Differential phase encoded measurement-device-independent quantum key distribution

Shashank Kumar Ranu, Anil Prabhakar, and Prabha Mandayam

Department of Electrical Engineering, Indian Institute of Technology Madras, Chennai, India
Department of Physics, Indian Institute of Technology Madras, Chennai, India

We present a novel phase-based encoding scheme for measurement-device-independent quantum key distribution (MDI-QKD). This protocol uses single photons in a linear superposition of three orthogonal states, for generating the key. These orthogonal states correspond to the three distinct paths in delay line interferometers used by two (trusted) sources. The key information is decoded 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 to phase fluctuations, and also ensures protection against detector side-channel attacks. We obtain the secure key rate for our protocol and show that it compares well to existing protocols in the asymptotic regime. We also prove unconditionally security by demonstrating an equivalent protocol involving shared entanglement between the two trusted parties. Finally, we bridge the gap between theory and practice by quantifying the performance of the proposed protocol in the finite-key regime.

I. INTRODUCTION

Quantum key distribution (QKD) is proven to be unconditionally secure in theory [1–5]. However, QKD protocols maybe rendered insecure in practice, because of the difference in the behavior of practical devices and their theoretical models used in security proofs. For example, the standard protocols and their security proofs fail to take into account side-channel attacks on the detectors [6–14], 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 [15, 16]. However, the complex nature of devices makes this approach very challenging to realize in practice. The other solution is to develop counter measures against the known side-channel attacks [17, 18], but the QKD system still remains vulnerable to unanticipated attacks. Device independent QKD (DI-QKD) [19, 20] is another viable candidate against side-channel attacks. The security of DI-QKD relies on the violations of Bell inequality. However, the requirement of loophole-free Bell test and an extremely low key rate at long distances makes this unfeasible with current technology [21, 22].

Measurement-device-independent QKD (MDI-QKD) [23] 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 the usual steps of 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 [23]. MDI protocols employing time-bin [24, 25] and phase-based encodings [26, 27] also exist in the literature – see [30] 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-shift MDI-QKD (DPS MDI-QKD) scheme, as a potential candidate for alleviating random phase and polarization fluctuations. In a differential phase encoded QKD protocol, the classical key is encoded in the phase difference between successive pulses generated by a source thereby canceling the effects of phase and polarization fluctuations. There are a few variants of differential-phase-shift keying proposed in the literature [31]. For example, the sender Alice could use a phase modulator in combination with a random number generator to apply a random phase of either 0 or \( \pi \), on a sequence of successive pulses generated by a weak coherent source [32]. Alternately, the phase modulation maybe done on a single photon pulse converted into a superposition of three orthogonal states corresponding to different time-bins, via a delay line interferometer [33].

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 [34], the single-photon based 3-pulse protocol is shown to be unconditionally secure [35]. 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.

Finite-key analysis of QKD protocols has attracted a lot of attention in the past decade. Effect of the finiteness of the key size on security parameters was first studied in [36]. Security of BB84 [37] and decoy state protocols [38, 40] against collective attacks in the finite-key regime has been established. Techniques used for finite-key analysis of conventional QKD have also been applied to MDI-QKD, for specific attacks [41]. More recently, a rigorous security proof of MDI-QKD against general attacks for a finite key length has been demonstrated [42].

In this paper, we present a measurement-device-
independent QKD scheme which incorporates the advantages of differential phase encoding. We show that our scheme offers better security in the asymptotic regime, and present a security proof in the finite-key regime as well. The rest of the paper is organized as follows. In Sec. II we briefly review the 3-pulse DPS-QKD protocol and its security aspects. We discuss our DPS-MDI protocol in Sec. III and obtain the secure key rate. We show that it maps to an entanglement-based protocol in Sec. IV A and finally present the finite-key analysis in Sec. IV.

II. PRELIMINARIES

Starting with the original proposal to implement the well known B92 protocol [43], differential-phase or distributed-phase protocols have been well studied in the QKD literature [31]. Such protocols are popular because they are relatively easy to implement (compared to polarization-based protocols) and are more robust to phase and polarization fluctuations. While the majority of the phase-based schemes use weak coherent pulses for encoding the key, here we use the single-photon scheme proposed in [33]. We shall henceforth refer to this scheme as the 3-pulse DPS-QKD protocol and provide a brief description below.

A. 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 pulses in the 3-pulse train. See Fig. 1 for a schematic of the full set-up. Alice encodes her random key bit \( \{0, 1\} \) as a random phase \( \{0, \pi\} \) 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.

\[
|\psi(\pm, \pm)\rangle = \frac{1}{\sqrt{3}} (|1\rangle_1|0\rangle_2|0\rangle_3 \pm |0\rangle_1|1\rangle_2|0\rangle_3 \pm |0\rangle_1|0\rangle_2|1\rangle_3 ). \quad (1)
\]

Here, \( |1\rangle \) and \( |0\rangle \) indicate the presence and absence of a photon respectively, in each of the paths labeled 1, 2, 3 in Fig. 1. The photon has an equal probability of traversing each of the paths.

Bob’s decoding setup comprises of an unbalanced Mach-Zehnder interferometer (MZI) and two single-photon detectors. The path lengths are chosen such that the longer arm of Bob’s MZI introduces a time delay \( \Delta t \) which is exactly equal to the time taken by the photon in traversing the difference in the lengths of the two successive arms of Alice’s delay line interferometer. Thus, Bob can detect the incoming photon in one of the four possible time-instances, which we label as \( t_1, t_2, t_3, t_4 \), which are separated by a time of \( \Delta t \). 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 \( \theta_{12} \) and \( \theta_{23} \) respectively (see Fig. 1). Specifically, Bob decodes the key bit associated with a given time-slot as a 0 (1) if detector \( D0 \) (\( D1 \)) 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 [32], which is a variant of the original B92 protocol [43]. In the pulse-train protocol, Alice generates a train of coherent pulses and applies a phase of 0 or \( \pi \) to the pulses randomly, to encode key bits \( \{0, 1\} \) respectively. These phase modulated pulse trains are sent to Bob, who passes the incoming pulses through
an unbalanced Mach-Zehnder interferometer (MZI). Depending upon the phase difference between two successive pulses, constructive or destructive interference happens. A measurement-device-independent QKD protocol based on the coherent-state pulse-train DPS protocol has been proposed recently [27].

We refer to [44] 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 [36] shows that the 3-pulse variant offers better security against individual attacks, in the following sense: the error rate introduced by an eavesdropper is typically higher, whereas the learning rate of the eavesdropper is typically lower for the 3-pulse protocol [44].

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 $n \geq 3$ [35]. However, while a larger $n$ achieves a higher sifted key rate per emitted photon, it also results in a lower key rate per pulse; in fact, the $n = 3$ protocol is shown to achieve the optimal secure key rate per pulse [35].

III. DPS-MDI-QKD

We now describe our measurement-device-independent QKD protocol based on the 3-pulse phase encoding scheme, using ideal single-photon sources. 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.

Firstly, the phase-independent nature of Hong-Ou-Mandel interference [16] makes it difficult to design a pulse-train protocol for ideal single-photon sources. An MDI protocol based on a two-pulse superposition has been studied in the literature [28]. However, this would require four different phase values for encoding the information, resulting in a phase-encoded version of BB84. Using only two phase values ($0$ and $\pi$) makes the states in a two-pulse protocol orthogonal, making them perfectly distinguishable [35]. Hence, we need at least 3-paths in the superposition to implement an MDI protocol using only a pair of phases $0$ and $\pi$ for the encoding.

A simple schematic is shown in Fig. 2. Alice and Bob generate single-photon pulses which are passed through their respective delay line interferometers. The splitting ratios of the beamsplitters (BSM) of the delay lines are selected such that every photon has an equal probability of traversing through each arm of the delay line. This ensures that Alice and Bob’s single-photon pulses are transformed into linear superpositions of three orthogonal states, corresponding to the three paths of their respective delay line interferometers, as described in Eq. (1). Alice and Bob then encode their random key bits $\{0, 1\}$ by assigning a relative phase difference of $\{0, \pi\}$ between two successive pulses, using their phase modulators (PM). Finally, they 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 announces as to which detector clicked ($D_c$ or $D_d$ or both) and the corresponding time-instance ($t_1$, $t_2$ or $t_3$) at which the click was observed. Based on this information, which is made public by Charles, Alice and Bob perform sifting and extract the sifted key. The sifting and reconciliation step is explained in detail in the following section.

A. 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,

$$|\psi(\phi_{a_1}, \phi_{a_2}, \phi_{b_1}, \phi_{b_2}) \rangle_{in} = \frac{1}{\sqrt{3}} \left( |1^{(a)}\rangle_{1} |0^{(a)}\rangle_{2} |0^{(a)}\rangle_{3} + e^{i\phi_{a_1}} |0^{(a)}\rangle_{1} |1^{(a)}\rangle_{2} |0^{(a)}\rangle_{3} + e^{i\phi_{a_2}} |0^{(a)}\rangle_{1} |0^{(a)}\rangle_{2} |1^{(a)}\rangle_{3} \right)$$
As before, \( |1\rangle \) and \(|0\rangle\) indicate the presence or absence of a photon in a particular path, and the subscripts 1, 2, 3 label the different possible paths of Alice and Bob’s delay lines respectively. Thus, \(|1(a)\rangle_1|0(a)\rangle_2|0(a)\rangle_3\) is the 3-pulse state corresponding to the photon traversing path 1\(_a\) in Alice’s set-up, \(|0(b)\rangle_1|1(b)\rangle_2|0(b)\rangle_3\) is a 3-pulse state corresponding to photon traversing path 2\(_b\) in Bob’s set-up, and so on.

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

\[
|\psi\rangle_{in} = \frac{1}{3} \left[ \left| 1(a) \right| \left| 1(b) \right|_t_1 \left| 0(a) \right| \left| 0(b) \right|_t_2 \left| 0(a) \right| \left| 0(b) \right|_t_3 + e^{i\phi_{a1}} \left| 0(a) \right| \left| 1(b) \right|_t_1 \left| 1(a) \right| \left| 0(b) \right|_t_2 \left| 0(a) \right| \left| 0(b) \right|_t_3 \right] \\
+ e^{i\phi_{a2}} \left| 0(a) \right| \left| 1(b) \right|_t_1 \left| 0(a) \right| \left| 0(b) \right|_t_2 \left| 1(a) \right| \left| 0(b) \right|_t_3 + e^{i\phi_{b1}} \left| 0(a) \right| \left| 0(b) \right|_t_1 \left| 0(a) \right| \left| 0(b) \right|_t_2 \left| 1(a) \right| \left| 0(b) \right|_t_3 \\
+ e^{i(\phi_{a1}+\phi_{b1})} \left| 0(a) \right| \left| 0(b) \right|_t_1 \left| 1(a) \right| \left| 1(b) \right|_t_2 \left| 0(a) \right| \left| 0(b) \right|_t_3 + e^{i(\phi_{a1}+\phi_{b2})} \left| 0(a) \right| \left| 0(b) \right|_t_1 \left| 0(a) \right| \left| 1(b) \right|_t_2 \left| 0(a) \right| \left| 0(b) \right|_t_3 \right].
\] (3)

Note that the pairs of photons that traverse through identical paths in Alice 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 \[46\] and come out of the same port of the beamsplitter. Further, recall that the action of the beamsplitter with input ports \(a, b\) and output ports \(c, d\), when there’s a photon incident on only one of the two ports is given by,

\[
\left| 1(a) \right| \left| 0(b) \right| \rightarrow \frac{1}{\sqrt{2}} \left( \left| 1(c) \right| \left| 0(d) \right| + \left| 0(c) \right| \left| 1(d) \right| \right), \\
\left| 0(a) \right| \left| 1(b) \right| \rightarrow \frac{1}{\sqrt{2}} \left( \left| 1(c) \right| \left| 0(d) \right| - \left| 0(c) \right| \left| 1(d) \right| \right). \] (4)

Using this, 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. From the form of the final state in Eq. \(A5\), we observe that depending on the values of the relative phases \(\Delta \phi_{a1} = \phi_{a1} - \phi_{b1}\) and \(\Delta \phi_{a2} = \phi_{a2} - \phi_{b2}\), Charles may have the same or different detectors click at two different time-instances.

Finally, Alice and Bob perform key reconciliation once Charles announces his measurement outcomes. Based on which detector (\(D_a\) or \(D_b\)) clicks and the time-instances \((t_1, t_2, t_3)\) corresponding to the clicks for each pair of signal states, Alice and Bob can generate the sifted key using either \(\Delta \phi_{a1}\) or \(\Delta \phi_{a2}\) as described in Table 1.

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

\[
R_{sift} = \frac{2}{3} \times \frac{2}{3} = \frac{4}{9}.
\] (5)

\[
\otimes \frac{1}{\sqrt{3}} \left( \left| 1(b) \right|_1 \left| 0(b) \right|_2 \left| 0(b) \right|_3 + e^{i\phi_{a1}} \left| 0(b) \right|_1 \left| 1(b) \right|_2 \left| 0(b) \right|_3 + e^{i\phi_{a2}} \left| 0(b) \right|_1 \left| 0(b) \right|_2 \left| 1(b) \right|_3 \right). \] (2)
Table I: Key reconciliation scheme for the proposed protocol

| Measurement outcome of Charles | Action of Alice and Bob | Requirement of bit flip |
|-------------------------------|-------------------------|------------------------|
| Det c clicks at both $t_1$ and $t_2$ | Extract key using $\Delta \phi_1$ | No |
| Det c clicks at both $t_2$ and $t_3$ | Discard the bits | - |
| Det d clicks at both $t_1$ and $t_3$ | Extract key using $\Delta \phi_2$ | No |
| Det d clicks at both $t_1$ and $t_2$ | Extract key using $\Delta \phi_1$ | No |
| Det d clicks at both $t_2$ and $t_3$ | Discard the bits | - |
| Det c clicks at $t_1$ and Det d at $t_2$ | Extract key using $\Delta \phi_1$ | No |
| Det c clicks at $t_2$ and Det d at $t_1$ | Extract key using $\Delta \phi_1$ | Yes |
| Det c clicks at $t_1$ and Det d at $t_3$ | Extract key using $\Delta \phi_2$ | Yes |
| Det c clicks at $t_3$ and Det d at $t_1$ | Extract key using $\Delta \phi_2$ | Yes |
| 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 | - |

and Bob. Therefore, the final step of this classical 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. (5) and following the standard analysis in [4], we obtain the following asymptotic secure key rate, for our MDI-DPS protocol.

$$R = R_{\text{sift}}^{\text{prac}} (1 - f(e) h(e)) .$$

(6)

Here, $R_{\text{sift}}^{\text{prac}}$ is the practical sifted key generation rate (in bits/s) and $f(e)$ represents the inefficiency of the error correction scheme employed by Alice and Bob. $R_{\text{sift}}^{\text{prac}}$ depends upon the probability of clicking of Charles’s detectors ($p_{\text{click}}$) and the repetition rate of the source ($\gamma$) as,

$$R_{\text{sift}}^{\text{prac}} = R_{\text{sift}} \gamma p_{\text{click}} .$$

(7)

Charles detectors can click either due to the signal photons or due to the background noise. The detector clicks due to background noise are referred as dark count. Hence,

$$p_{\text{click}} = p_{\text{signal}} + p_{\text{dark}} .$$

(8)

The probability of one of the detectors clicking due to the signal photons is proportional to the transmission efficiency ($T$) of the channel and Charles detection setup as,

$$T = \eta 10^{-\alpha L/10} .$$

(9)

Here, $\eta$ is the quantum efficiency of the single-photon detector of the Charles. The error rate ($e$) is determined only by the dark count and the baseline error rate ($b$) of the system as shown below.

$$e = \frac{1}{2} p_{\text{dark}} + b p_{\text{signal}} \frac{p_{\text{signal}} + p_{\text{dark}}}{p_{\text{signal}} + p_{\text{dark}}} .$$

(10)

A factor of half comes into Eq. (10) as half of the dark counts lead to correct clicking of the detectors because of the random nature of these clicks.

To get a numerical estimate of the asymptotic key rate, we now evaluate $R$ by taking the values of all the fixed parameters of the system from [45]. The detection efficiency of the single-photon detector is 10%, the loss co-efficient of channel is 0.2 dB/km and the baseline error rate is taken as 1%. $p_{\text{dark}}$ is taken as $2 \times 10^{-5}$. $\gamma$ is fixed at 10 MHz and $f(e)$ assumes a value of 1.16. We can now plot the variation in key rate with the length of the channel between Alice and Bob, as shown in Fig. 3.

Our plot compares the secure key rate obtained for our DPS-MDI-QKD with that obtained for 3-pulse DPS and the BB84 protocols. We see that the DPS-MDI protocol yields a non-zero secure key rate for much longer channel lengths, in comparison with the standard 3-pulse DPS protocol.
A. An equivalent entanglement-based protocol

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

$$|\psi\rangle_{\text{Alice}} = \frac{1}{\sqrt{3}} \sum_{k=1}^{3} a_k^\dagger |\text{vac}\rangle.$$  

(11)

Here, $a_k^\dagger$ denotes the creation operator for the photon in the $k^{th}$ time-instance. 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,

$$|\psi_j\rangle_{\text{Alice}} = \frac{1}{\sqrt{3}} \left( a_1^\dagger |\text{vac}\rangle + \sum_{k=2}^{3} (-1)^{j_k} a_k^\dagger |\text{vac}\rangle \right),$$  

(12)

where $j_k = \sum_{l=1}^{k-1} j_l$. Alice prepares and stores 2 qubits corresponding to each encoded block in her quantum memory, which are entangled with the encoded block as follows,

$$|\psi_j\rangle_{\text{Alice}} = \frac{1}{2} \sum_{j=0}^{3} (|j_1\rangle_{A_1} |j_2\rangle_{A_2} ) \otimes |\psi_j\rangle_{\text{Alice}}.$$  

(13)

Bob also carries out a similar encoding procedure as Alice to get his own register of qubits entangled with his encoding blocks. Along the lines of Eqs. (12) and (13), Bob’s state is written as,

$$|\psi_j\rangle_{\text{Bob}} = \frac{1}{2} \sum_{j=0}^{3} (|\tilde{j}_1\rangle_{B_1} |\tilde{j}_2\rangle_{B_2} ) \otimes |\psi_j\rangle_{\text{Bob}},$$  

(14)

where $\tilde{j}$ is the random 2-bit integer 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-instance. He sends the rest through his beamsplitter. Then publicly announces the time instance (say $k = 1, 2, 3$), as well as the detector $(D_c$ or $D_d)$, at which the photon was detected. As explained in Table I in Sec. [11] based upon Charles’s 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 $\Delta \phi_1$, Alice and Bob retain their corresponding ancilla qubits ($A_i$ and $B_i$, respectively) and discard the other ancilla qubit. As shown in Appendix [12] for those time-instances when they do not need to carry-out a bit flip operation, they share a perfectly correlated entangled state

$$|0\rangle_{A_i} |0\rangle_{B_i} - |1\rangle_{A_i} |1\rangle_{B_i}.$$  

On the other hand, corresponding to those time-instances when they execute a
bit-flip to extract the shared key, they share the anticorrelated Bell state \( \frac{1}{\sqrt{2}}[|0\rangle_A |1\rangle_{B_i} - |1\rangle_A |0\rangle_{B_i}] \). A detailed discussion of the joint state after Charles’ measurement and key-reconciliation can be found in Appendix B.

**FIG. 4:** Practical implementation of DPS-MDI-QKD.

### B. Finite key analysis

Finiteness of 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 the finite number of signal exchanges between Alice and Bob.

A perfect key is a uniformly distributed bit string, having no dependence on adversary’s knowledge. Practical keys deviate from this ideal scenario, and this deviation is captured by a parameter \( \varepsilon \), interpreted as the maximum probability of a practical key differing from a completely random bit string. Following [50, 51], we say that a key \( K \) is \( \varepsilon \)-secure with respect to an eavesdropper \( E \) if,

\[
\frac{1}{2} \| \rho_{KE} - \tau_K \otimes \rho_E \|_1 \leq \varepsilon.
\]

Here, \( \rho_{KE} \) is the joint state of the ‘key system’ \( K \) and the adversary \( E \), and \( \tau_K \) is the completely mixed state on \( K \).

In the asymptotic case, for any QKD protocol involving Alice and Bob sharing entangled pairs, under the assumption of collective attacks, the secure key rate \( R \) can be bounded as [1, 3, 52],

\[
R = H(X \mid E) - H(X \mid Y) - \text{leak}_{EC} - \Delta / n.
\]

Here \( X \) and \( Y \) represent Alice and Bob’s key systems respectively, \( E \) represents the eavesdropper, and \( H(\cdot \mid \cdot) \) is the conditional von Neumann entropy. Intuitively, Eq. (16) 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 [53],

\[
H(\bar{X} \mid \bar{E}) = 1 - h(e_b),
\]

where \( e_b \) is the bit error rate.

We follow the finite-key analysis presented in [53, 54], 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 Sec. IV A above. The generalized form of Eq. (16) in the finite-key regime can be expressed as [54],

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

where \( H_{\xi}(X \mid E) \) is the conditional smooth-min entropy, \( \text{leak}_{EC} \) is the number of bits needed to be shared over a classical channel for error correction and \( \Delta \) is as shown below,

\[
\Delta = 2 \log_2 \left[ \frac{1}{2(\varepsilon - \bar{\varepsilon} - \varepsilon_{EC})} \right] + 7 \sqrt{n \log_2(2/(\varepsilon - \bar{\varepsilon}))}
\]
where $\xi$ Eq. (17) translates to, asymptotic value of $H$. S. Nauerth, M. F"urst, T. Schmitt-Manderbach, H. Weier, Here, $\varepsilon_{EC}$ 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 3 of [54].

We calculate $H_\xi(X \mid E)$ for our protocol using the asymptotic value of $H(X \mid E)$. In the finite-key regime Eq. (17) translates to,

$$H_\xi(X \mid E) = 1 - h(\tilde{\varepsilon}_b),$$

where $\xi$ is a non-negative parameter (Lemma 3 of [54] given by,

$$\xi = \sqrt{\frac{2\ln(1/\varepsilon') + d\ln(m + 1)}{m}}.$$ (21)

The bit error rate in finite-key regime is expressed as $\tilde{\varepsilon}_b = \varepsilon_b + \xi(m, d = 2)$, where $m$ is the number of bits used in parameter estimation and $d$ is the number of possible POVM outcomes. Using Eqs. (19), (20), and (21) we may estimate the sifted key rate as described in Eq. (18). The performance of a practical error correcting code as analyzed in [54] gives leak$_{EC}/n = 1.2h(Q)$, where, $Q$ is the quantum bit error rate (QBER). This helps in estimating the second term of Eq. (18). $(N, \varepsilon, \text{leak}_{EC}, \varepsilon_{EC})$ are protocol dependent parameters, whereas $n, m, \varepsilon$ and $\varepsilon'$ are selected so as to maximize the key rate per signal $(r = (n/N)r')$ under the constraints $n + m \leq N$ and $\varepsilon - \varepsilon_{EC} > \varepsilon > \varepsilon' \geq 0$.

Fig. 5 shows the variation of key rate with the number of exchanged signals for the proposed protocol. We have used $\varepsilon = 10^{-5}$, $\varepsilon_{EC} = 10^{-10}$ for generating the plots for different values of $Q$. The key rate per signal $(r)$ tends to the sifted key rate of $\frac{2}{3}$ in the asymptotic limit, as expected. This is a reflection of the fact that only $\frac{2}{3}$ of the raw key bits can be used for key generation and rest is used for parameter estimation.

V. 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 is mapped to an entanglement-based protocol. This allows us to carry out the finite-key analysis of the protocol. We further simulated the variation in key rate with the number of exchanged signals of our protocol. One interesting question that arose during this work was regarding finite-key analysis of 3-path DPS-MDI using weak coherent source. Another interesting problem that can be addressed in the future works is tightening of the bounds used in the finite-key analysis of the proposed protocol.

---

[1] D. Mayers, Journal of the ACM (JACM) 48, 351 (2001).
[2] H.-K. Lo and H. F. Chau, Science 283, 2050 (1999).
[3] P. W. Shor and J. Preskill, Physical Review Letters 85, 441 (2000).
[4] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, in Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on (IEEE, 2004) p. 136.
[5] E. Biham, B. Huttner, and T. Mor, Physical Review A 54, 2651 (1996).
[6] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, arXiv preprint quant-ph/0512080 (2005).
[7] C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, Physical Review A 75, 032314 (2007).
[8] A. Lamas-Linares and C. Kurtsiefer, Optics Express 15, 9388 (2007).
[9] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Physical Review A 78, 042333 (2008).
[10] S. Nauerth, M. Fürst, T. Schmitt-Manderbach, H. Weier, and H. Weinfurter, New Journal of Physics 11, 065001 (2009).
[11] F. Xu, B. Qi, and H.-K. Lo, New Journal of Physics 12, 113026 (2010).
[12] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nature Photonics 4, 686 (2010).
[13] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Nature Communications 2, 349 (2011).
[14] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, New Journal of Physics 13, 073024 (2011).
[15] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, arXiv preprint arXiv:0802.3788 (2008).
[16] Ø. Marøy, L. Lydersen, and J. Skaar, Physical Review A 82, 032337 (2010).
[17] T. F. da Silva, G. B. Xavier, G. P. Temporão, and J. P. von der Weid, Optics Express 20, 18911 (2012).
[18] Z. Yuan, J. Dynes, and A. Shields, Applied Physics Letters 98, 231104 (2011).
Appendix A: Analysis of DPS-MDI-QKD protocol

FIG. 6: a and b are the input ports of the beamsplitter. The output ports are c and d.
We start with the form of the input to Charles' beamsplitter given in Eq. (3):

$$|\psi\rangle_{in} = \frac{1}{3} \left[ |1\rangle_{a} |1\rangle_{b} |0\rangle_{2} |0\rangle_{3} + e^{i\phi_{a1}} |0\rangle_{a} |1\rangle_{b} |1\rangle_{t1} |1\rangle_{b} |0\rangle_{3} + e^{i\phi_{a2}} |0\rangle_{a} |0\rangle_{b} |1\rangle_{t2} |0\rangle_{b} |0\rangle_{3} + e^{i\phi_{b1}} |1\rangle_{a} |0\rangle_{b} |0\rangle_{t2} |0\rangle_{b} |0\rangle_{3} + e^{i\phi_{b2}} |1\rangle_{a} |0\rangle_{b} |1\rangle_{t2} |0\rangle_{b} |0\rangle_{3} + e^{i\phi_{ab}} |0\rangle_{a} |0\rangle_{b} |1\rangle_{t1} |1\rangle_{b} |0\rangle_{3} + e^{i\phi_{ab}} |0\rangle_{a} |0\rangle_{b} |0\rangle_{t2} |0\rangle_{b} |0\rangle_{3} \right].$$

Eq. (A2)

The output can be further simplified as,

$$|\psi\rangle_{out} = \frac{1}{2\sqrt{6}} e^{i(\phi_{a1} + \phi_{a2})} \left[ e^{i\Delta\phi_{1}} |0\rangle_{c} |0\rangle_{d} |1\rangle_{t1} |1\rangle_{b} |0\rangle_{3} + e^{i\Delta\phi_{2}} |0\rangle_{a} |0\rangle_{b} |1\rangle_{t2} |1\rangle_{b} |0\rangle_{3} + e^{-i\phi_{a1}} \left( |1\rangle_{a} |0\rangle_{b} |0\rangle_{t2} |0\rangle_{b} |1\rangle_{3} + e^{i\Delta\phi_{2}} |0\rangle_{a} |0\rangle_{b} |1\rangle_{t2} |1\rangle_{b} |0\rangle_{3} \right) \right].$$

(A4)

Fig. [1] shows a typical 50 : 50 beamsplitter. The beamsplitter acts on the input states as shown below,

$$|1\rangle_{c} |0\rangle_{d} \rightarrow \frac{1}{\sqrt{2}} (|1\rangle_{c} |0\rangle_{d} + |0\rangle_{c} |1\rangle_{d}),$$

$$|0\rangle_{a} |1\rangle_{b} \rightarrow \frac{1}{\sqrt{2}} (|1\rangle_{c} |0\rangle_{d} - |0\rangle_{c} |1\rangle_{d}).$$

(A3)

Here, c and d are the output modes and a and b are the input modes. Applying the beamsplitter transformation to Eq. (A2), we get,

$$|\psi\rangle_{out} = \frac{1}{2\sqrt{6}} e^{i(\phi_{a1} + \phi_{a2})} \left[ e^{i\Delta\phi_{1}} |0\rangle_{c} |0\rangle_{d} |1\rangle_{t1} |1\rangle_{b} |0\rangle_{3} + e^{i\Delta\phi_{2}} |0\rangle_{a} |0\rangle_{b} |1\rangle_{t2} |1\rangle_{b} |0\rangle_{3} + e^{-i\phi_{a1}} \left( |1\rangle_{a} |0\rangle_{b} |0\rangle_{t2} |0\rangle_{b} |1\rangle_{3} + e^{i\Delta\phi_{2}} |0\rangle_{a} |0\rangle_{b} |1\rangle_{t2} |1\rangle_{b} |0\rangle_{3} \right) \right].$$

(A4)

The output can be further simplified as,

$$|\psi\rangle_{out} = \frac{1}{2\sqrt{6}} e^{i(\phi_{a1} + \phi_{a2})} \left[ e^{i\Delta\phi_{1}} |0\rangle_{c} |0\rangle_{d} |1\rangle_{t1} |1\rangle_{b} |0\rangle_{3} + e^{i\Delta\phi_{2}} |0\rangle_{a} |0\rangle_{b} |1\rangle_{t2} |1\rangle_{b} |0\rangle_{3} + e^{-i\phi_{a1}} \left( |1\rangle_{a} |0\rangle_{b} |0\rangle_{t2} |0\rangle_{b} |1\rangle_{3} + e^{i\Delta\phi_{2}} |0\rangle_{a} |0\rangle_{b} |1\rangle_{t2} |1\rangle_{b} |0\rangle_{3} \right) \right].$$

(A4)
from port reasoning can be used to complete the key reconciliation scheme as described in Table 1. For example, when Charles announces the clicking of the detector\

Similarly, clicking of the detector $D_c$ at $t_1$ and $t_2$ time-bins, this would indicate that $\Delta \phi_1$ and $\Delta \phi_2$ have taken values corresponding to Case 1 (Eq. (A6)) or Case 3 (Eq. (A8)) above. These are the only cases with terms denoting the clicking of the detector $c$ at both $t_1$ and $t_2$ time-bins. $\Delta \phi_2 = 0$ in both the cases whereas $\Delta \phi_2$ can be 0 or $\pi$. Alice and Bob therefore use $\Delta \phi_1$ to extract the key, when the detector $D_c$ clicks at the time-bins $t_1$ and $t_2$.

Similarly, clicking of the detector $D_c$ at $t_3$ and the detector $D_d$ at $t_2$ leads to Alice and Bob using $\Delta \phi_1$ for extracting the key. They also need to use a bit flip operation to get the same key bits. This is because only Eq. (A7) and Eq. (A9) have terms that correspond to the clicking of the detector $D_c$ at $t_1$ and the detector $D_d$ at $t_2$. $\Delta \phi_2$ is random whereas $\Delta \phi_1 = \pi$ in both the equations. Hence, they apply a bit flip operation to $\Delta \phi_1$ to extract the same key bits. Similar reasoning can be used to complete the key reconciliation scheme as described in Table 1.

\[
\begin{align*}
- |0(\phi_1^1)\phi_1(\phi_1^2)\phi_1(\phi_1^3)\rangle_{t_1} & \left( |0(\phi_1^1)\phi_1(\phi_1^2)\phi_1(\phi_1^3)\rangle_{t_2} + e^{i\Delta \phi_2} \left( |1(\phi_1^1)\phi_1(\phi_1^2)\phi_1(\phi_1^3)\rangle_{t_1} + |1(\phi_1^1)\phi_1(\phi_1^2)\phi_1(\phi_1^3)\rangle_{t_2} + |0(\phi_2^1)\phi_1(\phi_1^2)\phi_1(\phi_1^3)\rangle_{t_1} + |0(\phi_2^1)\phi_1(\phi_1^2)\phi_1(\phi_1^3)\rangle_{t_2} \right) \\
+ e^{-i\Delta \phi_2} \left( |1(\phi_1^1)\phi_1(\phi_1^2)\phi_1(\phi_1^3)\rangle_{t_1} + |1(\phi_1^1)\phi_1(\phi_1^2)\phi_1(\phi_1^3)\rangle_{t_2} - |0(\phi_2^1)\phi_1(\phi_1^2)\phi_1(\phi_1^3)\rangle_{t_1} - |0(\phi_2^1)\phi_1(\phi_1^2)\phi_1(\phi_1^3)\rangle_{t_2} \right) \right)
\end{align*}
\]

(A5)

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 $(\Delta \phi_1, \Delta \phi_2)$. In order 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-instances $(t_1, t_2$ or $t_3$).

**Case 1:** When both $\Delta \phi_1 = 0$ and $\Delta \phi_2 = 0$, using Eq. (A5), the two-photon state after the beamsplitter is,

\[
|\psi\rangle_{out} = \frac{1}{\sqrt{6}}e^{i(\phi_1 + \phi_2)} \left( \left( |0(t_1)1(t_2)1(t_3)\rangle_c |0(t_1)0(t_2)0(t_3)\rangle_d - |0(t_1)0(t_2)0(t_3)\rangle_c |0(t_1)1(t_2)1(t_3)\rangle_d \right) + e^{-i\phi_1} \left( |1(t_1)0(t_2)1(t_3)\rangle_c |0(t_1)0(t_2)0(t_3)\rangle_d - |0(t_1)0(t_2)0(t_3)\rangle_c |1(t_1)0(t_2)1(t_3)\rangle_d \right) + e^{-i\phi_2} \left( |1(t_1)1(t_2)1(t_3)\rangle_c |0(t_1)0(t_2)0(t_3)\rangle_d - |0(t_1)0(t_2)0(t_3)\rangle_c |1(t_1)1(t_2)1(t_3)\rangle_d \right) \right) \]

(A6)

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

\[
|\psi\rangle_{out} = \frac{1}{\sqrt{6}}e^{i(\phi_1 + \phi_2)} \left( \left( |0(t_1)1(t_2)1(t_3)\rangle_c |0(t_1)0(t_2)0(t_3)\rangle_d - |0(t_1)0(t_2)0(t_3)\rangle_c |0(t_1)1(t_2)1(t_3)\rangle_d \right) + e^{-i\phi_1} \left( |0(t_1)1(t_2)0(t_3)\rangle_c |1(t_1)0(t_2)0(t_3)\rangle_d - |1(t_1)0(t_2)0(t_3)\rangle_c |0(t_1)1(t_2)1(t_3)\rangle_d \right) + e^{-i\phi_2} \left( |0(t_1)1(t_2)0(t_3)\rangle_c |1(t_1)0(t_2)0(t_3)\rangle_d - |1(t_1)0(t_2)0(t_3)\rangle_c |0(t_1)1(t_2)1(t_3)\rangle_d \right) \right) \]

(A7)

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

\[
|\psi\rangle_{out} = \frac{1}{\sqrt{6}}e^{i(\phi_1 + \phi_2)} \left( \left( |0(t_1)0(t_2)1(t_3)\rangle_c |0(t_1)1(t_2)0(t_3)\rangle_d - |0(t_1)1(t_2)0(t_3)\rangle_c |0(t_1)0(t_2)1(t_3)\rangle_d \right) + e^{-i\phi_1} \left( |0(t_1)1(t_2)0(t_3)\rangle_c |1(t_1)0(t_2)0(t_3)\rangle_d - |1(t_1)0(t_2)0(t_3)\rangle_c |0(t_1)1(t_2)1(t_3)\rangle_d \right) + e^{-i\phi_2} \left( |1(t_1)1(t_2)0(t_3)\rangle_c |0(t_1)0(t_2)0(t_3)\rangle_d - |0(t_1)0(t_2)0(t_3)\rangle_c |1(t_1)1(t_2)1(t_3)\rangle_d \right) \right) \]

(A8)

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

\[
|\psi\rangle_{out} = \frac{1}{\sqrt{6}}e^{i(\phi_1 + \phi_2)} \left( \left( |0(t_1)1(t_2)0(t_3)\rangle_c |0(t_1)0(t_2)1(t_3)\rangle_d - |0(t_1)0(t_2)1(t_3)\rangle_c |0(t_1)1(t_2)0(t_3)\rangle_d \right) + e^{-i\phi_1} \left( |1(t_1)0(t_2)1(t_3)\rangle_c |0(t_1)0(t_2)0(t_3)\rangle_d - |0(t_1)0(t_2)0(t_3)\rangle_c |1(t_1)0(t_2)1(t_3)\rangle_d \right) + e^{-i\phi_2} \left( |0(t_1)1(t_2)0(t_3)\rangle_c |0(t_1)0(t_2)0(t_3)\rangle_d - |1(t_1)0(t_2)0(t_3)\rangle_c |0(t_1)1(t_2)1(t_3)\rangle_d \right) \right) \]

(A9)

We now formulate the key reconciliation scheme (see Table 1) based on Eqs. (A6)–(A9), and 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 $d$.
Appendix B: DPS-MDI as an entanglement-based protocol

We start with Eqs. (13) and (14), 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 Ai and Bi indicate the i-th qubit in their respective (ideal) quantum memories. The joint state thus reads as,

$$\psi_{\text{Alice}} \otimes \psi_{\text{Bob}} = \frac{1}{4} \sum_{j_1, j_2 \in\{0,1\}} (|j_1\rangle_A |j_2\rangle_A \otimes |\psi_1\rangle_A \otimes \sum_{j_1, j_2 \in\{0,1\}} (|\tilde{j}_1\rangle_B |\tilde{j}_2\rangle_B \otimes |\psi_2\rangle_B$$

$$= \frac{1}{4} \sum_{j_1, j_2, j_1, j_2 \in\{0,1\}} |j_1\rangle_A |\tilde{j}_1\rangle_B |j_2\rangle_A |\tilde{j}_2\rangle_B \otimes |\psi(j_1\tilde{j}_1j_2\tilde{j}_2)\rangle_{AB}. \quad (B1)$$

The state $|\psi(j_1\tilde{j}_1j_2\tilde{j}_2)\rangle_{AB}$, which eventually becomes the input to Charles’ beamsplitter, has the following form:

$$|\psi(j_1\tilde{j}_1j_2\tilde{j}_2)\rangle_{AB} = \left( a_1^\dagger b_1^\dagger + \sum_{i=1}^{2} (-1)^{j_i+\tilde{j}_i} a_{i+1}^\dagger b_{i+1}^\dagger + \sum_{i=1}^{2} (-1)^{\tilde{j}_i} d_{\tilde{i}}^\dagger a_{\tilde{i}}^\dagger b_{\tilde{i}}^\dagger$$

$$\sum_{i=1}^{2} (-1)^{j_i+\tilde{j}_i+j_\tilde{i}+\tilde{j}_\tilde{i}} d_{\tilde{i}}^\dagger a_{\tilde{i}}^\dagger b_{\tilde{i}}^\dagger - d_{\tilde{i}}^\dagger a_{\tilde{i}}^\dagger b_{\tilde{i}}^\dagger + \sum_{i=1}^{2} (-1)^{j_i+\tilde{j}_i+j_\tilde{i}+\tilde{j}_\tilde{i}} d_{\tilde{i}}^\dagger a_{\tilde{i}}^\dagger b_{\tilde{i}}^\dagger \right) |0^{(a)}0^{(b)}\rangle_{AB}. \quad (B2)$$

Here, $a_i^\dagger$ and $b_i^\dagger$ are the creation operators corresponding to a photon traversing through the i-th arm in Alice and Bob’s delay lines respectively, and $|0^{(a)}0^{(b)}\rangle_{AB}$ denotes the vacuum. 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 post-selection and discard input states which have photons arriving at the same time-instance from both Alice and Bob. As mentioned earlier, such photons do not contribute to the final key, due to Hong-Ou-Mandel interference. We thus drop terms of the form $a_i b_i^\dagger$ in Eq. (B2). When the photons arrive at different times, as represented by terms of the form $a_i^\dagger b_i$, they transform as,

$$a_i^\dagger \rightarrow \frac{1}{\sqrt{2}} (c_i^\dagger + d_i^\dagger); \quad b_i^\dagger \rightarrow \frac{1}{\sqrt{2}} (c_i^\dagger - d_i^\dagger).$$

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

$$|\Phi(j_1\tilde{j}_1j_2\tilde{j}_2)\rangle_{CD} = \frac{1}{2} \left[ (-1)^{j_1} (c_1^\dagger + d_1^\dagger)(c_2^\dagger - d_2^\dagger) + (-1)^{\tilde{j}_1}(c_3^\dagger + d_3^\dagger)(c_4^\dagger - d_4^\dagger) + (-1)^{j_2}(c_3^\dagger + d_3^\dagger)(c_4^\dagger - d_4^\dagger) \right] 0^{(a)}0^{(d)}_{CD}. \quad (B3)$$

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

$$|\chi\rangle_{A_1 A_2 B_1 B_2 CD} = \frac{1}{4} \sum_{j_1, j_2, j_\tilde{1}, j_\tilde{2} \in\{0,1\}} |\tilde{j}_1\rangle_A |j_1\rangle_B |\tilde{j}_2\rangle_A |j_2\rangle_B \otimes |\Phi(j_1\tilde{j}_1j_2\tilde{j}_2)\rangle_{CD}. \quad (B4)$$

As discussed in section IV A, 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,

$$\phi_{a_1} = j_1 \pi, \quad \phi_{a_2} = (j_2 + j_1) \pi, \quad \phi_{b_1} = \tilde{j}_1 \pi, \quad \phi_{b_2} = (\tilde{j}_2 + \tilde{j}_1) \pi.$$
For example, when Charles announces that the detector $c$ has clicked in both $t_1$ and $t_2$ bins, Eq. (B4) collapses to the post-measurement state,

$$
|\chi^{(1)}_{\text{out}}\rangle = \frac{1}{2\sqrt{6}} \left[ |0\rangle_{A_1} |0\rangle_{B_1} + |0\rangle_{A_1} |1\rangle_{B_1} + |1\rangle_{A_1} |0\rangle_{B_1} - |1\rangle_{A_1} |1\rangle_{B_1} \right]
$$

We see that in Eq. (B5), 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,

$$
|\chi^{(1)}_{\text{out}}\rangle = \frac{1}{2\sqrt{2}} \left[ |0angle_{A_1} |0\rangle_{B_1} - |1\rangle_{A_1} |1\rangle_{B_1} \right]
$$

When Charles announces that the detector $c$ clicked at $t_1$ and $d$ at $t_2$, the state presented in Eq. (B4) collapses to,

$$
|\chi^{(2)}_{\text{out}}\rangle = \frac{1}{2\sqrt{6}} \left[ |0\rangle_{A_1} |0\rangle_{B_1} + |0\rangle_{A_1} |1\rangle_{B_1} + |1\rangle_{A_1} |0\rangle_{B_1} - |1\rangle_{A_1} |1\rangle_{B_1} \right]
$$

As seen from Eq. (B7), 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.