Symmetric Incoherent Eavesdropping against MDI QKD

Arpita Maitra · Goutam Paul

Abstract In this paper, we concentrate on the very recently proposed Measurement Device Independent Quantum Key Distribution (MDI QKD) protocol by Lo, Curty and Qi (PRL, 2012). In this protocol, a secret key is established between Alice and Bob with the help of an untrusted third-party called Eve. We study how one can suitably mount a symmetric incoherent eavesdropping strategy on MDI QKD considering that Eve will not be honest. Similar to the idea of Fuchs et al. (1997), we show that inducing a disturbance $D$ on the Alice’s (or Bob’s) qubit, Eve can guess Alice’s (or Bob’s) bit with probability $\frac{1}{2} + \sqrt{D(1 - D)}$. If Eve likes to guess both the bits of Alice and Bob at the same time, then the success probability becomes $\frac{1}{4} + \frac{D}{2} + \sqrt{\frac{D}{4}}$ with an equivalent disturbance of $\Delta = 2D(1 - D)$ between Alice and Bob. We also study how well Eve can guess whether an error has been introduced between Alice and Bob due to her interaction. While in BB84, Eve can identify with certainty whether an error has been introduced because of eavesdropping, for MDI-QKD, she can only guess it with probability $\frac{1}{2} + 2D(1 - D)$.

Keywords BB84 · Eavesdropping · Entanglement Swapping · Quantum Key Distribution · Measurement Device Independence · Quantum Cryptography

Mathematics Subject Classification (2010) 94A60 · 81P94

CR Subject Classification (2012) Quantum communication and cryptography

The work of the first author was supported by the WOS-A fellowship of the Department of Science and Technology, Government of India.

This work was done in part while the second author was visiting RWTH Aachen, Germany as an Alexander von Humboldt Fellow.

Arpita Maitra
Applied Statistics Unit, Indian Statistical Institute, Kolkata 700 108, India
E-mail: arpita76b@rediffmail.com

Goutam Paul
Dept. of Computer Science and Engineering, Jadavpur University, Kolkata 700 032, India
E-mail: goutam.paul@ieee.org
1 Introduction

The idea of BB84 [1,2] protocol was initiated by Bennet and Brassard based on the seminal observation by Wiesner [15]. The BB84 protocol is used by two parties called Alice and Bob to settle on a secret classical bit-string over an insecure quantum channel where Eve, the eavesdropper, can have access. The argument behind the security of the BB84 [2] protocol is guided by the physical law that one cannot clone an unknown quantum state perfectly. This leads to the understanding that if one wants to distinguish two non-orthogonal quantum states, then obtaining any information is only possible at the expense of introducing disturbance in the state(s). As the BB84 protocol [2] exploits non-orthogonal quantum states, any kind of eavesdropping induces disturbance to the qubits communicated from Alice to Bob. Further, the disturbance caused due to Eve’s interaction can be modeled as a Binary Symmetric Channel (BSC) between Alice and Bob with some error. We use the idea of eavesdropping following [8,9] against MDI-QKD and then exploit elementary combinatorial techniques to obtain our results.

There are several variants of the traditional BB84 protocol [3–7,10–13] that received attention in literature. Given that BB84 is the most celebrated quantum cryptographic protocol, proposals for BB84 variants are of active interest and they come from different motivations. For example, the semiquantum protocol [4,5] considers that Bob will only have restricted capability that he can measure in a specific basis. The two-way protocol [11,12] is motivated from the idea that Alice and Bob will not discuss the basis in public for the qubits that correspond to secret key bits. The very recent proposals [6,10] are motivated from resistance against side channel attacks where they allow an untrusted party in the protocol.

To resist detector side channel attacks, Measurement Device Independent (MDI) Quantum Key Distribution (QKD) idea has been presented very recently in [10]. We will show how the idea of symmetric incoherent eavesdropping of [9] can be suitably modified to be accommodated in this scenario. As this proposal is very recent, to the best of our knowledge, such attack has not yet been studied.

In MDI QKD [10], Alice and Bob need not measure any qubit, and all the measurements are executed at Eve’s end, an untrusted third-party. Thus, for eavesdropping strategies, it is natural to consider that Eve herself will try to gather information about the secret key while assisting Alice and Bob. That is why, this attack can be termed as third-party attack. While the idea of [6] uses entanglement swapping [16] for building the protocol, it is interesting to note that we exploit this for third-party eavesdropping against MDI QKD [10]. The application of entanglement swapping is evident in such protocols (either in design or in analysis) due to the involvement of the third-party.

In this paper, we build on the basic idea of eavesdropping strategy explained in [9] on the traditional BB84 [2] protocol. In MDI QKD [10], Alice and Bob send their respective qubits to Eve. Eve, while pretending to support the protocol, may not be honest and may try to extract some information regarding the bits to be decided by Alice and Bob. In quantum scenario, any attempt by Eve, to interact with the qubits sent by Alice and Bob and further to extract additional information, will induce an error between Alice and Bob. We first show that an eavesdropping strategy similar to [9] can be mounted on the qubits of either Alice or Bob so that introducing a disturbance $D$, Eve can guess the respective bit with a success probability $\frac{1}{2} + \sqrt{D(1-D)}$. Further, we show that the attack can be...
Symmetric Incoherent Eavesdropping against MDI QKD

Extended on both the qubits of Alice and Bob to obtain a success probability \(\frac{1}{4} + \frac{1}{2} + \frac{\sqrt{3}}{2}\) with an equivalent disturbance \(\Delta = 2D(1 - D)\). We note that Eve’s capability to identify the bits where error had been introduced (or not) is reduced in MDI QKD as compared to BB84.

2 Description of MDI QKD [10]

To understand this algorithm, we need to use Bell states. These are two-qubit entangled states that can form orthogonal basis. The four Bell states can be written as \(|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}([00] \pm [11])\), \(|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}([01] \pm [10])\).

1 Alice and Bob create random bit strings at their ends and encodes the bits in either Z or X basis randomly and send those to Eve.
2 Eve receives each pair of qubits (one from Alice and one from Bob) and measures them in Bell basis\(^a\). The detection results are publicly announced.
3 for the cases where the basis of Bob and Alice match do
4   if the qubits of Alice and Bob are in Z basis and the measurement results at Eve are \(|\Psi^\pm\rangle\) then
5     One of Alice or Bob has to flip the bit;
6   end
7   if the qubits of Alice and Bob are in X basis and the measurement result at Eve is \(|\Phi^-\rangle\) or \(|\Psi^-\rangle\) then
8     One of Alice or Bob has to flip the bit;
9 end
10 Error estimation, information reconciliation (using error correcting codes) and privacy amplification are performed by Alice and Bob on the bits at their ends to obtain the final shared key bits.

Algorithm 1: A brief description of MDI QKD [10].

\(^a\) In the actual implementation, Eve can identify only two (\(|\Psi^\pm\rangle\)) of the four Bell states and that is claimed to be enough for the security proof to go through [10]. Our analysis will also go through in a similar manner in such a scenario.

<table>
<thead>
<tr>
<th>Qubits sent by Alice</th>
<th>Qubits sent by Bob</th>
<th>Probability (Eve’s end)</th>
<th>Flip</th>
</tr>
</thead>
<tbody>
<tr>
<td>[0]</td>
<td>[0]</td>
<td>(\frac{1}{2}) (\frac{1}{2}) (\frac{1}{2}) (\frac{1}{2})</td>
<td>No</td>
</tr>
<tr>
<td>[0]</td>
<td>[1]</td>
<td>0 (\frac{1}{2}) (\frac{1}{2}) (\frac{1}{2})</td>
<td>Yes</td>
</tr>
<tr>
<td>[1]</td>
<td>[0]</td>
<td>0 (\frac{1}{2}) (\frac{1}{2}) (\frac{1}{2})</td>
<td>Yes</td>
</tr>
<tr>
<td>[1]</td>
<td>[1]</td>
<td>(\frac{1}{2}) (\frac{1}{2}) (\frac{1}{2}) (\frac{1}{2})</td>
<td>No</td>
</tr>
<tr>
<td>(+)</td>
<td>(+)</td>
<td>(\frac{1}{2}) (\frac{1}{2}) (\frac{1}{2}) (\frac{1}{2})</td>
<td>No</td>
</tr>
<tr>
<td>(+)</td>
<td>(−)</td>
<td>0 (\frac{1}{2}) (\frac{1}{2}) (\frac{1}{2})</td>
<td>Yes</td>
</tr>
<tr>
<td>(−)</td>
<td>(+)</td>
<td>0 (\frac{1}{2}) (\frac{1}{2}) (\frac{1}{2})</td>
<td>Yes</td>
</tr>
<tr>
<td>(−)</td>
<td>(−)</td>
<td>(\frac{1}{2}) (\frac{1}{2}) (\frac{1}{2})</td>
<td>No</td>
</tr>
</tbody>
</table>

Table 1: Different cases in MDI QKD [10].
The untrusted third-party Eve measures the states received from Alice and Bob in this basis and informs the measurement result back to them. Towards eavesdropping, we will also study some other measurements by Eve on the qubits through which she will interact with the qubits sent by Alice and Bob. For such purposes, based on the public discussion between Alice and Bob, Eve will measure the qubits with her in proper basis. Before proceeding further, let us first explain the strategy of [10] in Algorithm 1.

We present Table 1 for understanding all the cases. When Alice and Bob generate qubits in different bases then those pairs of qubits are discarded and thus this is not shown in the table.

3 Attack Model

The eavesdropper can work on each individual qubit as well as on a set of qubits taken together. We study the first one that is called the incoherent attack, while the second one is known as the coherent attack. Another interesting issue in specifying the eavesdropping scenario is whether there will be equal error probability at Bob’s end corresponding to different bases. If this is indeed equal, then we call it symmetric and that is what we concentrate on here. It creates certain constraint on Eve in terms of extracting information from the communicated qubits. That is, as far as Alice and Bob are concerned, the interference by Eve will produce a binary symmetric channel in each case with an error probability that we will denote by $D$. There is also another model where this is not equal and then we call the eavesdropping model as asymmetric. Different error rates for different bases would be a clear indication to Alice and Bob that an eavesdropper (Eve) is interfering in the communication line. One may refer to [8] for details on this and it has been commented in the same paper that given any asymmetric attack (coherent or incoherent), one can always get a symmetric attack that can match the results of the non-symmetric strategy.

Fuchs et al. (Phy. Rev. A, 1997) [9] presented an optimal eavesdropping strategy on the four-state BB84 protocol with the qubits in $Z = \{|0\rangle, |1\rangle\}$ and $X = \{|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, - = \frac{|0\rangle - |1\rangle}{\sqrt{2}}\}$ basis. Later, Bruß (Phys. Rev. Lett., 1998) [7] described the use of the basis $\left\{\frac{|0\rangle + |1\rangle}{\sqrt{2}}, \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right\} (i = \sqrt{-1})$ along with the above two to show that the BB84 protocol with three conjugate bases (six-state protocol) provides improved security. In [14], a cryptanalytic view has been taken and it is shown that if one considers Eve’s success probability in guessing the secret key instead of the mutual information between Alice and Eve, then the security levels of the protocols have different interpretations depending on the ranges of parameters used. Motivated by [14], in this paper we take the same cryptanalytic view and consider Eve’s success probability as a measure of the protocol’s strength.

Without loss of generality, we assume throughout the paper that the qubits are sent in $Z$ basis. The analysis for the $X$ basis follows from symmetry.

3.1 Eavesdropping against BB84

Let us briefly describe the attack of [9] against BB84. Consider that Eve interacts with the qubit sent by Alice to Bob. We assume that Eve has a two-qubit initial
state $|W\rangle_A$. The unitary interactions at Eve’s end can be written as

$$
U|0\rangle_A|W\rangle_A = \sqrt{1-D}|0\rangle_A|E_{00}\rangle_A + \sqrt{D}|1\rangle_A|E_{01}\rangle_A,
$$
$$
U|1\rangle_A|W\rangle_A = \sqrt{1-D}|1\rangle_A|E_{11}\rangle_A + \sqrt{D}|0\rangle_A|E_{10}\rangle_A.
$$

(1)

where $D$ is the disturbance and $1-D$ is the fidelity and $E_{pq}$ is the state of Eve’s ancilla qubits after the interaction. This is similar to the idea of BSC in the sense that if Alice encodes 0 or 1 by a qubit and send that to Bob, then due to Eve’s interaction, an error probability $D$ is introduced in the channel. Naturally, Eve should be able to learn some information at the expense of introducing the error in between Alice and Bob.

If we rewrite the interactions expressed in [9, Equations 50-51] in our notation, we obtain the following expressions for $|E_{pq}\rangle$’s.

$$
|E_{00}\rangle_A = \sqrt{1-D}\frac{|00\rangle + |11\rangle}{\sqrt{2}} + \sqrt{D}\frac{|00\rangle - |11\rangle}{\sqrt{2}},
$$
$$
|E_{01}\rangle_A = \sqrt{1-D}\frac{|01\rangle + |10\rangle}{\sqrt{2}} - \sqrt{D}\frac{|01\rangle - |10\rangle}{\sqrt{2}},
$$
$$
|E_{10}\rangle_A = \sqrt{1-D}\frac{|01\rangle + |10\rangle}{\sqrt{2}} + \sqrt{D}\frac{|01\rangle - |10\rangle}{\sqrt{2}},
$$
$$
|E_{11}\rangle_A = \sqrt{1-D}\frac{|00\rangle + |11\rangle}{\sqrt{2}} - \sqrt{D}\frac{|00\rangle - |11\rangle}{\sqrt{2}}.
$$

(2)

Eve waits till Alice and Bob publicly share their basis and then measures the pair of qubits at her end in $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ basis. If Eve obtains $|ij\rangle$, then she guesses that Alice has sent the qubit $|i\rangle$ and Bob has received $|j\rangle$. It has been shown [9,8] that Eve can correctly guess the qubit sent by Alice and received by Bob with probability $\frac{1}{2} + \sqrt{D(1-D)}$.

For MDI QKD, we consider two attack models. In the first model, Eve eavesdrops only on one side, and in the second model, she eavesdrops on both the sides.

3.2 Eavesdropping against MDI QKD on one side

Let us first consider that Eve interacts with the qubit sent by Alice only and does not disturb the qubit communicated by Bob. The unitary interactions at Eve’s end can be written as in (1).

Now consider the case when both Alice and Bob send 0. The overall state at Eve’s end is given by

$$
(\sqrt{1-D}|0\rangle_A|E_{00}\rangle_A + \sqrt{D}|1\rangle_A|E_{01}\rangle_A)|0\rangle_B
$$
$$
= \sqrt{\frac{1-D}{2}}|E_{00}\rangle_A|\phi^+\rangle_{AB} + \sqrt{\frac{1-D}{2}}|E_{00}\rangle_A|\phi^-\rangle_{AB}
$$
$$
+ \sqrt{\frac{D}{2}}|E_{01}\rangle_A|\psi^+\rangle_{AB} - \sqrt{\frac{D}{2}}|E_{01}\rangle_A|\psi^-\rangle_{AB}.
$$

(3)
Similarly, when Alice sends 0 and Bob sends 1, the overall state at Eve’s end is given by

\[
\begin{align*}
(\sqrt{1-D}|0\rangle_A|E_{00}\rangle_A + \sqrt{D}|1\rangle_A|E_{01}\rangle_A)|1\rangle_B \\
= \sqrt{\frac{1-D}{2}}|E_{00}\rangle_A|\psi^+\rangle_{AB} + \sqrt{\frac{1-D}{2}}|E_{00}\rangle_A|\psi^-\rangle_{AB} \\
+ \frac{D}{2}|E_{01}\rangle_A|\phi^+\rangle_{AB} - \frac{D}{2}|E_{01}\rangle_A|\phi^-\rangle_{AB}.
\end{align*}
\] (4)

When Alice sends 1 and Bob sends 0, the overall state at Eve’s end is given by

\[
\begin{align*}
(\sqrt{1-D}|1\rangle_A|E_{11}\rangle_A + \sqrt{D}|0\rangle_A|E_{10}\rangle_A)|0\rangle_B \\
= \sqrt{\frac{1-D}{2}}|E_{11}\rangle_A|\psi^+\rangle_{AB} - \sqrt{\frac{1-D}{2}}|E_{11}\rangle_A|\psi^-\rangle_{AB} \\
+ \frac{D}{2}|E_{10}\rangle_A|\phi^+\rangle_{AB} + \frac{D}{2}|E_{10}\rangle_A|\phi^-\rangle_{AB}.
\end{align*}
\] (5)

When both Alice and Bob send 1, the overall state at Eve’s end is given by

\[
\begin{align*}
(\sqrt{1-D}|1\rangle_A|E_{11}\rangle_A + \sqrt{D}|0\rangle_A|E_{10}\rangle_A)|1\rangle_B \\
= \sqrt{\frac{1-D}{2}}|E_{11}\rangle_A|\phi^+\rangle_{AB} - \sqrt{\frac{1-D}{2}}|E_{11}\rangle_A|\phi^-\rangle_{AB} \\
+ \frac{D}{2}|E_{10}\rangle_A|\psi^+\rangle_{AB} + \frac{D}{2}|E_{10}\rangle_A|\psi^-\rangle_{AB}.
\end{align*}
\] (6)

3.3 Eavesdropping against MDI QKD on both the sides

We assume that Eve has two separate two-qubit initial states \(|W\rangle_A\) and \(|W\rangle_B\) respectively to interact with the qubits sent by Alice and Bob respectively. The unitary interactions at Eve’s end can be written as

\[
\begin{align*}
U|0\rangle_A|W\rangle_A &= \sqrt{1-D}|0\rangle_A|E_{00}\rangle_A + \sqrt{D}|1\rangle_A|E_{01}\rangle_A = |\tau_0\rangle_A, \\
U|1\rangle_A|W\rangle_A &= \sqrt{1-D}|1\rangle_A|E_{11}\rangle_A + \sqrt{D}|0\rangle_A|E_{10}\rangle_A = |\tau_1\rangle_A, \\
U|0\rangle_B|W\rangle_B &= \sqrt{1-D}|0\rangle_B|E_{00}\rangle_B + \sqrt{D}|1\rangle_B|E_{01}\rangle_B = |\tau_0\rangle_B, \\
U|1\rangle_B|W\rangle_B &= \sqrt{1-D}|1\rangle_B|E_{11}\rangle_B + \sqrt{D}|0\rangle_B|E_{10}\rangle_B = |\tau_1\rangle_B.
\end{align*}
\]

Note that for each \(p, q \in \{0, 1\}, |E_{pq}\rangle_B\) is exactly the same as \(|E_{pq}\rangle_A\) as given in Equation (2). Here \(|\tau_i\rangle_A, |\tau_i\rangle_B, i \in \{0, 1\}\), are three-qubit entangled states consisting of Alice’s (Bob’s) qubit and Eve’s two qubits in each case. Here we exploit the idea of entanglement swapping [16] and we get the following states for different cases.
Consider the case when both Alice and Bob send 0. The overall state at Eve’s end is given by

\[
U|0\rangle_A|W\rangle_B = (1 - D)|0\rangle_A|0\rangle_B|E_{00}\rangle_A|E_{00}\rangle_B + \sqrt{D(1 - D)}|1\rangle_A|0\rangle_B|E_{01}\rangle_A|E_{00}\rangle_B \\
+ \sqrt{D(1 - D)}|0\rangle_A|1\rangle_B|E_{00}\rangle_A|E_{01}\rangle_B + D|1\rangle_A|1\rangle_B|E_{01}\rangle_A|E_{01}\rangle_B
\]

where

\[
|F_{pqrs}\rangle = |E_{pq}\rangle_A|E_{rs}\rangle_B.
\]

Similarly, when Alice sends 0 and Bob sends 1, Eve’s state is

\[
\left(1 - D\right)|0\rangle_A|1\rangle_B|E_{01}\rangle_A|E_{10}\rangle_B + \sqrt{D(1 - D)}|1\rangle_A|0\rangle_B|E_{01}\rangle_A|E_{01}\rangle_B \\
+ \sqrt{D(1 - D)}|0\rangle_A|1\rangle_B|E_{01}\rangle_A|E_{01}\rangle_B + D|1\rangle_A|1\rangle_B|E_{01}\rangle_A|E_{10}\rangle_B
\]

Again, when Alice sends 1 and Bob sends 0, Eve’s state is

\[
\left(1 - D\right)|1\rangle_A|0\rangle_B|E_{00}\rangle_A|E_{10}\rangle_B + \sqrt{D(1 - D)}|1\rangle_A|0\rangle_B|E_{00}\rangle_A|E_{01}\rangle_B \\
+ \sqrt{D(1 - D)}|0\rangle_A|1\rangle_B|E_{01}\rangle_A|E_{01}\rangle_B + D|1\rangle_A|1\rangle_B|E_{01}\rangle_A|E_{10}\rangle_B
\]

Finally, when both Alice and Bob send 1, Eve’s state is

\[
\left(1 - D\right)|1\rangle_A|1\rangle_B|E_{11}\rangle_A|E_{11}\rangle_B + \sqrt{D(1 - D)}|1\rangle_A|1\rangle_B|E_{11}\rangle_A|E_{01}\rangle_B \\
+ \sqrt{D(1 - D)}|0\rangle_A|1\rangle_B|E_{01}\rangle_A|E_{11}\rangle_B + D|1\rangle_A|1\rangle_B|E_{01}\rangle_A|E_{11}\rangle_B
\]

We have the following result about the disturbance observed by Alice and Bob.

**Proposition 1** When Eve eavesdrops on both the sides, the effective disturbance at Alice and Bob’s end is given by \(\Delta(D) = 2D(1 - D)\).
Proof Eve measures the qubits of Alice and Bob in the Bell basis and sends the result to both Alice and Bob. When Alice and Bob sends bits in $Z$ basis and the result is $\Phi^{\pm}_{AB}$, they keep their bits; whereas if the result is $\Psi^{\pm}_{AB}$, one of them flips the bit. From Equations (7), (8), (9) and (10), the result follows. Note that for Equations (7) and (10), an error corresponds to the measurement output being $\Psi^{\pm}_{AB}$ and for Equations (8) and (9), an error corresponds to the measurement output being $\Phi^{\pm}_{AB}$. 

4 Eve’s Success Probability

According to the MDI QKD protocol described in Section 2, Eve first measures the qubits of Alice and Bob in the Bell basis and sends the result to both Alice and Bob. In our attack model, she applies the identity operators on the qubits at her disposal during this measurement. Let $M$ denote the state of Eve’s ancilla qubits after the measurement. After public communication and key establishment between Alice and Bob, Eve would again measure the state at her disposal in the computational basis. We reiterate that we only consider the case when Alice and Bob’s bases match, and without loss of generality we consider when both used $Z$ basis. Let $V$ denote the state of Eve’s ancilla qubits after the second measurement. Informally, we call it the measurement outcome in the computational basis. Let $A \in \{0, 1\}$ and $B \in \{0, 1\}$ denote the bits sent by Alice and Bob respectively. Let the guesses of Eve about what Alice and Bob sent be denoted by $G_A \in \{0, 1\}$ and $G_B \in \{0, 1\}$ respectively.

Analogous to [14, Theorem 2], we can write the following result for the optimal decision of Eve.

Proposition 2 Given an output $v$ from the measurement by Eve in the computational basis, her optimal decision is given by

$$S_{opt}(v) = \arg \max_{a,b} P(A = a, B = b \mid V = v),$$

and the corresponding optimal success probability is given by

$$P_{opt}(success) = \sum_v \max_{a,b} P(A = a, B = b, V = v),$$

where the notation $\arg \max$ denotes the particular tuple $(a_m, b_m)$ which maximizes the above conditional probability across all pairs $(a, b) \in \{0, 1\}^2$.

Basically, in each case, Eve’s optimal strategy would be to maximize the joint probability of what she observed and what Alice and Bob have sent and this maximum probability gives her optimal success probability.

4.1 Success probability for eavesdropping on one side

The attack model for this case has already been described in Section 3.2. Note that here $V \in \{0, 1\}^2$. We have the following result.
Table 2 Likelihood $P(V = v \mid A = a, B = b)$ for one-sided eavesdropping.

<table>
<thead>
<tr>
<th>$V$</th>
<th>$A = 0, B = 0$</th>
<th>$A = 0, B = 1$</th>
<th>$A = 1, B = 0$</th>
<th>$A = 1, B = 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>$(1 - D)d'$</td>
<td>$(1 - D)d'$</td>
<td>$(1 - D)d'$</td>
<td>$(1 - D)d'$</td>
</tr>
<tr>
<td>01</td>
<td>$Dd'$</td>
<td>$Dd'$</td>
<td>$Dd'$</td>
<td>$Dd'$</td>
</tr>
<tr>
<td>10</td>
<td>$Dd'$</td>
<td>$Dd'$</td>
<td>$Dd'$</td>
<td>$Dd'$</td>
</tr>
<tr>
<td>11</td>
<td>$(1 - D)d'$</td>
<td>$(1 - D)d'$</td>
<td>$(1 - D)d'$</td>
<td>$(1 - D)d'$</td>
</tr>
</tbody>
</table>

Lemma 1 The likelihoods $P(V = v \mid A = a, B = b)$, for $v \in \{0, 1\}^2$, $a, b \in \{0, 1\}$, are given as in Table 2, where $d = \frac{1}{2} + \sqrt{D(1 - D)}$ and $d' = \frac{1}{2} - \sqrt{D(1 - D)}$.

Proof The likelihood $P(V = v \mid A = a, B = b)$ can be computed as

$$
\sum_{p,q} P(M = |E_{pq}| \mid A = a, B = b)P(V = v \mid A = a, B = b, M = |E_{pq}|).
$$

In the above expression, the values of $P(M = |E_{pq}| \mid A = a, B = b)$ can be obtained directly from Equations (3), (4), (5) and (6) and $P(V = v \mid A = a, B = b, M = |E_{pq}|)$ can be directly obtained from the corresponding expressions in Equation (2).

Using Bayes’ theorem, one can compute the table for the values of $P(A = a, B = b \mid V = v)$ to obtain optimal decision.

Below we derive the success probability of Eve due to the above strategy.

Theorem 1 The optimal success probability of Eve in guessing the bit sent by Alice is given by $\frac{1}{2} + \sqrt{D(1 - D)}$.

Proof The strategy of Eve will be as follows. If Eve observes $V = 00$ or 10 (respectively $V = 01$ or 11), then she will consider Alice sent 0 (respectively 1). In this case the probability of Eve in correctly guessing Alice’s bit is $d = \frac{1}{2} + \sqrt{D(1 - D)}$. That gives the proof.

The following result is immediate as we do not have knowledge about Bob’s bit other than the random guess, i.e., Eve can guess Bob’s bit with probability $\frac{1}{4}$ only.

Corollary 1 Success probability for guessing both Alice’s and Bob’s bit is $P_1(D) = \frac{1}{2}d = \frac{1}{4} + \frac{1}{2}\sqrt{D(1 - D)}$.

4.2 Success probability for eavesdropping on two sides

Refer to Section 3.3 for the exact model of the attack. Note that here we have $V \in \{0, 1\}^4$. We begin by computing the likelihoods.

Lemma 2 The likelihoods $P(V = v \mid A = a, B = b)$, for $v \in \{0, 1\}^4$, $a, b \in \{0, 1\}$, are given as in Table 3, where $d_\pm = (\sqrt{1 - D} \pm \sqrt{D})^4$ and $d_2 = (1 - 2D)^2$.

Proof The likelihood $P(V = v \mid A = a, B = b)$ can be computed as

$$
\sum_{p,q,r,s} P(M = |F_{pqrs}| \mid A = a, B = b)P(V = v \mid A = a, B = b, M = |F_{pqrs}|).
$$

In the above expression, the values of $P(M = |F_{pqrs}| \mid A = a, B = b)$ can be obtained directly from Equations (7), (8), (9) and (10) and $P(V = v \mid A = a, B = b, M = |F_{pqrs}|)$ can be directly obtained from the corresponding expressions of $|F_{pqrs}| = |E_{pq}A|E_{rs}B$ via Equation (2).
In this case also, using Bayes’ theorem, one can calculate the values of $P(A = a, B = b | V = v)$. Theorem 2 gives the success probability of Eve due to the above strategy.

**Theorem 2** The optimal success probability of Eve in guessing a pair of bits sent by Alice and Bob is given by

$$P_2(D) = \frac{1}{4} + D(1 - D) + \sqrt{D(1 - D)}.$$

**Proof** We need to multiply each entry in Table 3 with $\frac{1}{2}$ to find out the joint probabilities. According to Proposition 2, for each possible outcome $v$, we need to find the maximum such joint probability and sum them up. In each row, we have three probabilities to compare, namely, $d_+ = (\sqrt{1 - D} + \sqrt{D})^4$, $d_- = (\sqrt{1 - D} - \sqrt{D})^4$, and $d_2 = (1 - 2D)^2$. Note that $d_+ = (\sqrt{1 - D} \pm \sqrt{D})^4 = 1 + 4D(1 - D) \pm 4\sqrt{D(1 - D)}$. For $0 \leq D \leq 1$, the last term is non-negative and so $d_+ \geq d_2$. Again, $d_2 = 1 - 4D + 4D^2 = 1 - 4D(1 - D) \leq 1 + 4D(1 - D) \leq d_+$. Adding up the maximum joint probabilities for each row, we get $\frac{1}{4} d_+$ that gives the required expression. \qed

Thus, from Proposition 1 and Theorem 2, we get the following result.

**Corollary 2** Introducing a disturbance $\Delta$, the optimal success probability of Eve in guessing a pair of bits sent by Alice and Bob is given by $\frac{1}{4} + \frac{1}{2} + \sqrt{\frac{1}{2}}$.

In Table 4, we list Eve’s optimal guesses $G_A$ and $G_B$ of what Alice and Bob sent respectively corresponding to her different measurement outcomes $V$.

4.3 Guessing the location of the errors

Consider the eavesdropping against BB84 as in (1). One may easily note that if Alice sends $|0\rangle$, then Eve will obtain either $|E_{00}\rangle$ or $|E_{01}\rangle$. The measurement is in $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ basis. Given the forms of $|E_{pq}\rangle$ as in (2), after measurement if Eve observes $|00\rangle$ or $|11\rangle$ basis, then she knows that Bob obtained $|0\rangle$, i.e., no error.
Table 4 Eve’s optimal guesses corresponding to her measurement outcomes.

Table 5 Studying the probability of Eve’s guess in correctly identifying whether error has occurred between Alice and Bob.

After estimating the bits of both Alice and Bob, and knowing the Bell states, Eve can probabilistically guess in which bit the error occurs. Let us now describe how this works.

One should have a look at the Table 1 also for the scenario when there is no eavesdropping. In our attack model, when the Bell measurement gives $\Phi^\pm$, none of Alice and Bob flips the bits. Hence, an error is introduced if one of Alice had sent 0 and the other had sent 1. So Eve can identify that an error has occurred if she
guesses one of Alice and Bob’s bits to be 0 and the other to be 1. Again, when the Bell measurement gives $\Psi^\pm$, one of Alice and Bob flips the bit. Hence, an error is introduced if both Alice and Bob had sent 0 or 1. So Eve can correctly identify the error if she guesses both Alice and Bob’s bits as 0 or 1. Thus, in both the cases, Eve’s can identify the error if she guesses both the bits correctly or both the bits wrongly. In Theorem 3, we derive the Probability of Eve’s correctly identifying the error at Alice and Bob’s ends.

**Theorem 3** Eve can guess whether an error has been introduced between Alice and Bob or not with probability $\frac{1}{2} + 2D(1 - D)$.

**Proof** Eve can correctly guess the error introduced between Alice and Bob when she guesses either both of the bits correctly or both of the bits incorrectly. Hence this probability is given by

$$\sum_{a,b} \left( P(A = a, B = b, G_A = a, G_B = b) + P(A = a, B = b, G_A = \overline{a}, G_B = \overline{b}) \right),$$

where $\overline{x}$ denotes the bit-compliment of $x$. From Table 4, we see a 1-to-1 correspondence between Eve’s guess $(G_A, G_B)$ and the measurement outcome $V$. Let $v(x, y)$ denote the outcome corresponding to the guess $G_A = x$, $G_B = y$. Thus, the above probability reduces to

$$\sum_{a,b} \left( P(A = a, B = b, V = v(a, b)) + P(A = a, B = b, V = v(\overline{a}, \overline{b})) \right).$$

From Table 3 we can easily compute the required joint probabilities and these are shown in Table 5. Thus the probability is $\frac{1}{16}(d_+ + d_+) = \frac{1}{2} + 2D(1 - D)$. $\square$

5 Discussion and Conclusion

In this paper, we have studied eavesdropping strategy on a recently proposed variant of BB84, which is refereed to as MDI QKD [10]. This variant is motivated from resistance against side channel attacks that relies on measurement device independence for the communicating parties. We analyze an existing eavesdropping strategy [9] against BB84 [2] on this MDI QKD protocol and critically compare the effectiveness of the strategy against BB84 and MDI QKD.

The difference between the attacker’s success probability and the probability of random guess gives the attacker’s advantage. In our analysis, the probability of random guess is $\frac{1}{4}$. Thus, Eve’s advantages for the one-sided and the two-sided attacks are respectively given by

$$A_1(D) = P_1(D) - \frac{1}{4} = \frac{1}{2} \sqrt{D(1 - D)} , \text{ and } A_2(D) = P_2(D) - \frac{1}{4} = D(1 - D) + \sqrt{D(1 - D)}.$$ 

In the analysis of both one-sided and two-sided eavesdropping, Eve measures all the ancilla qubits at her disposal. However, Eve may not concentrate on all the qubits. For the one-sided case, she needs to measure only the second qubit and for the two-sided case she needs to measure only the second and the fourth qubits. By forming likelihood tables corresponding to these partial measurements, it can be immediately shown that Eve arrives at the same success probabilities $P_1(D)$ and $P_2(D)$ respectively for the two attacks. Measuring the second one among the two qubits of the ancilla has already known in literature [9] and that can be followed here as well.

In two-sided eavesdropping, if Eve is interested to know only Alice’s bit, she would form a likelihood table similar to Table 3, but for the probabilities $P(V =$
By summing up the maximum joint probabilities for each row of this new table, one can easily see that the optimal success probability to guess only Alice’s bit for two-sided eavesdropping case is given by is \( \frac{1}{2} + \sqrt{D(1-D)} \), which is the same for one-sided eavesdropping as shown in Theorem 1. The same success probability is obtained for guessing only Bob’s bit in two-sided eavesdropping. It is tempting to multiply the success probabilities of two independent one-sided attacks to achieve \( \left( \frac{1}{2} + \sqrt{D(1-D)} \right)^2 = \frac{1}{4} + D(1 - D) + \sqrt{D(1-D)} \) which is the success probability for two-sided attack. However, we would like to emphasize that in presence of entanglement swapping, such independence should not be presumed. Rather, our direct derivation without any assumption brings forth an interesting observation: performing the attack on only one side is equivalent to performing the attack on both sides and then observing the result for only one side.

Apparently, the attack of [9] against BB84 protocol is sharper in the sense that both the bits of Alice and Bob could have been guessed with a probability \( d = \frac{1}{2} + \sqrt{D(1-D)} \) which is greater than \( P_1(D) \) or \( P_2(D) \). However, such a comparison is not fair, since in the attack of [9], Alice is the sender, Bob is the receiver and Eve’s only goal is to decide the bit that Alice has sent. Thus she has to guess only one bit at a time. Whereas in the current scenario, she has to guess two bits, one sent by Alice and the other sent by Bob. Definitely the latter is a more challenging case having twice as large a sample space as the former. However, if Eve does not want to know what Alice and Bob had sent individually, but she is interested only in the secret key bit established between Alice and Bob, then for MDI QKD she will perform just one-sided attack and would guess the secret key based on whether one of Alice and Bob flips the bit or not.

However, there is one aspect in which the eavesdropper has an extra advantage in traditional BB84 over MDI QKD. In BB84, Whenever Eve’s post-measurement state is \( |01\rangle \) or \( |10\rangle \), she knows with probability 1 that an error has occurred (i.e., Alice and Bob’s bits do not match), and when the state is \( |00\rangle \) or \( |11\rangle \), she knows with probability 1 that no error has occurred. But in MDI QKD, Eve cannot get any information about the location of the errors for one-sided attack. Even for two-sided attack, none of her post-measurement states tells her with certainty in which bits the errors are actually introduced. As Table 5 shows, she can get the additional information regarding the location of the bits where errors are actually introduced only with certain probabilities (and with an overall probability of \( \frac{1}{2} + 2D(1 - D) \)). In this aspect, MDI-QKD [10] leaks less information than BB84 [2].

References