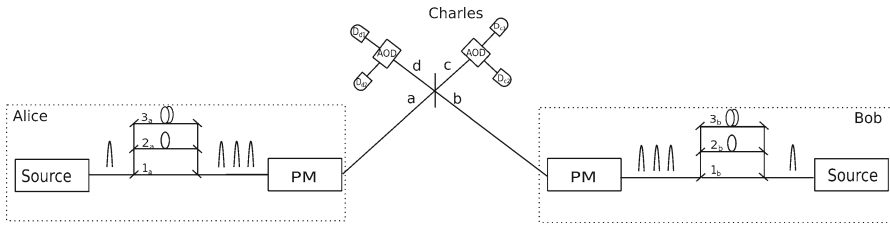
Fig. 6 Schematic of a practical 3-pulse DPS-MDI-QKD implementation. Alice and Bob use a phase modulators (PM) and a delay line interferometer each. Charlie's set-up comprises a beamsplitter, four detectors and two acousto-optic deflectors (AODs)

1. Key generation requires detection of two time-synchronized photons by a single detector. In practice, this would be constrained by the finite dead-time of a single-photon detector. Hence, an acousto-optic deflector (AOD) is used to route the photon in each time-bin to different single-photon detectors. This results in a slight modification to the key-reconciliation step, namely, Charles now announces which pair of detectors clicked in each time-bin.
2. Alice and Bob need a common phase reference, since they use independent laser sources for generating their single-photon pulses. The optical phase-locked loop (OPLL) technique [59,60], commonly used in coherent detections, can be used to phase lock the sources used by Alice and Bob. The OPLL has a simple setup and requires only off-the-shelf components [61].

4 Finite key analysis of DPS-MDI-QKD

Finiteness of the key size constitutes a major chink in the security proofs of practical QKD protocols. Most of the theoretical proofs provide a bound on the secure key rate by assuming the key size as infinite. However, practical implementations cannot run forever. This gap in theory and practice is bridged by providing security bounds for a finite number of signal exchanges between Alice and Bob.

A perfect key is a uniformly distributed bit string, having no dependence on an adversary's knowledge. Practical keys deviate from this ideal scenario, and this deviation is captured by a parameter ε, interpreted as the maximum probability of a practical key differing from a completely random bit string. Following [62,63], we say that a key K is ε-secure with respect to an eavesdropper E if,

$$\frac{1}{2} \parallel \rho_{KE} - \tau_K \otimes \rho_E \parallel_1 \leq \varepsilon. \tag{16}$$

Here, ρ_{KE} is the joint state of the 'key system' K and the adversary E, ρ_E is the state held by the adversary, and τ_K is the completely mixed state on K.

In the asymptotic case, for any QKD protocol where Alice and Bob share entangled pairs, the secure key rate (R) can be bounded under the assumption of collective attacks as [1,3,64],

$$R = H(X \mid E) - H(X \mid Y), . \tag{17}$$

Here, X and Y represent Alice and Bob's key systems, respectively, E represents the eavesdropper, and $H(.\mid.)$ is the conditional von Neumann entropy. Intuitively, Eq. (17) follows from the fact that the secure key rate is equal to Eve's uncertainty about the raw key X minus Bob's uncertainty. For our DPS-MDI protocol, the conditional entropy $H(X\mid E)$ can be expressed as [65],

$$H(\tilde{X}\mid\tilde{E}) = 1 - h(e_b) - h(e_p), \tag{18}$$

where e_b is the bit error rate, and e_p denotes the phase error rate.

We follow the finite-key analysis presented in [56,65], involving a generalization of von Neumann entropy, called the *smooth* entropy. The objective of this smoothening of the regular entropic functions is to take into account the fluctuations arising from the finite signal size. As in the asymptotic case, Alice and Bob are assumed to share entangled pairs, which holds for our proposed scheme, as outlined in Sect. 3.2 above. The generalized form of Eq. (17) in the finite-key regime can be expressed as [56],

$$r = H_\xi(X\mid E) - (\text{leak}_{\text{EC}} + \Delta)/n, \tag{19}$$

where $H_\xi(X\mid E)$ is the conditional smooth-min entropy, leak_{EC} is the number of bits needed to be shared over a classical channel for error correction and

$$\Delta = 2\,\log_2\frac{1}{[2(\varepsilon - \bar{\varepsilon} - \varepsilon_{\text{EC}})]} + 7\sqrt{n\log_2(2/(\bar{\varepsilon} - \bar{\varepsilon}'))}. \tag{20}$$

Here, ε_{EC} is the error probability, defined as the probability that Bob ends up with a wrong bit string after the error correction stage. $\bar{\varepsilon}$ and $\bar{\varepsilon}'$ are the smoothening parameters as mentioned in Lemma 2 of [56].

We calculate $H_\xi(X\mid E)$ for our protocol using the asymptotic value of $H(X\mid E)$ and bound the phase error rate in terms of the bit error rate. We have shown in "Appendix C" that the phase error rate of our protocol is bounded by the bit error rate as,

$$e_p \le e_b. \tag{21}$$

In the finite-key regime Eq. (18) translates to,

$$H_\xi(X\mid E) = 1 - h(\tilde{e}_b) - h(\tilde{e}_p). \tag{22}$$

Finally, the bit error rate in the finite-key regime is expressed as $\tilde{e}_b = e_b + \xi$ $(n, d = 9)$, where n is the number of raw key bits. Similarly, the phase error rate is given as $\tilde{e}_p = e_p + \xi$ $(m, d = 9)$, where m is the number of bits used in parameter estimation and d is the number of possible POVM outcomes. $d = 9$ for our protocol as there are eight scenarios at the detection unit (see Table 1) which contribute to the key generation. The ninth POVM corresponds to the case when BSM fails. ξ is a non-negative parameter, (Lemma 3 of [56]) given by,

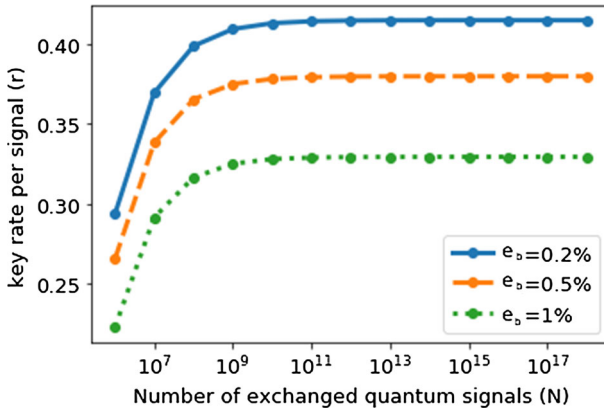$$\xi = \sqrt{\frac{2\ln(1/\bar{\varepsilon}') + d\ln(m+1)}{m}}. \tag{23}$$

Fig. 7 Key rate r as a function of the number of exchanged quantum signals for different values of e_b

Using Eqs. (20), (22), and (23) we estimate the sifted key rate described in Eq. (19). The performance of a practical error correcting code as analyzed in [56] gives $\text{leak}_{EC}/n = 1.2h(e_b)$, where, e_b is the quantum bit error rate. This helps in estimating the second term of Eq. (19). $(N, \varepsilon, \text{leak}_{EC}, \varepsilon_{EC})$ are protocol dependent parameters, whereas $n, m, \bar{\varepsilon}$ and $\bar{\varepsilon}'$ are selected so as to maximize the key rate per signal, $r = (n/N)r'$ under the constraints $n + m \leq N$ and $\varepsilon - \varepsilon_{EC} > \bar{\varepsilon} > \bar{\varepsilon}' \geq 0$.

Figure 7 shows the variation in key rate with the number of exchanged signals for our DPS-MDI protocol. We have used $\varepsilon = 10^{-5}$ and $\varepsilon_{EC} = 10^{-10}$ to generate the plots for different values of e_b. As expected, the key rate per signal (r) approaches the sifted key rate of $\frac{4}{9}$ in the asymptotic limit. This is a reflection of the fact that only $\frac{4}{9}$ of the raw key bits can be used for key generation and the rest is used for parameter estimation.

5 Conclusions

In this paper, we have presented a 3-path superposition based DPS-MDI-QKD protocol. We have shown the necessity and advantages of having the 3-path superposition. The proposed protocol has been mapped to an entanglement-based protocol, thereby establishing its unconditional security. We have carried out a security analysis of our scheme in the asymptotic regime assuming system imperfections.

We have shown that our protocol generates secure keys even when the ideal single-photon source is replaced with a weak coherent source (WCS). The security of the WCS-based scheme is established using decoy states and a suitable phase-post-selection technique. Finally, we have determined an upper-bound for the phase error rate of our protocol in terms of the bit error rate. This allows us to carry out the key analysis of the protocol in both asymptotic as well as finite-key regimes. We have further simulated the variation in key rate with the number of exchanged signals of our protocol.
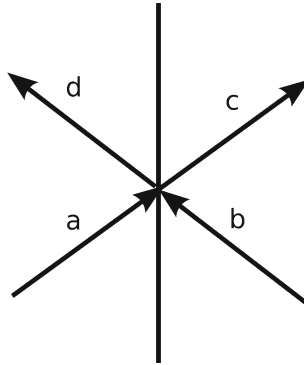
Fig. 8 *a* and *b* are input ports, and *c* and *d* are the output ports of the beamsplitter

An interesting direction for future work is the finite-key analysis of the 3-path DPS-MDI using a weak coherent source. Such a coherent-state DPS-MDI protocol will also be free from the issues arising due to the probabilistic nature of photon generation in single-photon sources. Another interesting problem that can be addressed in the future works is the tightening of the bound used in obtaining the secure key rates of our protocol.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

A Analysis of DPS-MDI-QKD protocol

We start with the form of the input to Charles' beamsplitter given in Eq. (3):

$$
|\psi\rangle_{\mathrm{in}} = \frac{1}{3} \Big[|100, 100\rangle_{ab} + e^{i\phi_{a_1}} |010, 100\rangle_{ab}
$$
$$
+ e^{i\phi_{a_2}} |001, 100\rangle_{ab} + e^{i\phi_{b_1}} |100, 010\rangle_{ab}
$$
$$
+ e^{i\phi_{b_2}} |100, 001\rangle_{ab} + e^{i(\phi_{a_1}+\phi_{b_1})} |010, 010\rangle_{ab} + e^{i(\phi_{a_1}+\phi_{b_2})} |010, 001\rangle_{ab}
$$
$$
+ e^{i(\phi_{a_2}+\phi_{b_1})} |001, 010\rangle_{ab} + e^{i(\phi_{a_2}+\phi_{b_2})} |001, 001\rangle_{ab} \Big].
$$

We leave out the states that correspond to photons traversing identical paths in Alice's and Bob's set-up, since they do not contribute to the sifted key, and consider the (normalized) state,

$$
|\psi\rangle_{\mathrm{in}} = \frac{1}{\sqrt{6}} \Big[e^{i\phi_{a_1}} |010, 100\rangle_{ab} + e^{i\phi_{a_2}} |001, 100\rangle_{ab}
$$

$$+ e^{i\phi_{b_1}} |100, 010\rangle_{ab} + e^{i\phi_{b_2}} |100, 001\rangle_{ab}$$
$$+ e^{i(\phi_{a_1}+\phi_{b_2})} |010, 001\rangle_{ab} + e^{i(\phi_{a_2}+\phi_{b_1})} |001, 010\rangle_{ab} \Big].$$
(24)

Writing $\phi_{a_1} - \phi_{b_1} = \Delta\phi_1$ and $\phi_{a_2} - \phi_{b_2} = \Delta\phi_2$ as the phase differences between corresponding pulses from Alice and Bob, the input to Charles' beamsplitter is written as,

$$|\tilde{\psi}\rangle_{\text{in}} = \frac{1}{\sqrt{6}} e^{i(\phi_{b_1}+\phi_{b_2})} \Big[e^{i\Delta\phi_1} |010, 001\rangle_{ab}$$
$$+ e^{i\Delta\phi_2} |001, 010\rangle_{ab} + e^{-i\phi_{b_1}} \Big(|100, 001\rangle$$
$$+ e^{i\Delta\phi_2} |001, 100\rangle \Big) + e^{-i\phi_{b_2}} \Big(|100, 010\rangle + e^{i\Delta\phi_1} |010, 100\rangle_{ab} \Big) \Big] (25)$$

Figure 8 shows a typical 50 : 50 beamsplitter. The action of the beamsplitter with input ports a, b and output ports c, d, when there is a photon incident on only one of the two ports is given by,

$$|1, 0\rangle_{ab} \longrightarrow \frac{1}{\sqrt{2}} \big(|1, 0\rangle_{cd} + |0, 1\rangle_{cd} \big),$$
$$|0, 1\rangle_{ab} \longrightarrow \frac{1}{\sqrt{2}} \big(|1, 0\rangle_{cd} - |0, 1\rangle_{cd} \big).$$
(26)

Using Eq. 26, we find that the beamsplitter transforms the terms present in the joint input state of Alice and Bob (Eq. 25) as shown below:

$$|010, 001\rangle_{ab} \longrightarrow \frac{1}{2} \Big(|011, 000\rangle_{cd} - |010, 001\rangle_{cd} + |001, 010\rangle_{cd} - |000, 011\rangle_{cd} \Big),$$
$$|001, 010\rangle_{ab} \longrightarrow \frac{1}{2} \Big(|011, 000\rangle_{cd} + |010, 001\rangle_{cd} - |001, 010\rangle_{cd} - |000, 011\rangle_{cd} \Big),$$
$$|100, 001\rangle_{ab} \longrightarrow \frac{1}{2} \Big(|101, 000\rangle_{cd} - |100, 001\rangle_{cd} + |001, 100\rangle_{cd} - |000, 101\rangle_{cd} \Big),$$
$$|001, 100\rangle_{ab} \longrightarrow \frac{1}{2} \Big(|101, 000\rangle_{cd} + |100, 001\rangle_{cd} - |001, 100\rangle_{cd} - |000, 101\rangle_{cd} \Big),$$
$$|100, 010\rangle_{ab} \longrightarrow \frac{1}{2} \Big(|110, 000\rangle_{cd} - |100, 010\rangle_{cd} + |010, 100\rangle_{cd} - |000, 110\rangle_{cd} \Big),$$
$$|010, 100\rangle_{ab} \longrightarrow \frac{1}{2} \Big(|110, 000\rangle_{cd} + |100, 010\rangle_{cd} - |010, 100\rangle_{cd} - |000, 110\rangle_{cd} \Big),$$
$$|100, 100\rangle_{ab} \longrightarrow \frac{1}{\sqrt{2}} \Big(|200, 000\rangle_{cd} - |000, 200\rangle_{cd} \Big),$$
$$|010, 010\rangle_{ab} \longrightarrow \frac{1}{\sqrt{2}} \Big(|020, 000\rangle_{cd} - |000, 020\rangle_{cd} \Big),$$
$$|001, 001\rangle_{ab} \longrightarrow \frac{1}{\sqrt{2}} \Big(|002, 000\rangle_{cd} - |000, 002\rangle_{cd} \Big).$$
(27)

Using Eq. (25) and Eq. (27), we get

$$
\begin{aligned}
|\psi\rangle_{\text{out}} = \frac{1}{2\sqrt{6}} e^{i(\phi_{b_1}+\phi_{b_2})} \Big[& e^{i\Delta\phi_1}\Big(|011,000\rangle_{cd} - |010,001\rangle_{cd} \\
& + |001,010\rangle_{cd} - |000,011\rangle_{cd} \Big) \\
& + e^{i\Delta\phi_2}\Big(|011,000\rangle_{cd} + |010,001\rangle_{cd} - |001,010\rangle_{cd} - |000,011\rangle_{cd} \Big) \\
& + e^{-i\phi_{b_1}}\Big\{ \Big(|101,000\rangle_{cd} - |100,001\rangle_{cd} + |001,100\rangle_{cd} - |000,101\rangle_{cd} \Big) \\
& + e^{i\Delta\phi_2}\Big(|101,000\rangle_{cd} + |100,001\rangle_{cd} - |001,100\rangle_{cd} - |000,101\rangle_{cd} \Big) \Big\} \\
& + e^{-i\phi_{b_2}}\Big\{ \Big(|110,000\rangle_{cd} - |100,010\rangle_{cd} + |010,100\rangle_{cd} - |000,110\rangle_{cd} \Big) \\
& + e^{i\Delta\phi_1}\Big(|110,000\rangle_{cd} + |100,010\rangle_{cd} - |010,100\rangle_{cd} - |000,110\rangle_{cd} \Big) \Big\} \Big].
\end{aligned}
$$
(28)

The output after the beamsplitter depends upon the random phase applied by Alice and Bob to their respective time-bins. We write down the four different final states realized, corresponding to the four possible values of $(\Delta\phi_1, \Delta\phi_2)$. To help understand the key-reconciliation step, we have rewritten the final state by grouping together the states at each output port (c or d), corresponding to the three different time-bins (t_1, t_2 or t_3).

Case 1: When $\Delta\phi_1 = \Delta\phi_2 = 0$, the two-photon state after the beamsplitter is,

$$
\begin{aligned}
|\psi\rangle_{\text{out}} = \frac{1}{\sqrt{6}} e^{i(\phi_{b_1}+\phi_{b_2})} \Big[& \Big(|011,000\rangle_{cd} - |000,011\rangle_{cd} \Big) + e^{-i\phi_{b_1}}\Big(|101,000\rangle_{cd} \\
& - |000,101\rangle_{cd} \Big) + e^{-i\phi_{b_2}}\Big(|110,000\rangle_{cd} - |000,110\rangle_{cd} \Big) \Big].
\end{aligned}
$$
(29)

Case 2: When $\Delta\phi_1 = \Delta\phi_2 = \pi$, the output state of the beamsplitter is,

$$
\begin{aligned}
|\psi\rangle_{\text{out}} = \frac{1}{\sqrt{6}} e^{i(\phi_{b_1}+\phi_{b_2})} \Big[& \Big(|011,000\rangle_{cd} - |000,011\rangle_{cd} + e^{-i\phi_{b_1}}\Big(|001,100\rangle_{cd} \\
& - |100,001\rangle_{cd} \Big) + e^{-i\phi_{b_2}}\Big(|010,100\rangle_{d} - |100,010\rangle_{d} \Big) \Big].
\end{aligned}
$$
(30)

Case 3: When $\Delta\phi_1 = 0$ and $\Delta\phi_2 = \pi$, the output state is,

$$
\begin{aligned}
|\psi\rangle_{\text{out}} = \frac{1}{\sqrt{6}} e^{i(\phi_{b_1}+\phi_{b_2})} \Big[& \Big(|001,010\rangle_{cd} - |010,001\rangle_{cd} \Big) + e^{-i\phi_{b_1}}\Big(|001,100\rangle_{cd} \\
& - |100,001\rangle_{cd} \Big) + e^{-i\phi_{b_2}}\Big(|110,000\rangle_{cd} - |000,110\rangle_{cd} \Big) \Big].
\end{aligned}
$$
(31)

Case 4: When $\Delta\phi_1 = \pi$ and $\Delta\phi_2 = 0$, the output state is,

$$|\psi\rangle_{\text{out}} = \frac{1}{\sqrt{6}}e^{i(\phi_{b_1}+\phi_{b_2})}\Big[\Big(|010,001\rangle_{cd} - |001,010\rangle_{cd}\Big) + e^{-i\phi_{b_1}}\Big(|101,000\rangle_{cd}$$
$$- |000,101\rangle_{cd}\Big) + e^{-i\phi_{b_2}}\Big(|010,100\rangle_{cd} - |100,010\rangle_{cd}\Big)\Big]. \tag{32}$$

We now formulate the key reconciliation scheme (see Table 1) based on Eqs. (29)-(32), while noting that detector D_c detects the photons from port c of the beamsplitter and correspondingly detector D_d clicks when photons exits from port d.

Consider the two examples when Alice and Bob use $\Delta\phi_1$ to extract the key.

1. When Charles announces the clicking of D_c in time-bins t_1 and t_2, this would indicate that $\Delta\phi_1$ and $\Delta\phi_2$ have taken values corresponding to Case 1 or Case 3 above, corresponding to $\Delta\phi_1 = 0$ and $\Delta\phi_2 = 0$ or π. Alice and Bob therefore use only $\Delta\phi_1$ to extract the key.
2. When Charles announces the clicking of D_c at t_1 and D_d at t_2, Alice and Bob again use $\Delta\phi_1$ to extract the key. However, they also need a bit flip operation to get the same key bits. Note that in this example also, $\Delta\phi_1 = 0$ and $\Delta\phi_2 = 0$ or π.

A similar reasoning can be used to complete the key reconciliation scheme as described in Table 1.

B DPS-MDI as an entanglement-based protocol

We start with Eqs. (7) and (8), to write the joint state of Alice and Bob after their encoding procedure. Recall that A and B indicate Alice and Bob's signal states, whereas A_i and B_i indicate the ith pair of ancilla qubit in respective (ideal) quantum memories. The joint state thus reads as,

$$|\psi\rangle_{\text{Alice}} \otimes |\psi\rangle_{\text{Bob}} = \frac{1}{4}\sum_{j_1,j_2\in\{0,1\}}(|j_1\rangle_{A_1}|j_2\rangle_{A_2})\otimes|\psi_{j_1 j_2}\rangle_a$$
$$\otimes \sum_{\tilde{j}_1,\tilde{j}_2\in\{0,1\}}(|\tilde{j}_1\rangle_{B_1}|\tilde{j}_2\rangle_{B_2})\otimes|\psi_{\tilde{j}_1,\tilde{j}_2}\rangle_b,$$
$$= \frac{1}{4}\sum_{j_1,j_2,\tilde{j}_1,\tilde{j}_2\in\{0,1\}}|j_1\rangle_{A_1}|\tilde{j}_1\rangle_{B_1}|j_2\rangle_{A_2}|\tilde{j}_2\rangle_{B_2}$$
$$\otimes|\Psi_{(j_1 j_2 \tilde{j}_1 \tilde{j}_2)}\rangle_{ab}. \tag{33}$$

The state $|\Psi_{j_1 j_2 \tilde{j}_1 \tilde{j}_2}\rangle_{ab}$, which eventually becomes the input to Charles' beamsplitter, has the following form:

$$|\Psi_{j_1 j_2 \tilde{j}_1 \tilde{j}_2}\rangle_{ab} = |\psi_{j_1 j_2}\rangle_a \otimes |\psi_{\tilde{j}_1 \tilde{j}_2}\rangle_b$$
$$= \Big(a_1^\dagger b_1^\dagger + \sum_{i=1}^{2}(-1)^{(j_i+\tilde{j}_i)}a_{i+1}^\dagger b_{i+1}^\dagger + (-1)^{\tilde{j}_1}a_1^\dagger b_2^\dagger + (-1)^{\tilde{j}_2}a_1^\dagger b_3^\dagger$$

$$
\begin{aligned}
&+(-1)^{j_1} a_2^\dagger b_1^\dagger + (-1)^{j_1+\tilde{j}_2} a_2^\dagger b_3^\dagger + (-1)^{j_2} a_3^\dagger b_1^\dagger \\
&+(-1)^{(j_2+\tilde{j}_1)} a_3^\dagger b_2^\dagger \Big) |0,0\rangle_{ab}.
\end{aligned} \tag{34}
$$

Here, $|0,0\rangle_{ab} = |0\rangle_a \otimes |0\rangle_b$, and denotes the vaccum at the input ports of the beam-splitter. $a_i^\dagger$ and $b_i^\dagger$ are the creation operators corresponding to a photon traversing through the ith arm in Alice and Bob's delay lines respectively. As indicated above, there is no entanglement yet between Alice and Bob's states; rather, each encoded state is entangled with their respective quantum memories.

To obtain the output state after measurement and key reconciliation, we first do a post-selection and discard input states which have photons arriving at the same time-bin from both Alice and Bob. As described in Sect. 3, such photons do not contribute to the final key, due to Hong–Ou–Mandel interference. Hence, we drop terms of the form $a_i^\dagger b_i^\dagger$ in Eq. (34). When the photons arrive at different times, as represented by terms of the form $a_i^\dagger b_j^\dagger$ for $i \neq j$, they transform as,

$$
a^\dagger \rightarrow \frac{1}{\sqrt{2}} (c^\dagger + d^\dagger); \quad b^\dagger \rightarrow \frac{1}{\sqrt{2}} (c^\dagger - d^\dagger).
$$

We may thus write down the final state after the action of the beamsplitter and post-selection as,

$$
\begin{aligned}
|\Phi_{j_1 j_2 \tilde{j}_1 \tilde{j}_2}\rangle_{cd} = \frac{1}{2} \Big[&(-1)^{\tilde{j}_1} (c_1^\dagger + d_1^\dagger)(c_2^\dagger - d_2^\dagger) + (-1)^{\tilde{j}_2} (c_1^\dagger + d_1^\dagger)(c_3^\dagger - d_3^\dagger) \\
&+(-1)^{j_1} (c_2^\dagger + d_2^\dagger) \\
&\times (c_1^\dagger - d_1^\dagger) + (-1)^{(j_1+\tilde{j}_2)} (c_2^\dagger + d_2^\dagger)(c_3^\dagger - d_3^\dagger) \\
&+(-1)^{j_2} (c_3^\dagger + d_3^\dagger)(c_1^\dagger - d_1^\dagger) \\
&+(-1)^{(j_2+\tilde{j}_1)} (c_3^\dagger + d_3^\dagger)(c_2^\dagger - d_2^\dagger) \Big] |0,0\rangle_{cd}.
\end{aligned} \tag{35}
$$

The complete state, including the registers A_1, A_2 and B_1, B_2, is of the form,

$$
|\chi\rangle_{A_1 B_1 A_2 B_2 cd} = \frac{1}{4} \sum_{j_1, j_2, \tilde{j}_1, \tilde{j}_2 \in \{0,1\}} |j_1\rangle_{A_1} |\tilde{j}_1\rangle_{B_1} |j_2\rangle_{A_2} |\tilde{j}_2\rangle_{B_2} \otimes |\Phi_{(j_1 j_2 \tilde{j}_1 \tilde{j}_2)}\rangle_{cd}. \tag{36}
$$

As discussed in Sect. 3.2 , Alice and Bob extract information about their relative phases $\Delta\phi_1 = \phi_{a_1} - \phi_{b_1}$ and $\Delta\phi_2 = \phi_{a_2} - \phi_{b_2}$ based on Charles' measurement outcomes, and hence obtain the shared key. Expressing all the phases in terms of the binary variables (j_1, j_2) and $(\tilde{j}_1, \tilde{j}_2)$, which characterize Alice and Bob's qubit registers respectively, we have,

$$
\phi_{a_1} = j_1 \pi, \quad \phi_{a_2} = j_2 \pi, \quad \phi_{b_1} = \tilde{j}_1 \pi, \quad \phi_{b_2} = \tilde{j}_2 \pi.
$$

Thus the relative phases are given by,

$$\Delta\phi_1 = (j_1 - \tilde{j}_1)\pi, \quad \Delta\phi_2 = (j_2 - \tilde{j}_2)\pi.$$

It is now easy to show that the joint state of Alice and Bob's registers collapses to an entangled state after Charles' measurement and the reconciliation process described in Table 1. In particular, when Alice and Bob use the phases ϕ_{a_i}, ϕ_{b_i} to generate their secret key bits without a bit flip operation, they end up with the perfectly correlated Bell state $\frac{1}{\sqrt{2}}[|00\rangle_{A_i B_i} - |11\rangle_{A_i B_i}]$. In those cases where they need to perform a bit flip operation, they end up sharing the anti-correlated entangled state $\frac{1}{\sqrt{2}}[|10\rangle_{A_i B_i} - |01\rangle_{A_i B_i}]$.

For example, when Charles announces that the detector c has clicked in both t_1 and t_2 bins, Eq. (36) collapses to the post-measurement state,

$$
\begin{aligned}
|\chi^{(1)}\rangle_{\text{out}} = \frac{1}{2\sqrt{2}}\Big[&|0000\rangle_{A_1 B_1 A_2 B_2} - |0001\rangle_{A_1 B_1 A_2 B_2} \\
&+ |0010\rangle_{A_1 B_1 A_2 B_2} - |0011\rangle_{A_1 B_1 A_2 B_2} \\
&- |1100\rangle_{A_1 B_1 A_2 B_2} + |1101\rangle_{A_1 B_1 A_2 B_2} \\
&- |1110\rangle_{A_1 B_1 A_2 B_2} + |1111\rangle_{A_1 B_1 A_2 B_2} \Big] \\
&\otimes |110, 000\rangle_{cd},
\end{aligned}
\tag{37}
$$

where we have represented $|j_1\rangle_{A_1} |\tilde{j}_1\rangle_{B_1} |j_2\rangle_{A_2} |\tilde{j}_2\rangle_{B_2}$ as $|j_1 \tilde{j}_1 j_2 \tilde{j}_2\rangle_{A_1 B_1 A_2 B_2}$. We see that in Eq. (37), the first ancilla registers (A_1 and B_1) of both Alice and Bob always have same bit value. Hence, Alice and Bob share the perfectly correlated Bell state, as shown explicitly below,

$$
\begin{aligned}
|\chi^{(1)}\rangle_{\text{out}} = \frac{1}{2\sqrt{2}}\Big[&|00\rangle_{A_1 B_1} - |11\rangle_{A_1 B_1} \Big] \\
&\otimes \Big[|00\rangle_{A_2 B_2} - |01\rangle_{A_2 B_2} + |10\rangle_{A_2 B_2} - |11\rangle_{A_2 B_2} \Big] \\
&\otimes |110, 000\rangle_{cd}.
\end{aligned}
\tag{38}
$$

When Charles announces that the detector c clicked at t_1 and d at t_2, the state presented in Eq. (36) collapses to,

$$
\begin{aligned}
|\chi^{(2)}\rangle_{\text{out}} = \frac{1}{2\sqrt{2}}\Big[&- |0100\rangle_{A_1 B_1 A_2 B_2} \\
&+ |0101\rangle_{A_1 B_1 A_2 B_2} - |0110\rangle_{A_1 B_1 A_2 B_2} + |0111\rangle_{A_1 B_1 A_2 B_2} \\
&- |1000\rangle_{A_1 B_1 A_2 B_2} - |1001\rangle_{A_1 B_1 A_2 B_2} \\
&+ |1010\rangle_{A_1 B_1 A_2 B_2} - |1011\rangle_{A_1 B_1 A_2 B_2} \Big] \\
&\otimes |100, 010\rangle_{cd}.
\end{aligned}
\tag{39}
$$

As seen from Eq. (39), the first ancilla registers (A_1 and B_1) of Alice and Bob are now always opposite in the bit value. This implies they share an anti-correlated entangled state. Hence, they require a bit flip operation after Charles announcement so as to ensure that both of them end up with similar key bits. We can extend similar lines of reasoning to the other entries of Table 1 to show that Alice and Bob indeed share maximally entangled states.

C Bounding of phase error rate in terms of bit error rate

In "Appendix B", we show that Charles measurement entangles Alice's and Bob's ancilla qubits. However, the EPR pairs shared by Alice and Bob become corrupt due to channel noise and eavesdropping. Alice and Bob extract a small number of perfect EPR pairs from the corrupted EPR pairs using a suitable entanglement distillation protocol based on Calderbank–Shor–Steane (CSS) codes, provided the channel is not too noisy [3]. Alice and Bob determine the bit and the phase error rates. They continue with the entanglement distillation protocol if the error rates are nominal, else they abort the protocol. The bit error rates can be easily estimated by sharing a certain fraction of the raw key generated during the experiment. However, phase errors cannot be determined experimentally, and hence, need to be estimated indirectly using experimentally observed quantities. We upper bound the phase error rate for our scheme in terms of the bit error rate in this section.

We begin with $|\psi\rangle_{\text{out}}^{(l)}$, which is the state after Charles announces his measurement result for the lth time slot, and is related to the joint input state of Alice and Bob $|\psi\rangle_{\text{in}}^{(l)}$ as,

$$|\psi\rangle_{\text{out}}^{(l)} = F^{(l)} M^{(l)} E^{(l)} |\psi\rangle_{\text{in}}^{(l)} . \tag{40}$$

Here, $M^{(l)}$ is the beamsplitter operator acting on the lth time slot, $F^{(l)}$ is the filtering operator and $E^{(l)}$ is a 3×3 "noise" matrix representing the effects of noise and Eve's most general attack in lth time slot. We assume that the noise and Eve affect the link connecting Alice to Charles and Bob to Charles independently. Hence, we decompose the overall noise matrix $E^{(l)}$ as $E_a^{(l)} \otimes E_b^{(l)}$. Both $E_a^{(l)}$ and $E_b^{(l)}$ are 3×3 matrices with matrix elements $(a)_{ij}$ and $(b)_{ij}$, respectively. $|a_{ij}|^2$ gives the probability of time-bin i getting affected given that the noise/Eve acts on time-bin j. We would like to clarify the terms "time-bin" and "time-slot" used here. We use the time-slot label to mark every single-photon state (in the ideal scenario) or weak coherent pulse (in a typical experiment) generated by the source, whether Alice or Bob. Each pulse labeled by a time-slot is eventually measured at one of three time-bins ($i/j = 1, 2, 3$) by Charlie, depending on which path the photon traversed in the DLI at the source. The form of these matrices depends upon the type of noise in the channel. The matrix structure is dependent upon the eavesdropper's attack too. Hereafter, in the interest of brevity, we drop the superscript (l).

For example, we can study a channel noise (or an attack) which flips the key bits. The key is encoded in the phase difference of the corresponding time-bins of Alice and Bob in our protocol. Hence, Eve would need to flip the phase of Alice's time-bins

or Bob's time-bins. So different noise matrices that can lead to such an attack are

$$
\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}_a \otimes \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_b \quad \text{or} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_a \otimes \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}_b \quad (41)
$$

Another example is of an attack where Eve just monitors the presence of a photon in the second time-bin of Alice's signal. We can write Alice's state as

$$
|\psi\rangle_{\text{in}} = \frac{1}{\sqrt{3}} \left(|100\rangle_a + e^{i\phi_{a_1}} |011\rangle_a + e^{i\phi_{a_2}} |001\rangle_a \right) \tag{42}
$$

When Eve discovers no photon in the second time-bin, the state shown in Eq. (42) collapses to

$$
|\psi\rangle_{\text{final}} = \frac{1}{\sqrt{2}} \left(|100\rangle_a + e^{i\phi_{a_2}} |001\rangle_a \right) \tag{43}
$$

One such noise matrix that achieves this attack is

$$
E_a = \begin{pmatrix} \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} \\ 0 & 0 & 0 \\ \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} \end{pmatrix} \tag{44}
$$

From the above examples, we conclude that the elements of these noise matrices can be predicted only when we know the nature of Eve's attack and the noise in the channel. Hence, by assuming a general form for these matrices, we can find the bit and phase error rates in our protocol for any general eavesdropping strategy.

Alice and Bob measure their EPR pairs in the Z (X) basis, which acts as a stabilizer for the bit (phase) error. Thus, the probability of obtaining a bit error in the lth time-slot is,

$$
e_{\text{b}} = 1 - \frac{1}{2} \big(\langle \psi | I_{cd} \otimes Z_{A_1 B_1} \otimes I_{A_2 B_2} | \psi_{\text{out}} \rangle + \langle \psi_{\text{out}} | I_{cd} \otimes I_{A_1 B_1} \otimes Z_{A_2 B_2} | \psi_{\text{out}} \rangle \big). \tag{45}
$$

Similarly, the probability of obtaining a phase error in the lth time-slot can be expressed as,

$$
e_{\text{p}} = 1 - \frac{1}{2} \big(\langle \psi_{\text{out}} | I_{cd} \otimes X_{A_1 B_1} \otimes I_{A_2 B_2} | \psi_{\text{out}} \rangle + \langle \psi_{\text{out}} | I_{cd} \otimes I_{A_1 B_1} \otimes X_{A_2 B_2} | \psi_{\text{out}} \rangle \big). \tag{46}
$$

Using Eq. (40), we rewrite the bit error rate as,

$$
\begin{aligned}
e_{\text{b}} = 1 - \frac{1}{2} \big(& \langle \psi_{\text{in}} | E^\dagger M^\dagger F_1^\dagger F_1 M E \otimes Z_{A_1 B_1} \otimes I_{A_2 B_2} | \psi_{\text{in}} \rangle \\
& + \langle \psi_{\text{in}} | E^\dagger M^\dagger F_2^\dagger F_2 M E \otimes I_{A_1 B_1} \otimes Z_{A_2 B_2} | \psi_{\text{in}} \rangle \big).
\end{aligned} \tag{47}
$$

Here, F_1 and F_2 are the filtering operators corresponding to the instances where Charles measurement and its public announcement effectively results in entangling the first and second ancilla qubits of Alice and Bob, respectively.

C.1 Decomposing $M^{(l)\dagger}F_1^{(l)\dagger}F_1^{(l)}M^{(l)}$

$|100\rangle$, $|010\rangle$ and $|001\rangle$ form an orthonormal basis for Alice's and Bob's system, where e.g. $|100\rangle$ represents a photon in the first time-bin. Using Eq. (27), for each time slot (l), we write,

$$
\begin{aligned}
M = \frac{1}{2}\Big[&\left(|100\rangle_c \langle 100|_a + |100\rangle_d \langle 100|_a \right) \otimes \left(|100\rangle_c \langle 100|_b - |100\rangle_d \langle 100|_b \right) \\
&+\left(|100\rangle_c \langle 100|_a + |100\rangle_d \langle 100|_a \right) \otimes \left(|010\rangle_c \langle 010|_b - |010\rangle_d \langle 010|_b \right) \\
&+\left(|100\rangle_c \langle 100|_a + |100\rangle_d \langle 100|_a \right) \otimes \left(|001\rangle_c \langle 001|_b - |001\rangle_d \langle 001|_b \right) \\
&+\left(|010\rangle_c \langle 010|_a + |010\rangle_d \langle 010|_a \right) \otimes \left(|100\rangle_c \langle 100|_b - |100\rangle_d \langle 100|_b \right) \\
&+\left(|010\rangle_c \langle 010|_a + |010\rangle_d \langle 010|_a \right) \otimes \left(|010\rangle_c \langle 010|_b - |010\rangle_d \langle 010|_b \right) \\
&+\left(|010\rangle_c \langle 010|_a + |010\rangle_d \langle 010|_a \right) \otimes \left(|001\rangle_c \langle 001|_b - |001\rangle_d \langle 001|_b \right) \\
&+\left(|001\rangle_c \langle 001|_a + |001\rangle_d \langle 001|_a \right) \otimes \left(|100\rangle_c \langle 100|_b - |100\rangle_d \langle 100|_b \right) \\
&+\left(|001\rangle_c \langle 001|_a + |001\rangle_d \langle 001|_a \right) \otimes \left(|010\rangle_c \langle 010|_b - |010\rangle_d \langle 010|_b \right) \\
&+\left(|001\rangle_c \langle 001|_a + |001\rangle_d \langle 001|_a \right) \otimes \left(|001\rangle_c \langle 001|_b - |001\rangle_d \langle 001|_b \right) \Big].
\end{aligned}
\tag{48}
$$

F_1 acts as identity for the measurement results which contribute towards the key. Hence, it can be expressed as,

$$
\begin{aligned}
F_1 = &|110\rangle_c \langle 110|_c \otimes |000\rangle_d \langle 000|_d + |000\rangle_c \langle 000|_c \otimes |110\rangle_d \langle 110|_d \\
&|100\rangle_c \langle 100|_c \otimes |010\rangle_d \langle 010|_d + |010\rangle_c \langle 010|_c \otimes |100\rangle_d \langle 100|_d .
\end{aligned}
\tag{49}
$$

Using Eq. (48) and Eq. (49), we get

$$
M^\dagger F_1^\dagger F_1 M = |100\rangle_a \langle 100|_a \otimes |010\rangle_b \langle 010|_b + |010\rangle_a \langle 010|_a \otimes |100\rangle_b \langle 100|_b .
\tag{50}
$$

We express Eq. (50) in the basis of $A \otimes B$. In a concise notation, we use $|a_i b_i\rangle$ to denote the basis of the system $A \otimes B$, where e.g. $|a_1 b_1\rangle$ equals $|100\rangle_a \otimes |100\rangle_b$. Using a completeness relation, we can write Eq. (50) as,

$$
M^\dagger F_1^\dagger F_1 M = |a_1 b_2\rangle \langle a_1 b_2| + |a_2 b_1\rangle \langle a_2 b_1| .
\tag{51}
$$

By defining a suitable F_2, we can write

$$
M^\dagger F_2^\dagger F_2 M = |a_1 b_3\rangle \langle a_1 b_3| + |a_3 b_1\rangle \langle a_3 b_1| .
\tag{52}
$$

C.2 Bit error rate (BER)

First, we evaluate one component of the bit error rate - $\langle \psi_{\text{in}} | E^\dagger | a_1 b_2 \rangle \langle a_1 b_2 | E \otimes Z_{A_1 B_1} \otimes I_{A_2 B_2} | \psi_{\text{in}} \rangle$. We assume that Eve acts independently on the channels connecting Alice to Charles and Bob to Charles. Hence, we can write $E = E_a \otimes E_b$. Using Eq. (33) and Eq. (34), we express $\langle \psi_{\text{in}} | E^\dagger | a_1 b_2 \rangle \langle a_1 b_2 | E \otimes Z_{A_1 B_1} \otimes I_{A_2 B_2} | \psi_{\text{in}} \rangle$ as,

$$
\sum_{|j\rangle = |0000\rangle}^{|1111\rangle} \Big(\langle a_1 b_1 | + (-1)^{j_1 + \tilde{j}_1} \langle a_2 b_2 | + (-1)^{j_2 + \tilde{j}_2} \langle a_3 b_3 |
$$
$$
+ (-1)^{\tilde{j}_1} \langle a_1 b_2 | + (-1)^{\tilde{j}_2} \langle a_1 b_3 |
$$
$$
+ (-1)^{j_1} \langle a_2 b_1 | + (-1)^{j_1 + \tilde{j}_2} \langle a_2 b_3 | + (-1)^{j_2} \langle a_3 b_1 | + (-1)^{j_2 + \tilde{j}_1} \langle a_3 b_2 | \Big)
$$
$$
\otimes \langle j_1 \tilde{j}_1 j_2 \tilde{j}_2 | E_a^\dagger \otimes E_b^\dagger | a_1 b_2 \rangle \langle a_1 b_2 | E_a \otimes E_b \otimes Z_{A_1 B_1} \otimes I_{A_2 B_2} \Big(|a_1 b_1 \rangle
$$
$$
+ (-1)^{j_1 + \tilde{j}_1} |a_2 b_2 \rangle + (-1)^{j_2 + \tilde{j}_2} |a_3 b_3 \rangle + (-1)^{\tilde{j}_1} |a_1 b_2 \rangle + (-1)^{\tilde{j}_2} |a_1 b_3 \rangle
$$
$$
+ (-1)^{j_1} |a_2 b_1 \rangle + (-1)^{j_1 + \tilde{j}_2} |a_2 b_3 \rangle + (-1)^{j_2} |a_3 b_1 \rangle + (-1)^{j_2 + \tilde{j}_1} |a_3 b_2 \rangle \Big)
$$
$$
\otimes |j_1 \tilde{j}_1 j_2 \tilde{j}_2 \rangle, \tag{53}
$$

where, $|j\rangle = |j_1 \tilde{j}_1 j_2 \tilde{j}_2\rangle$ is the state of the joint quantum memory of Alice and Bob. We define the $(a_{ij})^{\text{th}}$ matrix elements of E_a as $\langle a_i | E_a | a_j \rangle$ and the $(b_{ij})^{\text{th}}$ element of E_b as $\langle b_i | E_a | b_j \rangle$. Hence, we write Eq. (53) as,

$$
\sum_{|j\rangle = |0000\rangle}^{|1111\rangle} (-1)^{(j_1 + \tilde{j}_1)} \Big[\Big(a_{11}^* b_{21}^* + (-1)^{j_1 + \tilde{j}_1} a_{12}^* b_{22}^* + (-1)^{j_2 + \tilde{j}_2} a_{13}^* b_{23}^*
$$
$$
+ (-1)^{\tilde{j}_1} a_{11}^* b_{22}^*
$$
$$
+ (-1)^{\tilde{j}_2} a_{11}^* b_{23}^* + (-1)^{j_1} a_{12}^* b_{21}^* + (-1)^{j_1 + \tilde{j}_2} a_{12}^* b_{23}^* + (-1)^{j_2} a_{13}^* b_{21}^*
$$
$$
+ (-1)^{j_2 + \tilde{j}_1} a_{13}^* b_{22}^* \Big) \times \Big(a_{11} b_{21} + (-1)^{j_1 + \tilde{j}_1} a_{12} b_{22} + (-1)^{j_2 + \tilde{j}_2} a_{13} b_{23}
$$
$$
+ (-1)^{\tilde{j}_1} a_{11} b_{22} + (-1)^{\tilde{j}_2} a_{11} b_{23} + (-1)^{j_1} a_{12} b_{21} + (-1)^{j_1 + \tilde{j}_2} a_{12} b_{23}
$$
$$
+ (-1)^{j_2} a_{13} b_{21} + (-1)^{j_2 + \tilde{j}_1} a_{13} b_{22} \Big) \Big]. \tag{54}
$$

Eq. (54) can be factorised as,

$$
\sum_{|j\rangle = |0000\rangle}^{|1111\rangle} (-1)^{j_1 + \tilde{j}_1} \Big(a_{11}^* + (-1)^{j_1} a_{12}^* + (-1)^{j_2} a_{13}^* \Big) \Big(b_{21}^* + (-1)^{\tilde{j}_1} b_{22}^* + (-1)^{\tilde{j}_2} b_{23}^* \Big)
$$
$$
\times \Big(a_{11} + (-1)^{j_1} a_{12} + (-1)^{j_2} a_{13} \Big) \Big(b_{21} + (-1)^{\tilde{j}_1} b_{22} + (-1)^{\tilde{j}_2} b_{23} \Big), \tag{55}
$$

which further simplifies to,

$$16\Big(|a_{12}|^2 + |a_{11}|^2 - |a_{12} - a_{11}|^2\Big)\Big(|b_{22}|^2 + |b_{21}|^2 - |b_{22} - b_{21}|^2\Big). \tag{56}$$

Now, we evaluate the remaining terms of Eq. (47) and obtain the total BER in each time slot as,

$$\begin{aligned}
e_{\mathrm{b}} = 1 - \frac{16}{2 \times 144}\Bigg[&\Big(|a_{12}|^2 + |a_{11}|^2 - |a_{12} - a_{11}|^2\Big)\Big(|b_{22}|^2 + |b_{21}|^2 - |b_{22} - b_{21}|^2\Big) \\
+&\Big(|a_{21}|^2 + |a_{22}|^2 - |a_{21} - a_{22}|^2\Big)\Big(|b_{12}|^2 + |b_{11}|^2 - |b_{12} - b_{11}|^2\Big) \\
+&\Big(|a_{13}|^2 + |a_{11}|^2 - |a_{13} - a_{11}|^2\Big)\Big(|b_{33}|^2 + |b_{31}|^2 - |b_{33} - b_{31}|^2\Big) \\
+&\Big(|a_{33}|^2 + |a_{31}|^2 - |a_{33} - a_{31}|^2\Big)\Big(|b_{13}|^2 + |b_{11}|^2 - |b_{13} - b_{11}|^2\Big)\Bigg]. \tag{57}
\end{aligned}$$

C.3 Phase error rate

We begin by calculating one component of the phase error rate in the lth time slot, $\langle\psi_{\mathrm{in}}|E^\dagger |a_1 b_2\rangle \langle a_1 b_2| E \otimes X_{A_1 B_1} \otimes I_{A_2 B_2}|\psi_{\mathrm{in}}\rangle$ in this section. Similar to Eq.(55), we can factorize the phase error rate as,

$$\begin{aligned}
&(a_{11}^* - (-1)^{j_1}a_{12}^* + (-1)^{j_2}a_{13}^*)(b_{21}^* - (-1)^{\tilde{j}_1}b_{22}^* + (-1)^{\tilde{j}_2}b_{23}^*) \\
&\times\big(a_{11} + (-1)^{j_1}a_{12} + (-1)^{j_2}a_{13}\big)\big(b_{21} + (-1)^{\tilde{j}_1}b_{22} + (-1)^{\tilde{j}_2}b_{23}\big). \tag{58}
\end{aligned}$$

We use the fact that X flips the qubit $|j\rangle$, write $(-1)^{j+1}$ as $-(-1)^j$, and get the expanded value of Eq. (58) as,

$$16\Big(|a_{11}|^2 - |a_{12}|^2 + |a_{13}|^2\Big)\Big(|b_{21}|^2 - |b_{22}|^2 + |b_{23}|^2\Big). \tag{59}$$

We can also write Eq. (58) as,

$$\begin{aligned}
\big[&(a_{11}^* + (-1)^{j_1}a_{12}^* + (-1)^{j_2}a_{13}^*)(b_{21}^* + (-1)^{\tilde{j}_1}b_{22}^* + (-1)^{\tilde{j}_2}b_{23}^*) - 2((-1)^{j_1}a_{12}^*b_{21}^* \\
&+(-1)^{j_1+\tilde{j}_2}a_{12}^*b_{23}^* + (-1)^{\tilde{j}_1}a_{11}^*b_{22}^* + (-1)^{\tilde{j}_1+j_2}a_{13}^*b_{22}^*)\big](a_{11} + (-1)^{j_1}a_{12} \\
&+(-1)^{j_2}a_{13}\big)\big(b_{21} + (-1)^{\tilde{j}_1}b_{22} + (-1)^{\tilde{j}_2}b_{23}\big). \tag{60}
\end{aligned}$$

The above equation, when summed over all the possible values of $|j\rangle = |j_1 \tilde{j}_1 j_2 \tilde{j}_2\rangle$ gives

$$\begin{aligned}
&\langle\psi_{\mathrm{in}}|E^\dagger |a_1 b_2\rangle \langle a_1 b_2| E \otimes Z_{A_1 B_1} \otimes I_{A_2 B_2}|\psi_{\mathrm{in}}\rangle - \frac{2 \times 16}{2 \times 144}\Big[|a_{12}|^2\big(|b_{21}|^2 + |b_{23}|^2\big) \\
&+|b_{22}|^2\big(|a_{11}|^2 + |a_{13}|^2\big)\Big]. \tag{61}
\end{aligned}$$

Calculating the remaining three terms (cf. Eqs. (46), (51) and (52)) along the lines of Eq. (58) and Eq. (59), we get the total phase error rate as,

$$
1 - \frac{16}{2 \times 144}\Big[\big(|a_{11}|^2 - |a_{12}|^2 + |a_{13}|^2\big)\big(|b_{21}|^2 - |b_{22}|^2 + |b_{23}|^2\big)
$$
$$
+ \big(|a_{21}|^2 - |a_{22}|^2 + |a_{23}|^2\big)
$$
$$
\times \big(|b_{11}|^2 - |b_{12}|^2 + |b_{13}|^2\big)\big(|a_{11}|^2 + |a_{12}|^2 - |a_{13}|^2\big)\big(|b_{31}|^2 + |b_{32}|^2 - |b_{33}|^2\big)
$$
$$
+ \big(|a_{31}|^2 + |a_{32}|^2 - |a_{33}|^2\big)\big(|b_{11}|^2 + |b_{12}|^2 - |b_{13}|^2\big)\Big]. \tag{62}
$$

Along the lines of Eq. (61), we can express the phase error rate in terms of bit error rate as,

$$
e_{\mathrm{p}} = e_{\mathrm{b}} - \frac{2 \times 16}{2 \times 144}\Big[\big\{|a_{12}|^2\big(|b_{21}|^2 + |b_{23}|^2\big) + |b_{22}|^2\big(|a_{11}|^2 + |a_{13}|^2\big)\big\}
$$
$$
+ \big\{|a_{22}|^2\big(|b_{11}|^2
$$
$$
+ |b_{13}|^2\big) + |b_{12}|^2\big(|a_{21}|^2 + |a_{23}|^2\big)\big\} + \big\{|a_{13}|^2\big(|b_{31}|^2 + |b_{32}|^2\big)
$$
$$
+ |b_{33}|^2\big(|a_{11}|^2 + |a_{12}|^2\big)\big\} + \big\{|a_{33}|^2\big(|b_{11}|^2 + |b_{12}|^2\big)
$$
$$
+ |b_{13}|^2\big(|a_{31}|^2 + |a_{32}|^2\big)\big\}\Big]. \tag{63}
$$

From Eq. (63), we can bound the phase error in each time slot as,

$$
e_{\mathrm{p}}^{(l)} \le e_{\mathrm{b}}^{(l)}, \forall\, l. \tag{64}
$$

D Asymptotic key analysis of DPS-MDI

D.1 DPS-MDI key rate with single-photon states

We calculate the asymptotic key rate of the single-photon source based DPS-MDI, while taking into account the effects of channel loss, background counts, and misalignment errors. We model Alice's and Bob's lossy channels as beamsplitters with transmissivity η_a and η_b, respectively. After passing through the lossy channels, the joint input state of Alice and Bob (Eq. (2)) appears as a mixed state to Charles, before he carries out the beamsplitter measurement :

$$
\rho_{\mathrm{in}} = \frac{\eta_a \eta_b}{9}|\psi_{11}\rangle\langle\psi_{11}| + \frac{\eta_a(1-\eta_b)}{3}|\psi_{10}\rangle\langle\psi_{10}| + \frac{(1-\eta_a)\eta_b}{3}|\psi_{01}\rangle\langle\psi_{01}|
$$
$$
+ (1-\eta_a)(1-\eta_b)|\psi_{00}\rangle\langle\psi_{00}|, \tag{65}
$$

where,

$$|\psi_{11}\rangle = \left(|100\rangle_a + e^{i\phi_{a_1}} |010\rangle_a + e^{i\phi_{a_2}} |001\rangle_a \right)$$
$$\otimes \left(|100\rangle_b + e^{i\phi_{b_1}} |010\rangle_b + e^{i\phi_{b_2}} |001\rangle_b \right),$$

$$|\psi_{10}\rangle = \left(|100\rangle_a + e^{i\phi_{a_1}} |010\rangle_a + e^{i\phi_{a_2}} |001\rangle_a \right) \otimes |000\rangle_b,$$

$$|\psi_{01}\rangle = |000\rangle_a \otimes \left(|100\rangle_b + e^{i\phi_{b_1}} |010\rangle_b + e^{i\phi_{b_2}} |001\rangle_b \right),$$

and $\quad |\psi_{00}\rangle = |000\rangle_a \otimes |000\rangle_b.$ (66)

Here, $|\psi_{11}\rangle$ corresponds to the scenario when photons from both Alice and Bob reach the measurement unit. $|\psi_{10}\rangle$ ($|\psi_{01}\rangle$) is the joint input state of Alice and Bob when Bob's (Alice's) photon gets lost in the channel, and only Alice's (Bob's) photon reaches Charles. $|\psi_{00}\rangle$ represents the case when both Alice as well as Bob's photons get lost in the channel.

As per Eq. (27), the beamsplitter transforms $|\psi_{11}\rangle$ into

$$|\psi_{11}\rangle_{\text{out}} = \frac{1}{2} e^{i(\phi_{b_1}+\phi_{b_2})} \Big[e^{i\Delta\phi_1} \Big(|011, 000\rangle_{cd} - |010, 001\rangle_{cd}$$
$$+ |001, 010\rangle_{cd} - |000, 011\rangle_{cd} \Big)$$
$$+ e^{i\Delta\phi_2} \Big(|011, 000\rangle_{cd} + |010, 001\rangle_{cd} - |001, 010\rangle_{cd} - |000, 011\rangle_{cd} \Big)$$
$$+ e^{-i\phi_{b_1}} \Big\{ \Big(|101, 000\rangle_{cd} - |100, 001\rangle_{cd} + |001, 100\rangle_{cd} - |000, 101\rangle_{cd} \Big)$$
$$+ e^{i\Delta\phi_2} \Big(|101, 000\rangle_{cd} + |100, 001\rangle_{cd} - |001, 100\rangle_{cd} - |000, 101\rangle_{cd} \Big) \Big\}$$
$$+ e^{-i\phi_{b_2}} \Big\{ \Big(|110, 000\rangle_{cd} - |100, 010\rangle_{cd} + |010, 100\rangle_{cd} - |000, 110\rangle_{cd} \Big)$$
$$+ e^{i\Delta\phi_1} \Big(|110, 000\rangle_{cd} + |100, 010\rangle_{cd} - |010, 100\rangle_{cd} - |000, 110\rangle_{cd} \Big) \Big\} \Big]$$
$$+ \frac{1}{\sqrt{2}} e^{i(\phi_{b_1}+\phi_{b_2})} \Big[\Big(e^{-i(\phi_{b_1}+\phi_{b_2})} |200, 000\rangle_{cd} - |000, 200\rangle \Big) + e^{i(\phi_{a_1}-\phi_{b_2})}$$
$$\times \Big(|020, 000\rangle_{cd} - |000, 020\rangle_{cd} \Big) + e^{i(\phi_{a_2}-\phi_{b_1})} \Big(|002, 000\rangle - |000, 002\rangle \Big) \Big]$$
(67)

Similarly, the action of beamspitter on $|\psi_{10}\rangle$, $|\psi_{01}\rangle$ and $|\psi_{00}\rangle$ are

$$|\psi_{10}\rangle_{\text{out}} = \frac{1}{\sqrt{2}} \Big[|100, 000\rangle_{cd} + |000, 100\rangle_{cd}$$
$$+ e^{\phi_{a_1}} \Big(|010, 000\rangle_{cd} + |000, 010\rangle_{cd} \Big)$$
$$+ e^{\phi_{a_2}} \Big(|001, 000\rangle_{cd} + |000, 001\rangle_{cd} \Big) \Big],$$
(68)

$$|\psi_{10}\rangle_{\text{out}} = \frac{1}{\sqrt{2}}\Big[\ |100, 000\rangle_{cd} - |000, 100\rangle_{cd}$$
$$+ e^{\phi_{a_1}}\big(\ |010, 000\rangle_{cd} - |000, 010\rangle_{cd}\ \big)$$
$$+ e^{\phi_{a_2}}\big(\ |001, 000\rangle_{cd} - |000, 001\rangle_{cd}\ \big)\Big], \tag{69}$$
$$\text{and} \quad |\psi_{00}\rangle_{\text{out}} = |000, 000\rangle_{cd}. \tag{70}$$

Table 1 shows the instances corresponding to the successful measurement events. These outcomes correspond to successful BSMs as we have mapped the DPS-MDI to an equivalent entanglement-based protocol. The yield (Y_{11}) for our protocol is defined as the probability of a successful measurement provided both Alice and Bob send single-photon states. Using Eqs. (65)–(70), we determine the probability of a successful measurement for all the cases shown in Table 1 as,

$$Y_{11}^{c(t_1,t_2)} = (1 - p_{\text{dark}})^4 \Big[\frac{\eta_a \eta_b}{18} + p_{\text{dark}}\Big(\frac{\eta_a + \eta_b}{3} - \frac{5\eta_a \eta_b}{9}\Big) + p_{\text{dark}}^2 (1 - \eta_a)(1 - \eta_b)\Big], \tag{71}$$

where, p_{dark} is the dark count probability, and $Y_{11}^{c(t_1,t_2)}$ represents the probability that detector c clicks in time-bins 1 and 2, given that both Alice and Bob send single-photon states. We use this notation to express the probability of a successful BSM for the other cases tabulated in Table 1.

$$Y_{11}^{c(t_1,t_2)} = Y_{11}^{c(t_1,t_3)} = Y_{11}^{d(t_1,t_2)} = Y_{11}^{d(t_1,t_3)} = Y_{11}^{c(t_1),d(t_2)} = Y_{11}^{c(t_2),d(t_1)} = Y_{11}^{c(t_1),d(t_3)}$$
$$= Y_{11}^{c(t_3),d(t_1)}. \tag{72}$$

Hence, the yield (Y_{11}) is expressed as follows:

$$Y_{11} = Y_{11}^{c(t_1,t_2)} + Y_{11}^{c(t_1,t_3)} + Y_{11}^{d(t_1,t_2)} + Y_{11}^{d(t_1,t_3)} + Y_{11}^{c(t_1),d(t_2)} + Y_{11}^{c(t_2),d(t_1)}$$
$$+ Y_{11}^{c(t_1),d(t_3)} + Y_{11}^{c(t_3),d(t_1)}$$
$$= 8(1 - p_{\text{dark}})^4 \Big[\frac{\eta_a \eta_b}{18} + p_{\text{dark}}\Big(\frac{\eta_a + \eta_b}{3} - \frac{5\eta_a \eta_b}{9}\Big) + p_{\text{dark}}^2 (1 - \eta_a)(1 - \eta_b)\Big]. \tag{73}$$

There are different scenarios that lead to errors in the DPS-MDI protocol. For example, an error occurs when the detector c clicks in time-bins 1 and 2, but $\Delta\phi_1 = \pi$. In general, an error arises when clicks corresponding to a successful partial BSM occur due to background noise, but $\Delta\phi_i$ (i=1, 2) is flipped (see Table 1). Dark counts of the single-photon detectors primarily contribute to this background noise. Thus, the error rate due to background noise is given by

$$e_b' Y_{11} = 8(1 - p_{\text{dark}})^4 \Big[p_{\text{dark}}\Big(\frac{\eta_a + \eta_b}{3} - \frac{5\eta_a \eta_b}{9}\Big) + p_{\text{dark}}^2 (1 - \eta_a)(1 - \eta_b)\Big]. \tag{74}$$

We assume that the phase misalignment error is same for both $\Delta\phi_1$ and $\Delta\phi_2$, and denote this deviation of $\Delta\phi_1$ and $\Delta\phi_2$ by $\Delta\phi$. Phase misalignment error arises due to

the non-ideal nature of optical phase-locked loop and phase modulators used in the setup. Hence, considering phase misalignment errors, the total error rate is given by,

$$e_b Y_{11} = 8(1 - p_{\text{dark}})^4 \left[\frac{e_d \eta_a \eta_b}{18} + p_{\text{dark}} \left(\frac{\eta_a + \eta_b}{3} - \frac{5\eta_a \eta_b}{9} \right) + p_{\text{dark}}^2 (1 - \eta_a)(1 - \eta_b) \right],$$

(75)

where e_d is the variance of Δ_ϕ.

D.2 DPS-MDI with decoy states

Here, we calculate the parameters defined in Eq. (11). We assume an infinite number of decoy states to get an accurate estimate of these parameters. Phase randomization is integral to decoy-state analysis. A coherent state is seen as a mixture of Fock states upon phase randomization. This prevents Eve from getting information from multi-photon pulses coming from WCS. Hence, Alice and Bob prepare phase randomized weak coherent states with intensities μ_a and μ_b, respectively, of the form,

$$|e^{i\theta_a} \sqrt{\mu_a}\rangle^{(a)} \otimes |e^{i\theta_b} \sqrt{\mu_b}\rangle^{(b)}.$$

(76)

Here, θ_a and θ_b ($\in [0, 2\pi]$) are the overall randomized phases. Alice and Bob pass their coherent states through their respective delay lines. The construction of the delay line is such that a photon has an equal probability of traversing through each path of the delay line. This implies that when a coherent state $|\sqrt{\mu}\rangle$ with mean photon number μ passes through a 3-path delay line, each path has a coherent state $|\sqrt{\frac{\mu_a}{3}}\rangle$ with mean photon number $\frac{\mu}{3}$ traversing through it. Hence, the joint state after the coherent state passing through the delay line and the phase modulator is given as,

$$\left(\left| e^{i\theta_a} \sqrt{\frac{\mu_a}{3}} \right\rangle_{a_1} \left| e^{i(\phi_{a_1} + \theta_a)} \sqrt{\frac{\mu_a}{3}} \right\rangle_{a_2} \left| e^{i(\phi_{a_2} + \theta_a)} \sqrt{\frac{\mu_a}{3}} \right\rangle_{a_3} \right)$$
$$\otimes \left(\left| e^{i\theta_b} \sqrt{\frac{\mu_b}{3}} \right\rangle_{b_1} \left| e^{i(\phi_{b_1} + \theta_b)} \sqrt{\frac{\mu_b}{3}} \right\rangle_{b_2} \left| e^{i(\phi_{b_2} + \theta_b)} \sqrt{\frac{\mu_b}{3}} \right\rangle_{b_3} \right).$$

(77)

Here, $|\mu\rangle_{a_1}$ represents a coherent state traversing through path 1 of Alice's delay line (see Fig. 2). We model the lossy channels as beamsplitters and express the joint state arriving at Chales's beamsplitter as,

$$\left(\left| e^{i\theta_a} \sqrt{\frac{\eta_a \mu_a}{3}} \right\rangle_{a_1} \left| e^{i(\phi_{a_1} + \theta_a)} \sqrt{\frac{\eta_a \mu_a}{3}} \right\rangle_{a_2} \left| e^{i(\phi_{a_2} + \theta_a)} \sqrt{\frac{\eta_a \mu_a}{3}} \right\rangle_{a_3} \right)$$
$$\otimes \left(\left| e^{i\theta_b} \sqrt{\frac{\eta_b \mu_b}{3}} \right\rangle_{b_1} \left| e^{i(\phi_{b_1} + \theta_b)} \sqrt{\frac{\eta_b \mu_b}{3}} \right\rangle_{b_2} \left| e^{i(\phi_{b_2} + \theta_b)} \sqrt{\frac{\eta_b \mu_b}{3}} \right\rangle_{b_3} \right).$$

(78)

Coherent states can also be expressed as,

$$|\sqrt{\mu}\rangle = D(\sqrt{\mu})\,|0\rangle\,, \tag{79}$$

where $D(\sqrt{\mu})$ is the displacement operator, and is given as,

$$D(\sqrt{\mu}) = e^{(\sqrt{\mu}a^\dagger - \sqrt{\mu^*}a)}. \tag{80}$$

Here, a and $a^\dagger$ are annihilation and creation operators, respectively. The beamsplitter transforms $a^\dagger$ at the input mode as per Eq. (27). The output state of beamsplitter, when the input is Eq. (78) is,

$$
\left| e^{i\theta_a}\sqrt{\frac{\eta_a\mu_a}{6}} + e^{i\theta_b}\sqrt{\frac{\eta_b\mu_b}{6}} \right\rangle_{c_1}
\left| e^{i\theta_a}\sqrt{\frac{\eta_a\mu_a}{6}} - e^{i\theta_b}\sqrt{\frac{\eta_b\mu_b}{6}} \right\rangle_{d_1}
$$

$$
\otimes \left| e^{i(\phi_{a_1}+\theta_a)}\sqrt{\frac{\eta_a\mu_a}{6}} + e^{i(\phi_{b_1}+\theta_b)}\sqrt{\frac{\eta_b\mu_b}{6}} \right\rangle_{c_2}
\left| e^{i(\phi_{a_1}+\theta_a)}\sqrt{\frac{\eta_a\mu_a}{6}} \right.
$$

$$
\left. -e^{i(\phi_{b_1}+\theta_b)}\sqrt{\frac{\eta_b\mu_b}{6}} \right\rangle_{d_2}
$$

$$
\otimes \left| e^{i(\phi_{a_2}+\theta_a)}\sqrt{\frac{\eta_a\mu_a}{6}} + e^{i(\phi_{b_2}+\theta_b)}\sqrt{\frac{\eta_b\mu_b}{6}} \right\rangle_{c_3}
\left| e^{i(\phi_{a_2}+\theta_a)}\sqrt{\frac{\eta_a\mu_a}{6}} \right.
$$

$$
\left. -e^{i(\phi_{b_2}+\theta_b)}\sqrt{\frac{\eta_b\mu_b}{6}} \right\rangle_{d_3}. \tag{81}
$$

Here, $|\sqrt{\mu}\rangle_{c_1}$ denotes a coherent state of mean photon number μ hitting the detector c in time-bin t_1.

Hence, the probability of a detector clicking in a time-bin is given by,

$$
p_{c_1} = 1 - (1 - p_{\text{dark}})\exp\left(-\left| e^{i\theta_a}\sqrt{\frac{\eta_a\mu_a}{6}} + e^{i\theta_b}\sqrt{\frac{\eta_b\mu_b}{6}} \right|^2 \right),
$$

$$
p_{d_1} = 1 - (1 - p_{\text{dark}})\exp\left(-\left| e^{i\theta_a}\sqrt{\frac{\eta_a\mu_a}{6}} - e^{i\theta_b}\sqrt{\frac{\eta_b\mu_b}{6}} \right|^2 \right),
$$

$$
p_{c_2} = 1 - (1 - p_{\text{dark}})\exp\left(-\left| e^{i(\phi_{a_1}+\theta_a)}\sqrt{\frac{\eta_a\mu_a}{6}} + e^{i(\phi_{b_1}+\theta_b)}\sqrt{\frac{\eta_b\mu_b}{6}} \right|^2 \right),
$$

$$
p_{d_2} = 1 - (1 - p_{\text{dark}})\exp\left(-\left| e^{i(\phi_{a_1}+\theta_a)}\sqrt{\frac{\eta_a\mu_a}{6}} - e^{i(\phi_{b_1}+\theta_b)}\sqrt{\frac{\eta_b\mu_b}{6}} \right|^2 \right),
$$

$$
p_{c_3} = 1 - (1 - p_{\text{dark}})\exp\left(-\left| e^{i(\phi_{a_2}+\theta_a)}\sqrt{\frac{\eta_a\mu_a}{6}} + e^{i(\phi_{b_2}+\theta_b)}\sqrt{\frac{\eta_b\mu_b}{6}} \right|^2 \right),
$$

$$
p_{d_3} = 1 - (1 - p_{\text{dark}})\exp\left(-\left| e^{i(\phi_{a_2}+\theta_a)}\sqrt{\frac{\eta_a\mu_a}{6}} - e^{i(\phi_{b_2}+\theta_b)}\sqrt{\frac{\eta_b\mu_b}{6}} \right|^2 \right). \tag{82}
$$

We simplify Eq. (82) by defining following relations:

$$\mu' = \eta_a \mu_a + \eta_b \mu_b,$$
$$\Delta_\theta = \theta_a - \theta_b,$$
$$x = \sqrt{\eta_a \mu_a \eta_b \mu_b}/3,$$
$$y = (1 - p_{\text{dark}})e^{-\mu'/6}. \tag{83}$$

Here, μ' is the average number of photons reaching the measurement unit. Δ_θ denotes the phase difference between the overall random phase applied by Alice and Bob. Using Eq. (83), we simplify Eq. (82) as

$$
\begin{aligned}
p_{c_1} &= 1 - ye^{-x\,\cos\Delta_\theta}, & p_{d_1} &= 1 - ye^{x\,\cos\Delta_\theta}, \\
p_{c_2} &= 1 - ye^{-x\,\cos(\Delta_\theta+\Delta\phi_1)}, & p_{d_2} &= 1 - ye^{x\,\cos(\Delta_\theta+\Delta\phi_1)}, \\
p_{c_3} &= 1 - ye^{-x\,\cos(\Delta_\theta+\Delta\phi_2)}, & p_{d_3} &= 1 - ye^{x\,\cos(\Delta_\theta+\Delta\phi_2)}.
\end{aligned}
\tag{84}
$$

$Q_{\mu_a\mu_b}$ is the overall gain when Alice and Bob, respectively, use an average photon number of μ_a and μ_b, and a successful measurement occurs. We can express $Q_{\mu_a\mu_b}$ for our protocol as,

$$
\begin{aligned}
& p_{c_1} p_{c_2}\left(1 - p_{c_3}\right)\left(1 - p_{d_1}\right)\left(1 - p_{d_2}\right)\left(1 - p_{d_3}\right)\Big|_{\Delta\phi_1=0,\ \Delta\phi_2=0\ \text{or}\ \pi} \\
& + p_{c_1}\left(1 - p_{c_2}\right)p_{c_3}\left(1 - p_{d_1}\right)\left(1 - p_{d_2}\right)\left(1 - p_{d_3}\right)\Big|_{\Delta\phi_2=0,\ \Delta\phi_1=0\ \text{or}\ \pi} \\
& + \left(1 - p_{c_1}\right)\left(1 - p_{c_2}\right)\left(1 - p_{c_3}\right)p_{d_1} p_{d_2}\left(1 - p_{d_3}\right)\Big|_{\Delta\phi_1=0,\ \Delta\phi_2=0\ \text{or}\ \pi} \\
& + \left(1 - p_{c_1}\right)\left(1 - p_{c_2}\right)\left(1 - p_{c_3}\right)p_{d_1}\left(1 - p_{d_2}\right)p_{d_3}\Big|_{\Delta\phi_2=0,\ \Delta\phi_1=0\ \text{or}\ \pi} \\
& + p_{c_1}\left(1 - p_{c_2}\right)\left(1 - p_{c_3}\right)\left(1 - p_{d_1}\right)p_{d_2}\left(1 - p_{d_3}\right)\Big|_{\Delta\phi_1=\pi,\ \Delta\phi_2=0\ \text{or}\ \pi} \\
& + \left(1 - p_{c_1}\right)p_{c_2}\left(1 - p_{c_3}\right)p_{d_1}\left(1 - p_{d_2}\right)\left(1 - p_{d_3}\right)\Big|_{\Delta\phi_1=\pi,\ \Delta\phi_2=0\ \text{or}\ \pi} \\
& + p_{c_1}\left(1 - p_{c_2}\right)\left(1 - p_{c_3}\right)\left(1 - p_{d_1}\right)\left(1 - p_{d_2}\right)p_{d_3}\Big|_{\Delta\phi_2=\pi,\ \Delta\phi_1=0\ \text{or}\ \pi} \\
& + \left(1 - p_{c_1}\right)\left(1 - p_{c_2}\right)p_{c_3} p_{d_1}\left(1 - p_{d_2}\right)\left(1 - p_{d_3}\right)\Big|_{\Delta\phi_2=\pi,\ \Delta\phi_1=0\ \text{or}\ \pi}.
\end{aligned}
\tag{85}
$$

We substitute Eq. (83) in Eq. (85), and obtain the overall gain for a given realization of θ_a, θ_b as,

$$Q_{\mu_a\mu_b} = 4y^4[e^{2x\,\cos\Delta_\theta} + e^{-2x\,\cos\Delta_\theta} - 2ye^{x\,\cos\Delta_\theta} - 2ye^{-x\,\cos\Delta_\theta} + 2y^2]. \tag{86}$$

We should average the overall gain obtained in Eq. (86) over the random phases θ_a and θ_b. Integrating over Δ_θ for Eq. (86) gives the overall gain as,

$$Q_{\mu_a \mu_b} = 8y^4[I_0(2x) - 2yI_0(x) + y^2]. \tag{87}$$

Here, $I_0(x)$ is the modified Bessel function of the first kind. Next, we evaluate the gain of the single-photon states (Q_{11}) for our protocol. Q_{11} is the probability of a successful BSM, given that both Alice and Bob use weak coherent states with intensities μ_a and μ_b, respectively, and send single-photon pulses. We use the Poisson distribution of photon numbers in a coherent state to obtain Q_{11} as,

$$Q_{11} = \mu_a \mu_b e^{-\mu_a - \mu_b} Y_{11}, \tag{88}$$

where Y_{11} is obtained through Eq. (73).

The error rate in the sifted key is quantified by the overall QBER ($E_{\mu_a \mu_b}$). Error occurs in our protocol when correct set of detectors click in the right time-bins (see Table 1) due to dark counts even when Alice and Bob have applied wrong Δ_{ϕ_i} (i=1, 2). For example, clicking of detectors c and d when $\Delta_{\phi_1} = \pi$ leads to error. Hence, the overall QBER can be expressed as,

$$
p_{c_1} p_{c_2} \left(1 - p_{c_3}\right)\left(1 - p_{d_1}\right)\left(1 - p_{d_2}\right)\left(1 - p_{d_3}\right)\Big|_{\Delta\phi_1 = \pi, \ \Delta\phi_2 = 0 \text{ or } \pi}
$$
$$
+ p_{c_1} \left(1 - p_{c_2}\right) p_{c_3} \left(1 - p_{d_1}\right)\left(1 - p_{d_2}\right)\left(1 - p_{d_3}\right)\Big|_{\Delta\phi_2 = \pi, \ \Delta\phi_1 = 0 \text{ or } \pi}
$$
$$
+ \left(1 - p_{c_1}\right)\left(1 - p_{c_2}\right)\left(1 - p_{c_3}\right) p_{d_1} p_{d_2} \left(1 - p_{d_3}\right)\Big|_{\Delta\phi_1 = \pi, \ \Delta\phi_2 = 0 \text{ or } \pi}
$$
$$
+ \left(1 - p_{c_1}\right)\left(1 - p_{c_2}\right)\left(1 - p_{c_3}\right) p_{d_1} \left(1 - p_{d_2}\right) p_{d_3}\Big|_{\Delta\phi_2 = \pi, \ \Delta\phi_1 = 0 \text{ or } \pi}
$$
$$
+ p_{c_1} \left(1 - p_{c_2}\right)\left(1 - p_{c_3}\right)\left(1 - p_{d_1}\right) p_{d_2} \left(1 - p_{d_3}\right)\Big|_{\Delta\phi_1 = 0, \ \Delta\phi_2 = 0 \text{ or } \pi}
$$
$$
+ \left(1 - p_{c_1}\right) p_{c_2} \left(1 - p_{c_3}\right) p_{d_1} \left(1 - p_{d_2}\right)\left(1 - p_{d_3}\right)\Big|_{\Delta\phi_1 = 0, \ \Delta\phi_2 = 0 \text{ or } \pi}
$$
$$
+ p_{c_1} \left(1 - p_{c_2}\right)\left(1 - p_{c_3}\right)\left(1 - p_{d_1}\right)\left(1 - p_{d_2}\right) p_{d_3}\Big|_{\Delta\phi_2 = 0, \ \Delta\phi_1 = 0 \text{ or } \pi}
$$
$$
+ \left(1 - p_{c_1}\right)\left(1 - p_{c_2}\right) p_{c_3} p_{d_1} \left(1 - p_{d_2}\right)\left(1 - p_{d_3}\right)\Big|_{\Delta\phi_2 = 0, \ \Delta\phi_1 = 0 \text{ or } \pi}. \tag{89}
$$

Substituting Eq. (83) in Eq. (89),

$$E'_{\mu_a \mu_b} Q_{\mu_a \mu_b} = 8y^4[1 - ye^{x \cos \Delta_\theta} - ye^{-x \cos \Delta_\theta} + y^2]. \tag{90}$$

Averaging over Δ_θ in Eq. 90, we get

$$E'_{\mu_a\mu_b} Q_{\mu_a\mu_b} = 8y^4[1 - 2yI_0(x) + y^2]. \tag{91}$$

D.3 Phase randomization with post selection

As evident from Fig. 4, phase randomization leads to a high intrinsic QBER. To reduce the QBER, Alice and Bob divide the overall phase into different splices as per Eq. (13). They announce the segment that they used for phase randomization while sifting. This improved data processing [66] reduces the cost of error correction (cf. Eq. (12)).

$$I_{\text{ec}} = \sum_{m=0}^{N-1} Q^m f H(E^m) \tag{92}$$

We assume that Alice picks up one slice out of N slices randomly and Bob always select the first phase slice. Hence, for estimation the overall gain Eq. (86) needs to be averaged over Δ_θ from $\frac{m\pi}{N}$ to $\frac{(m+1)\pi}{N}$, i.e.,

$$Q^m = \frac{N}{\pi} \int_0^{\pi/N} d\theta_b \frac{1}{\pi} \int_{m\pi/N}^{(m+1)\pi/N} d\theta_a \times 4y^4 \left[e^{2x \cos\Delta_\theta} + e^{-2x \cos\Delta_\theta} \right.$$
$$\left. -2ye^{x \cos\Delta_\theta} - 2ye^{-x \cos\Delta_\theta} + 2y^2 \right]. \tag{93}$$

Similarly, we can write the QBER as

$$E'^m_{\mu_a\mu_b} Q^m_{\mu_a\mu_b} = \frac{N}{\pi} \int_0^{\pi/N} d\theta_b \frac{1}{\pi} \int_{m\pi/N}^{(m+1)\pi/N} d\theta_a \times 8y^4[1 - ye^{x \cos\Delta_\theta} - ye^{-x \cos\Delta_\theta} + y^2]. \tag{94}$$

Finally, we perform a numerical integration to evaluate the QBER.

References

1. Mayers, D.: Unconditional security in quantum cryptography. J. ACM (JACM) **48**(3), 351 (2001)
2. Lo, H.K., Chau, H.F.: Unconditional security of quantum key distribution over arbitrarily long distances. Science **283**(5410), 2050 (1999)
3. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. **85**(2), 441 (2000)
4. Gottesman, D., Lo, H.K., Lutkenhaus, N., Preskill, J.: Security of quantum key distribution with imperfect devices. In: Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on (IEEE, 2004), p. 136
5. Biham, E., Huttner, B., Mor, T.: Quantum cryptographic network based on quantum memories. Phys. Rev. A **54**(4), 2651 (1996)
6. Qi, B., Fung, C.H.F., Lo, H.K., Ma, X.: Time-shift attack in practical quantum cryptosystems. Quantum Inf. Comput. **7**(1), 73 (2007)

7. Fung, C.H.F., Qi, B., Tamaki, K., Lo, H.K.: Phase-remapping attack in practical quantum-key-distribution systems. Phys. Rev. A **75**(3), 032314 (2007)
8. Lamas-Linares, A., Kurtsiefer, C.: Breaking a quantum key distribution system through a timing side channel. Opt. Express **15**(15), 9388 (2007)
9. 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**(4), 042333 (2008)
10. Nauerth, S., Fürst, M., Schmitt-Manderbach, T., Weier, H., Weinfurter, H.: Information leakage via side channels in freespace BB84 quantum cryptography. New J. Phys. **11**(6), 065001 (2009)
11. Xu, F., Qi, B., Lo, H.K.: Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. New J. Phys. **12**(11), 113026 (2010)
12. Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J., Makarov, V.: Hacking commercial quantum cryptography systems by tailored bright illumination. Nat. Photonics **4**(10), 686 (2010)
13. Gerhardt, I., Liu, Q., Lamas-Linares, A., Skaar, J., Kurtsiefer, C., Makarov, V.: Full-field implementation of a perfect eavesdropper on a quantum cryptography system. Nat. Commun. **2**, 349 (2011)
14. Weier, H., Krauss, H., Rau, M., Fürst, M., Nauerth, S., Weinfurter, H.: Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors. New J. Phys. **13**(7), 073024 (2011)
15. Ko, H., Lim, K., Oh, J., Rhee, J.K.K.: Informatic analysis for hidden pulse attack exploiting spectral characteristics of optics in plug-and-play quantum key distribution system. Quantum Inf. Process. **15**(10), 4265 (2016)
16. Fung, C.H.F., Tamaki, K., Qi, B., Lo, H.K., Ma, X.: Security proof of quantum key distribution with detection efficiency mismatch. Quantum Inf. Comput. **9**(1), 131–165 (2009)
17. Marøy, Ø., Lydersen, L., Skaar, J.: Security of quantum key distribution with arbitrary individual imperfections. Phys. Rev. A **82**(3), 032337 (2010)
18. Kang, G.D., Zhou, Q.P., Fang, M.F.: Measurement-device-independent quantum key distribution with uncharacterized coherent sources. Quantum Inf. Process. **19**(1), 1 (2020)
19. da Silva, T.F., Xavier, G.B., Temporão, G.P., von der Weid, J.P.: Real-time monitoring of single-photon detectors against eavesdropping in quantum key distribution systems. Opt. Express **20**(17), 18911 (2012)
20. Yuan, Z., Dynes, J., Shields, A.: Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography. Appl. Phys. Lett. **98**(23), 231104 (2011)
21. Mayers, D., Yao, A.: Quantum Cryptography with Imperfect Apparatus. In: Proceedings of the 39th Annual Symposium on Foundations of Computer Science (IEEE Computer Society, USA, 1998), FOCS '98, p. 503
22. Biham, E., Boyer, M., Boykin, P.O., Mor, T., Roychowdhury, V.: A proof of the security of quantum key distribution. J. Cryptol. **19**(4), 381 (2006)
23. Gisin, N., Pironio, S., Sangouard, N.: Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier. Phys. Rev. Lett. **105**(7), 070501 (2010)
24. Curty, M., Moroder, T.: Heralded-qubit amplifiers for practical device-independent quantum key distribution. Phys. Rev. A **84**, 010304 (2011)
25. Lo, H.K., Curty, M., Qi, B.: Measurement-device-independent quantum key distribution. Phys. Rev. Lett. **108**(13), 130503 (2012)
26. Braunstein, S.L., Pirandola, S.: Side-channel-free quantum key distribution. Phys. Rev. Lett. **108**(13), 130502 (2012)
27. Wang, Q., Zhang, C.H., Luo, S., Guo, G.C.: An enhanced proposal on decoy-state measurement device-independent quantum key distribution. Quantum Inf. Process. **15**(9), 3785 (2016)
28. Wang, L., Zhou, Y.Y., Zhou, X.J., Chen, X., Zhang, Z.: New scheme for measurement-device-independent quantum key distribution. Quantum Inf. Process. **17**(9), 231 (2018)
29. Zhu, J.R., Zhu, F., Zhou, X.Y., Wang, Q.: The enhanced measurement-device-independent quantum key distribution with two-intensity decoy states. Quantum Inf. Process. **15**(9), 3799 (2016)
30. Rubenok, A., Slater, J.A., Chan, P., Lucio-Martinez, I., Tittel, W.: Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks. Phys. Rev. Lett. **111**(13), 130501 (2013)
31. Liu, Y., Chen, T.Y., Wang, L.J., Liang, H., Shentu, G.L., Wang, J., Cui, K., Yin, H.L., Liu, N.L., Li, L., et al.: Experimental measurement-device-independent quantum key distribution. Phys. Rev. Lett. **111**(13), 130502 (2013)

32. Tamaki, K., Lo, H.K., Fung, C.H.F., Qi, B.: Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw. Phys. Rev. A **85**(4), 042307 (2012)
33. Ferenczi, A.: Security proof methods for quantum key distribution protocols, University of Waterloo (2013)
34. Ma, X., Razavi, M.: Alternative schemes for measurement-device-independent quantum key distribution. Phys. Rev. A **86**(6), 062319 (2012)
35. Lin, J., Lutkenhaus, N.: Simple security analysis of phase-matching measurement-device-independent quantum key distribution. Phys. Rev. A **98**(4), 042332 (2018)
36. Ma, X., Zeng, P., Zhou, H.: Phase-matching quantum key distribution. Phys. Rev. X **8**(3), 031043 (2018)
37. Xu, F., Curty, M., Qi, B., Lo, H.K.: Measurement-device-independent quantum cryptography. IEEE J. Sel. Top. Quantum Electron. **21**(3), 148 (2014)
38. Inoue, K.: Differential phase-shift quantum key distribution systems. IEEE J. Sel. Top. Quantum Electron. **21**(3), 109 (2015)
39. Inoue, K., Waks, E., Yamamoto, Y.: Differential-phase-shift quantum key distribution using coherent light. Phys. Rev. A **68**(2), 022317 (2003)
40. Inoue, K., Waks, E., Yamamoto, Y.: Differential phase shift quantum key distribution. Phys. Rev. Lett. **89**(3), 037902 (2002)
41. Waks, E., Takesue, H., Yamamoto, Y.: Security of differential-phase-shift quantum key distribution against individual attacks. Phys. Rev. A **73**(1), 012344 (2006)
42. Wen, K., Tamaki, K., Yamamoto, Y.: Unconditional security of single-photon differential phase shift quantum key distribution. Phys. Rev. Lett. **103**(17), 170503 (2009)
43. Inamori, H., Lutkenhaus, N., Mayers, D.: Unconditional security of practical quantum key distribution. Eur. Phys. J. D **41**(3), 599 (2007)
44. Tomamichel, M., Lim, C.C.W., Gisin, N., Renner, R.: Tight finite-key analysis for quantum cryptography. Nat. Commun. **3**, 634 (2012)
45. Hayashi, M., Nakayama, R.: Security analysis of the decoy method with the Bennett-brassard 1984 protocol for finite key lengths. New J. Phys. **16**(6), 063009 (2014)
46. 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)
47. Wang, Y., Bao, W.S., Zhou, C., Jiang, M.S., Li, H.W.: Finite-key analysis of practical decoy-state measurement-device-independent quantum key distribution with unstable sources. JOSA B **36**(3), B83 (2019)
48. Ma, X., Fung, C.H.F., Razavi, M.: Statistical fluctuation analysis for measurement-device-independent quantum key distribution. Phys. Rev. A **86**(5), 052305 (2012)
49. 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)
50. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**(21), 3121 (1992)
51. Ranu, S.K., Shaw, G.K., Prabhakar, A., Mandayam, P.: Security with 3-pulse differential phase shift quantum key distribution. In: 2017 IEEE Workshop on Recent Advances in Photonics (WRAP). IEEE, pp. 1–7 (2017)
52. Diamanti, E.: Security and implementation of differential phase shift quantum key distribution systems, Stanford University (2006)
53. Shaw, G., Sridharan, S., Ranu, S., Shingala, F., Mandayam, P., Prabhakar, A.: Equivalence of space and time-bins in DPS-QKD, arXiv preprint quant-ph, arXiv:2008.03083 (2020)
54. Ou, Z.Y.J.: Multi-photon Quantum Interference. Springer, Berlin (2007)
55. Korzh, B., Walenta, N., Houlmann, R., Zbinden, H.: A high-speed multi-protocol quantum key distribution transmitter based on a dual-drive modulator. Opt. Express **21**(17), 19579–19592 (2013)
56. Scarani, V., Renner, R.: Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way postprocessing. Phys. Rev. Lett. **100**(20), 200501 (2008)
57. 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
58. 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
59. Kahn, J., Kasper, B., Pollock, K.: Optical phaselock receiver with multigigahertz signal bandwidth. Electron. Lett. **25**(10), 626 (1989)

60. Kazovsky, L.G.: Decision-driven phase-locked loop for optical homodyne receivers: performance analysis and laser linewidth requirements. IEEE Trans. Electron Devices **32**(12), 2630 (1985)
61. Ferrero, V., Camatel, S.: Optical phase locking techniques: an overview and a novel method based on single side sub-carrier modulation. Opt. Express **16**(2), 818 (2008)
62. Renner, R., Konig, R.: Quantum cryptography and universal composability-universally composable privacy amplification against quantum adversaries. Lecture Notes Comput. Sci. **3378**, 407 (2005)
63. Ben-Or, M., Horodecki, M., Leung, D.W., Mayers, D., Oppenheim, J.: The universal composable security of quantum key distribution. In: Theory of Cryptography Conference. Springer, pp. 386–406 (2005)
64. Devetak, I.: Proceedings of the Royal Society A **461**, 207 (2005)
65. Renner, R.: Security of quantum key distribution. Int. J. Quantum Inf. **6**(01), 1 (2008)
66. Ma, X., Lutkenhaus, N.: Improved data post-processing in quantum key distribution and application to loss thresholds in device independent QKD. Quantum Inf. Comput. **12**(3–4), 203–214 (2012)