Measurement-Device-Independenization of Quantum Key Distribution Protocols

Hao Shu

Abstract Quantum key distribution (QKD) allows the legitimate partner to establish a secret key whose security only depends on physical laws. In recent years, research on QKD by employing insecure measurement devices, namely measurement-device-independent QKD (MDI-QKD), is increased. MDI-QKD removes all attacks on measurement devices and thus an untrusted third party can be employed for measuring. However, a weakness of previous MDI-QKD protocols is the need for joint measurements such as Bell measurements whose efficiency is low in practice. On the other hand, can all QKD protocols become measurement-device-independent remains a problem. In this paper, we present a scheme making prepare-measure QKD protocols become MDI-QKD protocols, called ‘measurement – device – independentization’, which does not need to employ joint measurements and could be efficiently implemented by weak coherence sources. The protocol might look like the detector-device-independent (DDI) protocols but it is also secure under the Trojan horse attack. To illustrate this, we investigate the photon-number-adding (PNA) attack and present a scheme, called ‘photon – number – purification’, which can also be employed to close loopholes for previous protocols such as DDI and plug-and-play ones.

Keywords Quantum key distribution · Measurement-device-independent · Qubit · Photon number adding · Photon number purification

1 Introduction

Quantum key distribution (QKD) could be the most significant application in quantum information theory, which allows the legitimate partner to share a one-time pad with security that only depends on physical laws. In nearly
four decades, substantial QKD protocols are proposed\cite{1,2,3,7,8,9,10,11,12,13}. Traditional security analyses of QKD protocols focus on attacks on channels. However, the devices of the legitimate partner may also be insecure. To solve this problem, research on device-independent quantum key distribution (DI-QKD)\cite{2,14,15,16,17,18,19} becomes interesting. Despiteness, completed DI-QKD usually results in impractical requirements. To balance the security and the practice, measurement-device-independent quantum key distribution (MDI-QKD) appears.

The setting of MDI-QKD is that QKD protocols are implemented by insecure measurement devices, namely it might send the measurement outcomes to an eavesdropper, might employ a different measurement instead of the required one, might provide a fake outcome, and so on. In the worst case, the measurement might be totally controlled by the eavesdropper who can do whatever can be done under physical laws to obtain the best interests. Therefore, an MDI-QKD can be simply understood as a QKD in which measurements are provided by an untrusted third party. The first MDI-QKD protocol\cite{20} was published in 2012, in which respectively, the legitimate partner randomly chooses one of the two BB84 bases and sends one of the states randomly to an untrusted third party for measuring via a Bell measurement, for each bit. If their bases agree, they can know whether the states they prepared are the same or different. Since they know the bit they prepared, respectively, they can learn the other one and thus agree with a key, while the third party only knows whether they have the same bits but does not learn what they are, and thus their key is private for the party. After the protocol was published, several relative works followed\cite{21,22,23,24,25}. In 2018, the idea of twin-field QKD\cite{27} was proposed, which might overcome traditional limitations of distance\cite{28,29}. Inspired by it, other QKD protocols appeared\cite{30,31}.

A weakness of all such MDI-QKD protocols is the need for joint measurements such as Bell measurements which are lowly efficient in practice, while a completed Bell measurement can not be provided by linear optics\cite{32}. Recently, an MDI-QKD scheme without joint measurements was presented\cite{33} by employing order-rearrangement technology. However, it still needs to be supplied by other technologies, for example, teleportations (which also result in the need for Bell measurements) as the author suggested, to obtain security. Therefore, as far as we know, no previous MDI-QKD protocols can avoid joint measurements securely. On the other hand, can all QKD protocols become measurement-device-independent ones remains a problem.

In this paper, we present a scheme without employing joint measurements, making a prepare-measure QKD protocol measurement-device-independent, which would be called ‘measurement – device – independentization’ of QKD protocols, see Figure 1. The protocol might look like the detector-devices-independent (DDI) QKD protocols which are insecure under Trojan horse attacks\cite{34,35,36,37,38}. However, after applying a new scheme, our protocol can be immune to the Trojan horse attack in DDI protocols. To illustrate this, we investigate the photon-number-adding (PNA) attack which is exactly the Trojan horse attack when applying to DDI protocols, and provide a solution called
the photon-number-purification (PNP) scheme. The scheme can also close loopholes in previous protocols, such as the DDI protocol, the protocol in [33], and the plug-and-play protocol [39,40]. Finally, we provide a protocol under practical assumptions.

The main advances of the paper include (1) We demonstrate that Joint measurements can be avoided securely in an MDI-QKD protocol; (2) We present a scheme by which any prepare-measure QKD protocol can become an MDI-QKD protocol with nearly the same security and efficiency; (3) We present the PNP scheme to solve a kind of two-stage attack, which is considered as a Trojan horse attack in some previous protocols, in QKD.

2 For BB84 type protocol under ideal assumptions

Let us investigate prepare-measure QKD protocols of BB84 type with assumptions that the legitimate partner, Alice and Bob, employs perfect devices except ones for measuring, for simplicity.

We first state how employing insecure measurement devices can influence the BB84 protocol. In the ordinary BB84 protocol, the sender, Alice, chooses one of the two bases \{ |0\rangle, |1\rangle \} and \{ |+\rangle, |-\rangle \} randomly and sends one of the states in the chosen basis randomly to the receiver, Bob. After Bob receives the state, he randomly chooses one of the bases for measuring. If the choices of the bases of the legitimate partner are the same, they go to the next step, else discard the bit. There are a lot of attacks an eavesdropper, Eve, can employ if she controls the measurement devices. For example, she can intercept the state sent by Alice, measuring via a randomly chosen basis above, and resend the output state to Bob. If Bob chooses the different basis as she chose, then she lets the measurement devices report nothing (since she controls the devices), pretending that the state was lost. Hence, all effective states are eavesdropped on by Eve without improving any error as she measured the states sent by Alice with the same bases chosen by Alice. In fact, a simpler scenario can be that Eve reads the measurement outcomes and obtains the same information as Bob if she controls the detectors.

The explanation above demonstrates that the BB84 protocol is not an MDI-QKD protocol. However, employing a novel scheme, a BB84-type protocol that can be implemented by insecure measurement devices is provided as follow.
BB84 type Protocol:

**Step 1 (Alice’s turn):** Alice prepares a state for each bit randomly in one of the four states $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ and sends it to Bob. Alice and Bob agree that the legitimate bit is 0 if Bob encodes the state by Pauli operator $Z$ or Hadamard gate $H$ and 1 if Bob encodes by Pauli operator $X$ or operator $HXZ$.

**Step 2 (Bob’s turn):** After receiving the state, Bob implements the PNP scheme firstly (see section VI), and then provides a unitary operator, randomly in $Z, X, H$ and $HXZ$ on the state employed for coding. Then he sends the employed state to the untrusted third party, Eve, for measuring.

**Step 3 (Eve’s turn):** Eve is required to measure the state via basis $\{ |0\rangle, |1\rangle \}$, or $\{ |+\rangle, |-\rangle \}$, randomly (the basis can be chosen by Alice or Bob to improve the efficiency) and publicly announce the outcome.

These steps will be repeated several times until Alice and Bob share a long enough bit string.

**Step 4 (sifting turn):** For each bit, Alice publicly announces the chosen basis as in BB84 protocol while Bob announces whether his operator is in $\{ H, HXZ \}$ (but not what it is). If Bob’s operator belongs to $\{ H, HXZ \}$ while the basis of Alice and Eve are the same or if Bob’s operator does not belong to $\{ H, HXZ \}$ while the bases of Alice and Eve are different, the bit will be discarded.

**Step 5 (error estimating and raw key generating turn):** Bob chooses part of the bit string for error estimating. He announces his operations on those bits for Alice who knows the ordinary states to estimate the bit error rate. If the error rate is acceptable, they generate a raw key by the remaining bits and continue error-correcting and privacy amplification procedures.

The protocol is MDI because the whole measurement is implemented by an untrusted third party Eve while the legitimate partner does not need to know if Eve is honest. Note that in the protocol, Bob knows what he encoded by while Alice knows the states she sent as well as the measurement outcomes, and therefore, also knows what Bob encoded by. On the other hand, however, since Eve only knows the measurement outcomes, the legitimate bits are random for her. Also, note that the protocol might look like the DDI protocols which are insecure under Trojan horse attacks. However, they are different. On one hand, the above protocol is measurement-device independent, not only detector-device independent, since the measurement is assumed to be implemented by an untrusted third party. On the other hand, the above one can be immune to the Trojan horse attack, thanks to the PNP scheme (which will be discussed in section VI). From now on, let us ignore the Trojan horse attack temporarily until section VI.
3 Security and efficiency

The security of the protocol comes from the security of the ordinary BB84 protocol and the indistinguishability of operators employed by Bob. Precisely, to access a bit, the eavesdropper, without loss generality says Eve, which is the worst case for Alice and Bob, has to discriminate either the state sent by Alice or the operator provided by Bob. The security of the first case is the same as in the ordinary BB84 protocol while the security of the second one comes from the indistinguishability of the operators employed by Bob.

In detail, $X$, $Z$, $H$, and $HXZ$ are indistinguishable even unambiguously since they are linearly dependent. Moreover, we have the following theorem.

**Theorem 1** Distinguishing the operators $X$, $Z$, $H$, and $HXZ$ (with errors) is as difficult as distinguishing the four BB84 states $|0\rangle$, $|1\rangle$, $|+\rangle$, $|−\rangle$.

The theorem could be verified as follow. Generally, to distinguish the four operators, Eve sends the B partita of a state $|s_eB\rangle \in C^d \otimes C^2$ to Bob and provides a bipartite measurement after Bob operated partita B. After Bob’s operation, the problem for Eve is to distinguish $|s_Z\rangle = (I \otimes Z)|s\rangle$, $|s_X\rangle = (I \otimes X)|s\rangle$, $|s_H\rangle = (I \otimes H)|s\rangle$, $|s_{HXZ}\rangle = (I \otimes HXZ)|s\rangle$ in $C^d \otimes C^2$.

On the other hand, to distinguish the four BB84 states, a protocol can be implemented as follow. An isometric transformation $U$ transforming $|0\rangle, |1\rangle \in C^2$ into $|s_Z\rangle$, $|s_X\rangle \in C^d \otimes C^2$, respectively, is implemented in the first step, which can be done since $|s_Z\rangle$ is orthogonal to $|s_X\rangle$, followed by a distinguishing protocol of the result states, namely $UT|0\rangle = |s_T\rangle$, where $T \in \{Z, X, H, HXZ\}$. Therefore, distinguishing the four BB84 states can be transformed into distinguishing the four operators while the error rate is not larger than the optimal error rate in distinguishing the operators. Similarly, by taking $|s\rangle = |0\rangle \in C^2$, distinguishing the four operators becomes the problem of distinguishing the four BB84 states. Therefore, distinguishing the four operators is as difficult as distinguishing the BB84 states.

This result is not surprising since the dimension of the subspace of the four operators is 2 and thus no matter what state is employed to distinguish them, the four states would be in a subspace of dimension at most 2, in which at most two states can be distinguished. Note that increasing the dimension of the space would not give benefits for state distinguishing[41].

Hence, attacking Bob’s bits would not provide benefits for Eve, compared with conventional attacks, namely eavesdropping on the channel, as in ordinary BB84 protocol.

Therefore, the analysis of the above protocol can be justified as follow. By equivalently letting Bob provide measurements with untrusted measurement devices, the protocols are exactly the ordinary ones except for Bob’s encoding operations. However, the encoding operation of Bob, namely operating a single qubit gate, could be nearly perfect. Note that the single qubit gates could be highly efficient in practice[42,43]. Hence, the security and efficiency are nearly the same as the ordinary ones.
4 Employing more operators and the six-state type protocol

In the above protocol, Bob employs four operators. In fact, he can employ more, for example, eight operators which are $I$, $X$, $Z$, $XZ$, $H$, $HX$, $HZ$, and $HXZ$ for the BB84 type protocol. If the bases of Alice and Eve agree, Alice and Bob discard the states operated by the right four operators while if the bases of Alice and Eve do not agree, they discard the left four, see Table 1. The efficiency will not decrease but the operators of Bob could be more difficult to distinguish.

The same argument is suitable for employing three mutually unbiased bases as in the six-state protocol. In the measurement-device-independenization of the protocol, Alice randomly sends states in the three bases while Bob can employ twenty-four operators without decreasing efficiency, see Table 2, where

\[
H_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ i & -1 \end{pmatrix}, \quad H_2 = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad H_3 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -i & i \end{pmatrix}, \quad H_4 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix},
\]

$|a\rangle = \frac{1}{\sqrt{2}} (|0\rangle + i|1\rangle)$, $|b\rangle = \frac{1}{\sqrt{2}} (|0\rangle - i|1\rangle)$, and all states are up to global phases which affect nothing.

Hence, only $\frac{1}{3}$ of the states are left as in the six-state protocol. For example, if Alice employs basis $\{ |0\rangle, |1\rangle \}$ while Eve measures via $\{ |0\rangle, |1\rangle \}$, then states on which Bob operates $I$, $X$, $Z$, $XZ$, $H$, $HX$, $HZ$, $HXZ$ are left with others discarded. Here, Alice and Bob can decide on coding methods after Eve’s turn and error estimating, namely, for example, they could agree to encode 0 by $I$, $Z$, $H_2$, $H_2Z$ and encode 1 by $X$, $XZ$, $H_2X$, $H_2XZ$ after estimating error rate by states in randomly chosen operators. See Table 2.

5 Measurement-device-independenization of prepare-measure QKD protocols

Let us investigate the general scheme of measurement-device-independenization for a prepare-measure QKD protocol. Assume that the ordinary protocol encodes 0 by state $|0\rangle$ and 1 by state $|y\rangle = x_1 |0\rangle - x_0 |1\rangle \neq |0\rangle$, where without loss generality $x_0, x_1$ are real and hence $x_0^2 + x_1^2 = 1$ since we can always view the two vectors in the same plane. By making the encoding states symmetric,
namely, the bit 0 is encoded by states $|0\rangle$ and $|x\rangle = x_0|0\rangle + x_1|1\rangle$ while the bit 1 is encoded by states $|1\rangle$ and $|y\rangle = x_1|0\rangle - x_0|1\rangle$, respectively, the protocol is described as follow.

For each bit, Alice randomly sends one of the four states to Bob. After Bob receives the state, he implements the PNP scheme and randomly provides an operator in one of $I$, $U$, $XZ$, $UXZ$, $X$, $Z$, $UX$, $UZ$, $XU$, $ZU$, $UXU$ and $UZU$ to the state employed for coding, where $U = \begin{pmatrix} x_0 & x_1 \\ x_1 & -x_0 \end{pmatrix}$ is the (real) unitary operator transforming basis $\{|0\rangle, |1\rangle\}$ to basis $\{|x\rangle, |y\rangle\}$. Then Bob sends the state together with a chosen basis to Eve for measuring. In detail, Bob chooses basis $\{|0\rangle, |1\rangle\}$ if he operates $X$, $Z$, $XU$ or $ZU$, chooses basis $\{|x\rangle, |y\rangle\}$ if operates $UX$, $UZ$, $UXU$, or $UZU$, while randomly chooses one of the two bases if he operates others. For Eve, she is required to measure the state via the chosen basis and announce the outcome. Finally, Alice announces her basis choices for Bob to discard those bits with incompatible bases while others are employed for estimating the bit error rate and generating a raw key as in the BB84 type protocol.

In such a protocol, $\frac{1}{4} \times \frac{1}{4} + \frac{1}{4} \times 1 + \frac{1}{4} \times 0 = \frac{1}{2}$ states would be left after the sifting procedure, see Table 3, where N represents that the pair of Alice’s state and Bob’s operator is invalid no matter what bases does Bob choose. In fact, the measurement bases can be chosen by Eve but the efficiency would be halved since the bits with non-matched bases should be discarded.

The discussions of protocols employing more than two bases are similar. It is worth noting that the efficiency of a general protocol might not be higher than the BB84 type protocol, which employs mutually unbiased bases, while the optimal strategy for the eavesdroppers and thus the secure bounds for the legitimate partner might need to recalculate. Despite, the theoretical

| Table 2: Twenty four operators |
|-----------------------------|
| Alice | Bob | Alice | Bob | Alice | Bob | Alice | Bob | Alice | Bob | Alice | Bob | Alice | Bob |
| 0>   | 0>  | 1>   | 0>  | 1>   | 0>  | 1>   | 0>  | 1>   | 0>  | 1>   | 0>  | 1>   | 0>  | 1>   | 0>  | 1>   | 0>  | 1>   | 0>  | 1>   | 0>  | 1>   |
| 1>   | 1>  | 0>   | 1>  | 0>   | 1>  | 0>   | 1>  | 0>   | 1>  | 0>   | 1>  | 0>   | 1>  | 0>   | 1>  | 0>   | 1>  | 0>   | 1>  | 0>   | 1>  | 0>   |
| +>   | +>  | +>   | +>  | +>   | +>  | +>   | +>  | +>   | +>  | +>   | +>  | +>   | +>  | +>   | +>  | +>   | +>  | +>   | +>  | +>   | +>  | +>   |
| a>   | a>  | a>   | a>  | a>   | a>  | a>   | a>  | a>   | a>  | a>   | a>  | a>   | a>  | a>   | a>  | a>   | a>  | a>   | a>  | a>   | a>  | a>   |
| b>   | b>  | b>   | b>  | b>   | b>  | b>   | b>  | b>   | b>  | b>   | b>  | b>   | b>  | b>   | b>  | b>   | b>  | b>   | b>  | b>   | b>  | b>   |
| 0>   | 0>  | 0>   | 0>  | 0>   | 0>  | 0>   | 0>  | 0>   | 0>  | 0>   | 0>  | 0>   | 0>  | 0>   | 0>  | 0>   | 0>  | 0>   | 0>  | 0>   | 0>  | 0>   |
| 1>   | 1>  | 1>   | 1>  | 1>   | 1>  | 1>   | 1>  | 1>   | 1>  | 1>   | 1>  | 1>   | 1>  | 1>   | 1>  | 1>   | 1>  | 1>   | 1>  | 1>   | 1>  | 1>   |
| +>   | +>  | +>   | +>  | +>   | +>  | +>   | +>  | +>   | +>  | +>   | +>  | +>   | +>  | +>   | +>  | +>   | +>  | +>   | +>  | +>   | +>  | +>   |
| a>   | a>  | a>   | a>  | a>   | a>  | a>   | a>  | a>   | a>  | a>   | a>  | a>   | a>  | a>   | a>  | a>   | a>  | a>   | a>  | a>   | a>  | a>   |
| b>   | b>  | b>   | b>  | b>   | b>  | b>   | b>  | b>   | b>  | b>   | b>  | b>   | b>  | b>   | b>  | b>   | b>  | b>   | b>  | b>   | b>  | b>   |

For such a protocol, $\frac{1}{4} \times \frac{1}{4} + \frac{1}{4} \times 1 + \frac{1}{4} \times 0 = \frac{1}{2}$ states would be left after the sifting procedure, see Table 3, where N represents that the pair of Alice’s state and Bob’s operator is invalid no matter what bases does Bob choose. In fact, the measurement bases can be chosen by Eve but the efficiency would be halved since the bits with non-matched bases should be discarded.
feasibility of the scheme for coding by general states is verified. Most of the prepare-measure QKD protocols can be measurement-device-independent by the scheme. It might not be surprising that the scheme can be modified for entanglement-based protocols.

6 Photon-number-adding attack, Photon number purification scheme, and practical implement

In this section, we will investigate the photon-number-adding (PNA) attack, which is exactly the Trojan horse attack when applied in DDI protocols, and provide a solution called the photon-number-purification (PNP) scheme. Then we will modify the BB84-type protocol for practical settings.

6.1 Photon-number-adding attack: A problem

The PNA attack is described as follows. Eve adds several states in the signal (state) Alice sends to Bob (or even substitutes the signal by hers). These states are employed for distinguishing Bob’s operators and will be removed before measuring. Note that despite the indistinguishability of Bob’s operators via a single state, they can be unambiguously distinguished via multiplied copies. If Bob can not count the photon numbers in a signal, Eve can implement such an attack without being noticed. Essentially, it is such an attack that breaks the security of certain protocols such as the detector-devices-independent (DDI) QKD protocol[34,35,36,37,38], the protocol in [33], and the plug-and-play protocol[39,40].

6.2 Photon number purification: A solution

The PNA attack can be handled by applying C-NOT gates which can be highly efficient, namely with more than 99% fidelity[44,45]. We provide a solution for BB84-type protocol while it would be easily generalized to others. Denote the two C-NOT gates as follow, where \( x, y \) denote the partite.
The scheme is described as follows. Before Bob encodes the state sent by Alice, he randomly copies the state via basis \( \{ |0\rangle, |1\rangle \} \) or \( \{ |+\rangle, |-\rangle \} \), namely, employs source \( |0\rangle_B \) and operates \( C_{0_{AB}} \) or employs source \( |+\rangle_B \) and operates \( C_{+_{AB}} \), where \( B \) denotes the auxiliary partita and \( A \) denotes the ordinary partita. Then he aborts the ordinary state which might still be employed for estimating, and employs partita \( B \). Hence, extra states in the signal are removed and the PNA attack becomes a substituted attack (which might even not be successful), for which the security is guaranteed. We will call the procedure ‘photon number purification’ (PNP). After it, Bob encodes partita \( B \) as usual and sends it to measure.

In such a procedure, a state is discarded if it is wrongly purified, namely, if the state sent by Alice is not on the same basis chosen by Bob for copying. The same investigations are suitable for the six-state type protocol, in which Bob purifies via randomly chosen three bases.

Note that the PNP scheme could also be applied to DDI-QKD protocol, in which the PNA attack is exactly the combination of an intercept-resend attack and a Trojan horse attack [34,35,36,37,38], as well as the protocol in [33] or plug-and-play protocol, to close the loopholes [39,40]. To verify this, just let the legitimate partner implement the PNP scheme after receiving signals and before further operations.

In fact, the PNP scheme might be viewed as a kind of device isolation and thus might be applied to other tasks too, besides QKD. The input signal will not be output while the output signal does not contain the input photons. The same work can be done by teleportation [46], but the PNP scheme could be more efficient since it does not need to employ entanglement and Bell measurement.

6.3 The practical BB84 type protocol

Inspired by the above investigations, the final BB84 type protocol employing weak coherence sources and without photon number counting technologies is described as follows, see Figure 2.

In detail, Alice prepares and sends her qubit to Bob with the decoy-state method [47,48,49] against photon-number-splitting (PNS) attack [50,51] (step 1) while Bob employs the PNP procedure above. The ordinary signal (partita \( A \)) is employed for estimating the channel between Alice and Bob, for which Bob only needs to determine whether it is empty with insecure devices, making the decoy-state methods of Alice work. Then Bob encodes the signal of partita \( B \) and sends it (also by the decoy-state method) to untrusted Eve for measuring (steps 2, 3). Steps 4 and 5 are similar to the protocol with ideal assumptions.

Note that in the protocol, all non-decoy states sent by Alice are employed by Bob. Therefore, to generate a raw secret bit, 4 qubits needed to be sent by Alice, not including the decoy ones, of which half are employed as decoy states.
by Bob, while in the scenario that Bob assumes the measurements instead of Eve, only 2 qubits needed to be sent. Note that in the standard MDI-QKD protocol [20] (employing Bell measurements with two inclusive results), 8 qubits, not including the decoy ones, are required for obtaining a secret bit. Therefore, our protocol could even be more efficient.

7 Conclusion

In conclusion, we presented MDI-QKD protocols without employing joint measurements. Their performances can nearly be the same as the ordinary ones (for example, BB84 protocol) since they can be analyzed in exactly the same way, except ours are measurement-device-independent, assisted by the PNP scheme which could be nearly perfect. Employing more bases or operators could improve their security, as we have discussed in the situation of the six-state protocol, while the legitimate partner can decide the coding methods even after the turns of Eve and error estimating. The scheme is suitable for general prepare-measure QKD protocols, making them MDI-QKD protocols, which is called 'measurement − device − independence' of QKD protocols. It will not be surprising that it can be modified for even entanglement-based protocols.

We also investigated the PNA attack and presented the PNP scheme as a solution, which might also be employed in other tasks. Finally, we provided the BB84-type protocol in practical settings. The protocol could be more efficient than the standard MDI-QKD protocol while it does not need to employ joint measurements.

Although our protocol seems similar to the DDI-QKD protocol which has been proven to be insecure under certain attacks, they are different both in the need for joint measurements and the need for security in measurement devices. The loopholes in the DDI-QKD protocol are not suitable for ours since the PNP scheme. In fact, the PNP scheme can also be employed for closing the
loopholes in DDI protocol as well as two-stage protocols such as plug-and-play protocol.

Finally, there might be a corresponding version for the asymptotically optimal protocols which might not be efficient in practice, however, might provide an asymptotic secure bound of the bit error rate.

References

1. C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, 1984.
2. A. K. Ekert. Quantum cryptography based on bell’s theorem. Physical Review Letters, 67:661–663, Aug 1991.
3. C. Bennett, G. Brassard, and N. Mermin. Quantum cryptography without bell’s theorem. Physical Review Letters, 68:557–559, Feb 1992.
4. C. H. Bennett. Quantum cryptography using any two nonorthogonal states. Physical Review Letters, 68:3121, 1992.
5. L. Goldenberg and L. Vaidman. Quantum cryptography based on orthogonal states. Physical Review Letters, 75(7):1239–1243, Aug 1995.
6. D. Bruss. Optimal eavesdropping in quantum cryptography with six states. Physical Review Letters, 81:3018, 1998.
7. H. Lo and H. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. Science, 283(5410):2050–2056, 1999.
8. N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin. Security of quantum key distribution using d-level systems. Physical Review Letters, 88(12):127902, 2002.
9. V. Scarani, A. Acín, G. Ribordy, and N. Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. Physical Review Letters, 92(5), Feb 2004.
10. S. Kak. A three-stage quantum cryptography protocol. Foundations of Physics Letters, 19(3):293–296, Apr 2006.
11. V. Sharma, K. Thapliyal, A. Pathak, and S. Banerjee. A comparative study of protocols for secure quantum communication under noisy environment: single-qubit-based protocols versus entangled-state-based protocols. Quantum Information Processing, 15(11):4681–4710, Jul 2016.
12. G. Gordon and G. Rigolin. Quantum cryptography using partially entangled states. Optics Communications, 283(1):184–188, 2010.
13. H. Shu. Quantum key distribution based on orthogonal state encoding. International Journal of Theoretical Physics, 61, 2021.
14. J. Barrett, L. Hardy, and A. Kent. No signaling and quantum key distribution. Physical Review Letters, 95(1), Jun 2005.
15. A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani. Device-independent security of quantum cryptography against collective attacks. Physical Review Letters, 98:230501, Jun 2007.
16. E. Hänggi and R. Renner. Device-independent quantum key distribution with commuting measurements. 2010.
17. L. Masanes, S. Pironio, and A. Acín. Secure device-independent quantum key distribution with causally independent measurement devices. Nature Communications, 2(1), Mar 2011.
18. C. C. W. Lim, C. Portmann, M. Tomamichel, R. Renner, and N. Gisin. Device-independent quantum key distribution with local bell test. Physical Review X, 3(3), Jul 2013.
19. E. A. Aguilar, R. Ramanathan, J. Kofler, and M. Pawłowski. Completely device-independent quantum key distribution. Physical Review A, 94(2), Aug 2016.
20. H. K. Lo, M. Curty, and B. Qi. Measurement-device-independent quantum key distribution. Physical Review Letters, 108(13), Mar 2012.
21. X. F. Ma and M. Razavi. Alternative schemes for measurement-device-independent quantum key distribution. Physical Review A, 86(6), Dec 2012.
22. A. Mizutani, K. Tamaki, R. Ikuta, T. Yamamoto, and N. Imoto. Measurement-device-independent quantum key distribution for scarani-acin-ribordy-gisin 04 protocol. *Scientific Reports*, 4(1), Jun 2014.
23. C. Jiang, Z. W. Yu, and X. B. Wang. Measurement-device-independent quantum key distribution with source state errors and statistical fluctuation. *Physical Review A*, 95(3), Mar 2017.
24. W. I. Wang, K. Tamaki, and M. Curty. Measurement-device-independent quantum key distribution with leaky sources. *Scientific Reports*, 11(1), Jan 2021.
25. H. J. Ding, X. Y. Zhou, C. H. Zhang, J. Li, and Q. Wang. Measurement-device-independent quantum key distribution with insecure sources. 2021.
26. C. Jiang, Z. W. Yu, X. L. Hu, and X. B. Wang. Higher key rate of measurement-device-independent quantum key distribution through joint data processing. *Physical Review A*, 103(1), Jan 2021.
27. M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature*, 557(7795):400–403, May 2018.
28. S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd. Direct and reverse secret-key capacities of a quantum channel. *Physical Review Letters*, 102:050503, Feb 2009.
29. S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi. Fundamental limits of repeaterless quantum communications. *Nature Communications*, 8(1), Apr 2017.
30. X. F. Ma, P. Zeng, and H. Y. Zhou. Phase-matching quantum key distribution. *Physical Review X*, 8(3), Aug 2018.
31. C. H. Cui, Z. Q. Yin, R. Wang, W. Chen, S. Wang, G. C. Guo, and Z. F. Han. Twin-field quantum key distribution without phase postselection. *Physical Review Applied*, 11(3), Mar 2019.
32. N. Lütkenhaus, J. Calsamiglia, and K. A. Suominen. Bell measurements for teleportation. *Physical Review A*, 59:3295–3300, May 1999.
33. G. P. He. Measurement-device-independent quantum key distribution with classical bob and no joint measurement. *Quantum Inf Process*, 21(32), 2021.
34. C. C. W. Lim, B. Korzh, A. Martin, F. Bussières, R. Thew, and H. Zbinden. Detector-device-independent quantum key distribution. *Applied Physics Letters*, 105(22):221112, Dec 2014.
35. B. Qi. Trustworthiness of detectors in quantum key distribution with untrusted detectors. *Physical Review A*, 91:020303, Feb 2015.
36. P. González, L. Rebón, T. Ferreira da Silva, M. Figueroa, C. Saavedra, M. Curty, G. Lima, G. B. Xavier, and W. A. T. Nogueira. Quantum key distribution with untrusted detectors. *Physical Review A*, 92:022337, Aug 2015.
37. W. Y. Liang, M. Li, Z. Q. Yin, W. Chen, S. Wang, X. B. An, G. C. Guo, and Z. F. Han. Simple implementation of quantum key distribution based on single-photon bell-state measurement. *Physical Review A*, 92:012319, Jul 2015.
38. S. Sajeed, A. Huang, S. H. Sun, F. H. Xu, V. Makarov, and M. Curty. Insecurity of detector-device-independent quantum key distribution. *Physical Review Letters*, 117:250505, Dec 2016.
39. A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin. “plug and play” systems for quantum cryptography. *Applied Physics Letters*, 70(7):793–795, Feb 1997.
40. N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy. Trojan horse attacks on quantum-key-distribution systems. *Physical Review A*, 73(2), Feb 2006.
41. H. Shu. The independence of distinguishability and the dimension of the system. *International Journal of Theoretical Physics*, 61(146), 2022.
42. F. Brito, D. P. DiVincenzo, R. H. Koch, and M. Steffen. Efficient one- and two-qubit pulsed gates for an oscillator-stabilized josephson qubit. *New Journal of Physics*, 10(3):035027, mar 2008.
43. D. C. McKay, C. J. Wood, S. Sheldon, J. M. Chow, and J. M. Gambetta. Efficient z-gates for quantum computing. *Physical Review A*, 96(2), Aug 2017.
44. A. Kandala, K. X. Wei, S. Srinivasan, E. Magesan, S. Carnevale, G. A. Keefe, D. Klaus, O. Dial, and D. C. McKay. Demonstration of a high-fidelity cnot gate for fixed-frequency transmons with engineered z suppression. *Physical Review Letters*, 127:130501, Sep 2021.
45. A. Noiri, K. Takeda, T. Nakajima, T. Kobayashi, A. Sammak, G. Scappucci, and S. Tarucha. Fast universal quantum gate above the fault-tolerance threshold in silicon. Nature, 601(7893):338–342, Jan 2022.
46. C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wooters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. Physical Review Letters, 70(13):1895–1899, 1993.
47. W. Y. Hwang. Quantum key distribution with high loss: Toward global secure communication. Physical Review Letters, 91:057901, Aug 2003.
48. H. K. Lo, X. F. Ma, and K. Chen. Decoy state quantum key distribution. Physical Review Letters, 94(23), Jun 2005.
49. X. F. Ma, B. Qi, Y. Zhao, and H. K. Lo. Practical decoy state for quantum key distribution. Physical Review A, 72:012326, Jul 2005.
50. B. Huttner, N. Imoto, N. Gisin, and T. Mor. Quantum cryptography with coherent states. Physical Review A, 51:1863–1869, Mar 1995.
51. N. Lütkenhaus and M. Jahma. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. New Journal of Physics, 4:44-44, Jul 2002.
52. H. Shu. Asymptotic optimal quantum key distribution protocols. 2021.