Quantum Inf Process (2017) 16:305
DOI 10.1007/s11128-017-1757-x

Measurement device-independent quantum dialogue

Arpita Maitra

Received: 22 May 2017 / Accepted: 26 October 2017 / Published online: 8 November 2017
© Springer Science+Business Media, LLC 2017

Abstract Very recently, the experimental demonstration of quantum secure direct communication (QSDC) with state-of-the-art atomic quantum memory has been reported (Zhang et al. in Phys Rev Lett 118:220501, 2017). Quantum dialogue (QD) falls under QSDC where the secret messages are communicated simultaneously between two legitimate parties. The successful experimental demonstration of QSDC opens up the possibilities for practical implementation of QD protocols. Thus, it is necessary to analyze the practical security issues of QD protocols for future implementation. Since the very first proposal for QD by Nguyen (Phys Lett A 328:6–10, 2004), a large number of variants and extensions have been presented till date. However, all of those leak half of the secret bits to the adversary through classical communications of the measurement results. In this direction, motivated by the idea of Lo et al. (Phys Rev Lett 108:130503, 2012), we propose a measurement device-independent quantum dialogue scheme which is resistant to such information leakage as well as side-channel attacks. In the proposed protocol, Alice and Bob, two legitimate parties, are allowed to prepare the states only. The states are measured by an untrusted third party who may himself behave as an adversary. We show that our protocol is secure under this adversarial model. The current protocol does not require any quantum memory, and thus, it is inherently robust against memory attacks. Such robustness might not be guaranteed in the QSDC protocol with quantum memory (Zhang et al. 2017).

Keywords Quantum secure direct communication · Measurement device independence · Security analysis · Symmetric cipher

Arpita Maitra
arpita76b@gmail.com

1 Centre for Theoretical Studies, Indian Institute of Technology Kharagpur, Kharagpur, West Bengal 721302, India
1 Introduction

Since the pioneering result of Shor [1] in 1994, an immense attention had been directed toward quantum cryptography. The subdomain, quantum key distribution, achieves enormous proliferation. However, the other domains such as quantum secure direct communication (QSDC) and quantum private query (QPQ) are growing gradually.

The ancestor of QSDC is quantum superdense coding [2]. In superdense coding, two classical bits of information are communicated exploiting only one qubit. The original protocol exploited entangled states to perform this goal.

The first-generation QSDC protocols [3–11] considered one direction, i.e., the classical bits were communicated from Alice to Bob. The subsequent work of [12] proposed bidirectional QSDC where secret messages can flow in both the directions, i.e., from Alice to Bob as well as from Bob to Alice. Such two-way communication is known as quantum dialogue (QD).

In [13], the authors showed that the QD protocol was susceptible to intercept and resend attack and proposed a modified version of it. Since then, several variants [14–18] have been proposed till date.

Very recently, the experimental demonstration of QSDC with state-of-the-art atomic quantum memory has been reported [19]. As QD protocols are motivated toward providing algorithms for bidirectional QSDC, this experimental success opens up the possibility for practical QD. It is thus necessary to examine the vulnerabilities of the existing QD protocols. Unfortunately, all the existing QD protocols inherently leak some information to the adversary through the public announcement of the measurement results [20,21]. (Detailed calculations are shown in Sect. 4.)

In this direction, motivated by the idea of Lo et al. [22], we, here, propose a measurement device-independent quantum dialogue (MDI-QD) protocol which is robust against not only this type of information leakage but also all side-channel attacks. Moreover, our proposed protocol does not require any quantum memory.

In QSDC Alice and Bob share $N$ number of entangled pairs which are initially prepared in $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ state. Alice retains one half of each entangled pair and transmits other half to Bob. Alice and Bob randomly choose some entangled pairs to estimate the error in the channel. If the error lies below the predefined threshold, Alice encodes her qubits with messages, i.e., performs the operation $I$, $\sigma_z$, $\sigma_x$ or $i\sigma_y$ on her qubits. Alice then sends her encoded qubits to Bob who performs Bell state measurement to decode the message coming from Alice. If he obtains $|\phi^+\rangle$ (Alice performed $I$), he concludes that Alice’s message was 00. If it is $|\psi^-\rangle$ (Alice performed $\sigma_z$), he understands that it was 01. If he gets $|\psi^-\rangle$ (Alice performed $\sigma_x$), the message was 10. If he measures $|\psi^-\rangle$ (Alice performed $i\sigma_y$), the message was 11.

In QSDC, due to the transmission of $N$ qubits and the above encoding operations, the entangled pairs shared between Alice and Bob are required to be stored for some time. Hence, quantum memory is necessary to accomplish the communication task in QSDC. However, in the present protocol, we assume that as soon as Eve (the UTP) gets the qubits from Alice and Bob, she measures those in Bell basis and announces the result publicly. Depending on the announcement, Alice and Bob perfectly decode the information coming from their respective counterparts. Hence, quantum memory
is not an essential part here. One may bypass quantum memory to make the protocol inherently robust against any type of memory attacks.

In existing quantum dialogue protocols [12–18], Alice or Bob measures the states coming from their respective counterparts at her or his end. Contrary to this, in the current proposal, we propose a scheme where the measurement devices are with Eve only, who might work as an adversary. Her motivation is to steal the information regarding the communication between two legitimate parties, namely Alice and Bob. In this initiative, we prove that our scheme is secure.

The security of the proposed protocol depends on the following three assumptions. First, we assume the inherent physical correctness of quantum mechanics. Second, we have an assumption that no information leakage takes place from the legitimate parties’ (Alice and Bob) laboratories. Finally, we consider that the legitimate parties have a sufficiently good knowledge about their sources.

2 Proposed protocol

In this section we present the protocol. To describe the algorithm, we need to exploit the Bell states. These are two-qubit entangled states that can form orthogonal basis. The four Bell states can be written as

\[ |\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}} (|00\rangle \pm |11\rangle), \quad |\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}} (|01\rangle \pm |10\rangle). \]

Our current protocol is divided into two parts. We compose two different protocols (BB84 [23] and a modified version of MDI-QKD [22]) to propose our measurement device-independent quantum dialogue protocol. One may replace BB84 part by MDI-QKD also. We have a brief discussion regarding this issue in Sect. 6.

In the first part, Alice and Bob perform BB84 [23] protocol to establish a secret key of \(m\) bits between themselves. This key will be used to prepare the states at both ends. We denote this key by \(b\). When \(b_j = 0, j \in \{1, \ldots, m\}\), Alice (Bob) prepares her (his) state in \(\{|0\rangle, |1\rangle\}\) basis. When \(b_j = 1\), Alice (Bob) prepares her (his) state in \(\{|+\rangle, |-\rangle\}\) basis. Here, \(|+\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)\) and \(|-\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)\). Now, Alice (Bob) chooses a random stream \(a(a')\) of \(m\) bits. The encoding algorithm is presented in Algorithm 2.

**Algorithm 1** Algorithm for encoding

1. When \(a_j(a'_j) = 0\) and \(b_j = 0\), Alice (Bob) prepares \(|0\rangle\).
2. When \(a_j(a'_j) = 1\) and \(b_j = 0\), Alice (Bob) prepares \(|1\rangle\).
3. When \(a_j(a'_j) = 0\) and \(b_j = 1\), Alice (Bob) prepares \(|+\rangle\).
4. When \(a_j(a'_j) = 1\) and \(b_j = 1\), Alice (Bob) prepares \(|-\rangle\).

Alice (Bob) sends her (his) qubit to the UTP (Eve). UTP measures the two particles (one from Alice and one from Bob) in Bell basis. Depending on the announcement by Eve (the result of the Bell measurement), Alice and Bob decode their information.

From Table 1, it is clear that when Alice sends \(|0\rangle\) (\(|1\rangle\)) and the measurement result is either \(|\Phi^+\rangle\) or \(|\Phi^-\rangle\), she concludes with probability 1 that the state sent by Bob is \(|0\rangle\) (\(|1\rangle\)), which means she comes to know with certainty that Bob wants to communicate
Table 1  Different cases in MDI QSDC

| Qubits sent by Alice | Probability (Eve’s end) | Communicated Bits |
|---------------------|-------------------------|-------------------|
|                     | |Φ⟩⁺ |Φ⟩⁻ |Ψ⟩⁺ |Ψ⟩⁻ |
|                     | By Alice | By Bob |
| 0                   | 1/2       | 1/2  | 0   | 0   | 0    | 0    |
| 0                   | 0         | 0    | 1/2 | 1/2 | 0    | 1    |
| 1                   | 0         | 0    | 1/2 | 1/2 | 1    | 0    |
| 1                   | 1/2       | 1/2  | 0   | 0   | 1    | 1    |
|                       | 0         | 1/2  | 0   | 1/2 | 0    | 1    |
|                       | 1         | 0    | 1/2 | 1/2 | 1    | 0    |
|                       | 1/2       | 0    | 1/2 | 0   | 1    | 1    |

the classical bit 0(1). When Alice prepares |0⟩ (|1⟩) and the measurement result is either |ψ⁺⟩ or |ψ⁻⟩, Alice concludes that Bob wants to communicate 1 (0). If Alice prepares |⁺⟩ (|⁻⟩) and the measurement result is either |φ⁺⟩ or |φ⁻⟩, Alice concludes that Bob likes to communicate 0(1). Similarly, when Alice prepares |⁺⟩ (|⁻⟩) and the measurement result is |φ⁻⟩ or |ψ⁻⟩, Bob’s communicated bit must be 1(0). Similar things happen for Bob too. Hence, with probability 1, Alice and Bob can exchange two classical bits of information at a time between themselves.

One can notice that in case of |φ⁺⟩, Eve knows that the communicated bits between Alice and Bob are either 00 or 11. Similarly, in case of |ψ⁻⟩ those must be either 01 or 10, which means in these two cases, the measurement outcomes leak 1 bit of information to Eve. To avoid this situation, Alice and Bob will continue the QD protocol only for the cases where the measurement outcomes are |φ⁻⟩ or |ψ⁺⟩.

Similar to the first phase (BB84 phase) of the protocol, in this phase also, we need to check the error introduced due to eavesdropping. This is because the adversary certainly knows which phase is being implemented at a given time and according to that she could adapt her strategy. To resist this, Alice and Bob choose a subset of γm/2 number of runs among remaining m/2 number of runs, where γ is a small fraction. For this γm/2 runs, Alice and Bob reveal their respective guesses about the communicated bits by their counterparts and check the noise introduced in the channel. If the noise lies below the predefined threshold value, Alice and Bob will continue the protocol. Otherwise, they abort.

To reduce the misuse of bits, one could exploit the discarded bits for error estimation. However, if it opens up any security loop hole is out of the scope here.

One may find that after sharing the bit stream b, Alice and Bob can communicate m/2 bits to each other directly, i.e., not via an UTP. Precisely, m/2 bits will be used for communications from Alice to Bob and the other half from Bob to Alice. In this case, Alice and Bob use two different bits for communications. Hence, the communications become sequential not simultaneous, whereas in our proposed scheme exploiting the same bit, Alice and Bob can communicate simultaneously.

Moreover, for the first case, as we have to exploit P&M (preparation and measure) method, we cannot guarantee no side-channel leakage from the measurement devices.
of the legitimate parties. On the other hand, if we consider the proposed MDI scheme, it automatically certifies the robustness against any side-channel attacks. Though there is no bitwise advantage between these two protocols (one, where Alice (res. Bob) uses $\frac{n}{2}$ bits for communications and other, the proposed protocol), the current protocol offers better security.

For the first phase of the protocol, we consider the security analysis for the finite key length BB84 QKD presented by Tommamichel et al. [24]. Resting on this, we prove the entire security of our composed protocol. We formalize our proposed protocol in Algorithm 2.

The BB84 security analysis has been performed assuming the sources that emit weak coherent (light) pulses (WCP). However, the analysis can be extended for photon tagging [25] and decoy states [26].

For the first phase of the protocol, one may perform decoy state BB84 to establish the secret key $b$ between Alice and Bob. However, for the second phase of the protocol, i.e., for the actual quantum dialogue part, one need not to use decoy states for the following reason.

Decoy states are exploited to resist photon number splitting (PNS) attack [27–29]. In a QKD protocol, after the exchange of qubits, the legitimate parties announce their measurement bases publicly. This public announcement is exploited in PNS attack.

Contrary to this, here, in MDI-QD phase the measurement bases have been predetermined through BB84 QKD. Hence, there is no need to announce the bases publicly. Conditional on the event that the key distribution part has been performed securely, Eve cannot perform PNS attack even if she gets several copies of a photon.

The setup for QD part is shown in Fig. 1.

This optical setup is similar to the optical setup considered in [22]. Here, we omit the intensity modulators (decoy-IMs) which are used to prepare decoy states. It is commented in [22] that this optical setup can only distinguish $|\psi^+\rangle$ and $|\psi^-\rangle$. However, this will not create any problem in our case. We will consider the cases where Eve declares $|\psi^+\rangle$ and discard the cases when Eve announces $|\psi^-\rangle$. The security analysis remains the same.

We should mention that the practical implementation of the proposed protocol is feasible exploiting current quantum technology. BB84 quantum key distribution devices are available in the international market [30]. Experimental demonstration of MDI-QKD has also been reported [31]. As the current protocol is the combination of these two, the experimental demonstration is possible in practice. Moreover, the protocol under consideration does not require any quantum memory which is still hard to achieve.

### 3 Security analysis of the proposed protocol

Before explaining the security analysis, we like to define some security notions required for the security proof of the suggested protocol. As the proposed protocol is based on BB84 QKD, we first define some security notions used in the security proof of BB84 [24]. Then we extend those security notions to QSDC. To the best of
Fig. 1  Schematic diagram of MDI-QD phase. Alice and Bob send weak coherent pulses (WCP) in predetermined polarizations. Those signals interfere at the 50:50 beam splitter (BS) which has a polarizing beam splitter (PBS) at each end. Each PBS projects the incoming photons into either horizontal (H) or vertical (V) polarization states. A click in the single-photon detectors $D_{1H}$ and $D_{2V}$ or in $D_{1V}$ and $D_{2H}$ indicates a projection into the Bell state $\left| \psi^- \right\rangle = \frac{1}{\sqrt{2}} (|HV\rangle - |VH\rangle)$, while a click in $D_{1H}$ and $D_{1V}$ or in $D_{2H}$ and $D_{2V}$ implies a projection into the Bell state $\left| \psi^+ \right\rangle = \frac{1}{\sqrt{2}} (|HV\rangle + |VH\rangle)$.

To our knowledge, this is the first effort to formalize the security issues in this way in the domain of quantum secure direct communication.

In this regard, it should be mentioned that all the existing QSDC [3–11] and QD protocols [12–18] analyze the security issues showing the robustness against some specific type of attacks. For example, the security of a protocol is shown against intercept and resend attack, disturbance attack or modification attack, entanglement measure attack, man-in-the-middle attack, etc. In the present draft, instead of studying individual attack model we consider an approach which is exploited to prove the composable security of a protocol against any arbitrary attack. In this direction, we consider the entropic uncertainty relations presented in [32].

It should be noted that protocols for direct quantum communication generally suffer from the fact that error correction and privacy amplification become problematic. However, error estimation phase is still there. We, here, show how the security of the proposed protocol is based on this error estimation phase. The information leakage to the adversary depends on the amount of quantum bit error rate (QBER) allowed by the protocol.

3.1 Security notions used in QKD

In this subsection, we accumulate the security notions used to prove the composable security of QKD protocols.
Algorithm 2 Protocol for MDI QSDC

1. Alice and Bob perform BB84 protocol to establish a $m$ bit key stream ($b$) between themselves.
2. Alice chooses a random bit string $a$ of length $m$ bits and Bob chooses another random bit string $a'$ of length $m$ bits.
3. Alice (Bob) prepares the qubits at her (his) end according to the following strategy.
   - if $a_j(a'_j) = 0$ and $b_j = 0$, prepares $|0\rangle$.
   - if $a_j(a'_j) = 1$ and $b_j = 0$, prepares $|1\rangle$.
   - if $a_j(a'_j) = 0$ and $b_j = 1$, prepares $|+\rangle$.
   - if $a_j(a'_j) = 1$ and $b_j = 1$, prepares $|−\rangle$.
4. Alice (Bob) sends the prepared qubit to the third party Eve who in turn, measures the two qubits (one from Alice and one from Bob) in Bell basis and announces the result.
5. If Alice prepares $|0\rangle$ ($|1\rangle$) and the measurement result is either $|φ^+\rangle$ or $|φ^−\rangle$, Alice concludes with probability 1 that the communicated bit of Bob is 0 (1).
6. If Alice prepares $|0\rangle$ ($|1\rangle$) and the measurement result is either $|ψ^+\rangle$ or $|ψ^−\rangle$, Alice concludes with probability 1 that the communicated bit of Bob is 1 (0).
7. If Alice prepares $|+\rangle$ ($|−\rangle$) and the measurement result is either $|φ^+\rangle$ or $|ψ^+\rangle$, Alice concludes with probability 1 that the communicated bit of Bob is 0 (1).
8. If Alice prepares $|+\rangle$ ($|−\rangle$) and the measurement result is either $|φ^−\rangle$ or $|ψ^−\rangle$, Alice concludes with probability 1 that the communicated bit of Bob is 1 (0).
9. Similar thing happens for Bob too.
10. Then they consider only the cases where the measurement results were $|φ^−\rangle$ or $|ψ^+\rangle$ and discard the cases for $|φ^+\rangle$ and $|ψ^−\rangle$.
11. To estimate the error introduced in this phase, Alice and Bob choose $\frac{γm}{2}$ number of rounds, where $γ$ is a small fraction and reveal their respective guesses for these rounds.
12. If the observed error lies below the predefined threshold value, they continue the protocol for the remaining $(1−γ)m$ rounds, otherwise they abort.

Definition 1 Correctness: A QKD protocol is said to be correct if for any strategy of an adversary, the key generated at Alice’s end ($K_A$) is same with the key generated at Bob’s end ($K_B$). More precisely, a QKD protocol is correct if and only if

$$K_A = K_B$$

Definition 2 $\epsilon_{\text{cor}}$-correct: A QKD protocol is said to be $\epsilon_{\text{cor}}$-correct if it is $\epsilon_{\text{QKD}}$ indistinguishable from a correct protocol, i.e., a protocol is $\epsilon_{\text{cor}}$-correct if

$$\Pr[K_A \neq K_B] \leq \epsilon_{\text{QKD}}$$

Definition 3 $\Delta$-secret: A key generated from a QKD protocol is called $\Delta$-secret from an adversary ($E$), if it is $\Delta_{\text{sec}}^{QKD}$ close to a uniformly distributed key that is uncorrelated with the adversary, i.e., if

$$\min_\rho_E \frac{1}{2} ||\rho_{K_AE} − \omega_{K_A} \otimes \rho_E|| \leq \Delta_{\text{sec}}^{QKD},$$

where $\rho_{K_AE}$ describes the correlation between the classical key ($K_A$) of Alice and the eavesdropper ($E$), $\omega_{K_A}$ denotes the fully mixed state on $K_A$ and $\rho_E$ is the marginal state on the system of the adversary $E$. 

\(\odot\) Springer
Definition 4 Secrecy: A QKD protocol is said to be completely secret if for any attack strategy of an eavesdropper, $\Delta_{\text{QKD}} = 0$ whenever the protocol outputs a key. The key is called $\epsilon_{\text{sec}}$ if it is $\epsilon_{\text{QKD}}$-indistinguishable from a secret protocol. Precisely, a protocol is $\epsilon_{\text{sec}}$-secret if it outputs $\Delta_{\text{sec}}$-secure keys with $(1 - p_{\text{abort}}) \Delta_{\text{QKD}} \leq \epsilon_{\text{sec}}$, where $p_{\text{abort}}$ is the probability that the protocol aborts.

Definition 5 Security: A QKD protocol is called secure if it is both correct and secret. A protocol is $\epsilon$-secure if it is both $\epsilon_{\text{cor}}$-correct and $\epsilon_{\text{sec}}$-secret. In other words, a protocol is $\epsilon$-secure if

$$\epsilon_{\text{cor}} + \epsilon_{\text{sec}} \leq \epsilon_{\text{QKD}}.$$

3.2 Security notions defined for QSDC

In this subsection, we extend the above security notions for QSDC protocols.

Definition 6 Correctness: The QSDC protocol is said to be correct if for any strategy of an adversary, Alice’s (Bob’s) guess $G_A$ ($G_B$) is same as Bob’s (Alice’s) communicated bits $C_B$ ($C_A$), i.e.,

$$\Pr(G_A = C_B) = \Pr(G_B = C_A) = 1$$

Definition 7 $\epsilon_{\text{cor}}$-correct: A QSDC protocol is said to be $\epsilon_{\text{cor}}$-correct if it is $\epsilon_{\text{QSDC}}$ indistinguishable from a correct protocol, i.e., a protocol is $\epsilon_{\text{cor}}$-correct if

$$\Pr[G_A \neq C_B] = \Pr[G_B \neq C_A] \leq \epsilon_{\text{cor}}$$

Definition 8 $\Delta$-secret: A QSDC protocol is called $\Delta$-secret from an adversary ($E$), if the information extracted by the adversary from the protocol about the communicated bits of a legitimate party is $\Delta_{\text{sec}}$ close to the random guess of the adversary, i.e.,

$$\min_{\rho'_E} \frac{1}{2} ||\rho'_{CAE} - \omega'_{CA} \otimes \rho'_E|| \leq \Delta_{\text{sec}}$$

where $\rho'_{CAE}$ describes the correlation between the communicated bits of Alice and Eve, $\omega'_{CA}$ is the completely mixed state on $C_A$, and $\rho'_E$ is the marginal state on the system $E$.

Definition 9 Secrecy: A QSDC protocol is said to be completely secret if for any attack strategy of an eavesdropper, $\Delta_{\text{QSDC}} = 0$. The protocol is called $\epsilon_{\text{sec}}$ if it is $\epsilon_{\text{QSDC}}$-indistinguishable from a secret protocol. Precisely, a protocol is $\epsilon_{\text{sec}}$-secret if it outputs $\Delta_{\text{sec}}$-secure communications with $(1 - p_{\text{abort}}) \Delta_{\text{QSDC}} \leq \epsilon_{\text{QSDC}}$, where $p_{\text{abort}}$ is the probability that the protocol aborts.
Definition 10 Security: A QSDC protocol is called secure if it is both correct and secret. A protocol is $\epsilon$-secure if it is both $\epsilon_{\text{corr}}$-correct and $\epsilon_{\text{sec}}$-secret. In other words, a protocol is $\epsilon$-secure if

$$\epsilon_{\text{QSDC}}^{\text{corr}} + \epsilon_{\text{QSDC}}^{\text{sec}} \leq \epsilon_{\text{QSDC}}.$$ 

Let us now discuss the security-related issues of our protocol with respect to the above definitions.

The security of our protocol completely depends on the security of $b$ which is generated exploiting BB84 QKD. Hence, our foremost job is to discuss the security of BB84 protocol which is the fundamental building block of our scheme. As we require finite length of the key, we consider the security proof of Tomamichel et al. [24] where the security of BB84 for finite length key has been proven considering weak coherent light pulses. They claimed that the protocol is $\epsilon_{\text{sec}}$-secret if the secret key of length $l$ satisfies the following condition.

$$l \leq \left\lfloor n(q - h(Q + \mu) - \text{Leak}_{\text{EC}} - \log_2(2/\epsilon_{\text{corr}}) - 2 \log_2(1/2\bar{\epsilon})) \right\rfloor$$

where $n$ is the number of raw key bits, $q$ is the quality of the source which emits qubits, $Q$ is the tolerable quantum bit error rate (QBER), and $\mu$ is the statistical deviation. $\mu$ is equal to $\sqrt{n + k/nk^2} \ln(1/\epsilon_Q)$, where $k$ is the number of bits chosen for error estimation and $\epsilon_Q$ is a negligibly small quantity in order of approximately $10^{-10}$. $\text{Leak}_{\text{EC}} + 2 \log(2/\epsilon_{\text{corr}}) + 2 \log_2(1/2\bar{\epsilon})$ is the maximal bits of information that are revealed to the eavesdropper during the protocol. $h(x)$ is the truncated binary entropy function, i.e., $h(x) = -(1-x) \log(1-x) - x \log(x)$ if $x \leq 1/2$ but 1 otherwise [33].

Now we prove the security of the second phase of our protocol, i.e., the actual quantum dialogue part. The security of the entire protocol is solely based on how secure the key ($b$) is. For example, suppose the adversary succeeds to extract a single bit of the key ($b$). In this case, she will successfully extract the secret communications between the legitimate parties corresponding to that bit. Now, we assume that in the first phase of the protocol, Alice and Bob were able to extract a $\epsilon_{\text{sec}}$-secure key of length $m$. Conditional on this event, we now analyze the security of the quantum dialogue phase.

Let the communicated bit by Alice be $C_A$. After the classical announcement of Bell basis measurement, let Bob’s guess about $C_A$ be $G_B$ and the corresponding guess by Eve be $G_E$.

Now, from the tripartite uncertainty relation [32], we get that if $G_B$ is strongly correlated with $C_A$ in {$|0\rangle$, $|1\rangle$} basis or in $Z$ basis, then $G_E$ should be completely uncorrelated with $C_A$ in {$|+\rangle$, $|-\rangle$} basis or in $X$ basis. Hence, we can write

$$H(X|G_E) + H(Z|G_B) = -\log_2 c$$

where $c$ is the maximum overlap of the two bases, i.e., $c = \max_{u,v} |\langle \theta_X^u | \theta_Z^v \rangle|^2$, where $|\theta_X^u\rangle$ and $|\theta_Z^v\rangle$ are the eigenvectors of two measurement operators $X$ and $Z$, respectively. Here, $-\log_2 c = 1$. 

 Springer
As Alice and Bob always choose the same basis which has been predetermined through BB84 QKD, they should be completely correlated (or anti-correlated) in each run of the protocol. Conditional on the event that the key distribution part is $\epsilon_{\text{sec}}$-secure and from the principle of no-cloning [35,36], we get that the information gain by Eve is only possible by introducing some error in the channel.

Let the quantum bit error rate (QBER) at $\{|0\rangle, |1\rangle\}$ basis be $Q'$. Hence, we can write, $H(Z|G_B) = H(Q')$.\(^1\)

As the protocol is symmetric, i.e., $H(X|G_B) = H(Q')$, the total uncertainty of Bob about $C_A$ can be written as

$$H(C_A|G_B) = 2H(Q')$$

Now, if Eve was completely uncorrelated with $C_A$, then $H(C_A|G_E) = H(C_A) = 1$. However, we assume that mounting an arbitrary attack Eve will be successful to extract some information about $C_A$. In exchange she has to introduce some error in the channel. This disturbance is quantified by the uncertainty of Bob about $C_A$. And hence, the total uncertainty of Eve about $C_A$ becomes

$$H(C_A|G_E) = H(C_A) - H(C_A|G_E)$$

$$= 1 - 2H(Q')$$

Now, from the Serfling lemma [37] and its corresponding corollary [38] we can immediately conclude that for the remaining set of $\frac{(1-\gamma)m}{2}$ bits the QBER in $\{|0\rangle, |1\rangle\}$ basis must be in the range $[Q' - \nu, Q' + \nu]$, where $\nu$ is the statistical deviation and $\nu = \sqrt{\frac{(\gamma m + 2)}{\gamma^2 (1-\gamma) m^2} \ln \frac{1}{\epsilon_{\text{QSDC}}}}$. Thus, the maximum mutual information between Alice and Eve becomes

$$I(C_A; G_E) = H(C_A) - H(C_A|G_E)$$

$$\leq 2H(Q' + \nu).$$

Whether the parties abort the protocol completely depends on the error estimation phase. If QBER ($Q'$) is less than the tolerable bit error rate suggested by the protocol, then $p_{\text{QSDC abort}} = 0$ that means conditional on the event that the error estimation phase passed, we can write

$$\Delta_{\text{sec}}^{\text{QSDC}} \leq \epsilon_{\text{sec}}^{\text{QSDC}}.$$  

It means the protocol is $\epsilon_{\text{sec}}$-secure as

$$\min \frac{1}{2} \| \rho'_{C_A E} - \omega'_{C_A} \otimes \rho'_{E} \| \leq \Delta_{\text{sec}}^{\text{QSDC}} \leq \epsilon_{\text{sec}}^{\text{QSDC}}.$$  

---

\(1\) By the abuse of notation, we can write $H(U) = H(p)$ [34], where, $U$ is a discrete random variable with corresponding probability mass function $p$. 

\(\circ\) Springer
Now, we analyze the correctness of our protocol. If the announced result was correct, then Alice as well as Bob can predict the communicated bits by her or his counter parts with probability 1 (see Table 1). Precisely,

$$\Pr(G_A = C_B) = 1.$$ 

However, due to the noise of the channel $\Pr(G_A = C_B)$ should not be 1. Rather, we can write

$$\Pr(G_A \neq C_B) \leq (Q' + \nu).$$

To ensure the $\epsilon_{\text{cor}}$-correctness of the protocol, we have to restrict the value of $Q'$ by $\epsilon_{\text{cor}}^{\text{QSDC}}$, i.e., $(Q' + \nu) \leq \epsilon_{\text{cor}}^{\text{QSDC}}$. Now, we choose $\epsilon_{\text{cor}}^{\text{QSDC}} \approx \epsilon_{\text{sec}}^{\text{QSDC}} \approx \frac{\epsilon_{\text{QSDC}}}{2}$. Finally, if we assume that $\epsilon_{\text{QSDC}}$ is proportional to $\epsilon_{\text{QKD}}$, then we can say that our protocol is $\epsilon$-secure as the following holds.

$$\epsilon_{\text{sec}}^{\text{QSDC}} + \epsilon_{\text{cor}}^{\text{QSDC}} \approx \epsilon_{\text{QSDC}} \approx \epsilon_{\text{QKD}}$$

However, one may find that it is not sufficient for the security as there is no privacy amplification process like QKD. Thus, if the tolerable bit error rate is too large, the information of the communicated bits in the dialogue phase will be leaked too much. On the other hand, if the tolerable bit error rate is set to be zero, then the protocol will become impractical as it requires infinite number of qubits. To remove such ambiguity, in the following section, we give a detailed study of information leakage in existing QD protocols and compare that with the information leakage of the proposed protocol.

### 4 Comparison with existing QD protocols

We start with the very first protocol by Nguyen [12]. In this protocol Bob starts with $N$ entangled pairs initially prepared in state $|\psi^+\rangle$. Bob retains one half of each entangled pair and sends other half to Alice. There are two modes of operations. One is called control mode (CM), and another is called message mode (MM). Alice can randomly shifts between these two modes. CM mode is performed to check the error in the channel. If the error rate is lower than the predefined threshold value, they will continue the protocol. Otherwise, they will abort.

In MM Alice chooses any one of the operators from the set $\{I, \sigma_x, i\sigma_y, \sigma_z\}$. Each operation is encoded by two classical bits. For example, $I$ is encoded by 00, $\sigma_x$ is encoded by 01, $i\sigma_y$ is encoded by 10 and $\sigma_z$ is encoded by 11. Alice encodes her qubit by applying the operator on it and returns that back to Bob. Bob then encodes the same qubit by choosing one of the above operators. After that he measures the encoded qubit and the qubit retained by him in Bell basis and announces the result publicly. Depending on the announcement, Bob and Alice decode the messages of their respective counterparts.

Now, suppose after Bell measurement Bob obtains $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. The announcement of this measurement result provides the following information.
– Bob applies $I$, Alice applies $\sigma_z$ or vice versa
– Bob applies $\sigma_x$, Alice applies $i\sigma_y$ or vice versa

Thus, from the announcement, the adversary (Eve) immediately comes to know that the communicated bits between Bob and Alice must be one of the followings.

– (00, 11), (01, 10), (10, 01), (11, 00).

However, from the perspective of cryptography, the protocol would be completely secure if the situation before the announcement and after the announcement remains indistinguishable. Precisely, after the announcement the communicated bits between Bob and Alice should still be a random guess to Eve. That is Eve should only know the communicated bits can be any of the following exhaustive possibilities.

– (00, 00), (00, 01), (00, 10), (00, 11), (01, 00), (01, 01), (01, 10), (01, 11),
  (10, 00), (10, 01), (10, 10), (10, 11), (11, 00), (11, 01), (11, 10), (11, 11).

Hence, the incorrect usage of classical communication provides Eve $-4 \times \frac{1}{4} \log \frac{1}{4} = 2$ bits of information among 4 bits without introducing any noise in the channel. Unfortunately, all the variants [13–18] of [12] suffer from such information leakage.

On the other hand, we design our protocol in such a way so that we can remove this inherent information leakage through the protocols. Close observation of Table 1 reveals that if the measurement result is either $|\phi^+\rangle$ or $|\psi^-\rangle$, Eve immediately comes to know that the communicated bits between Bob and Alice will be either {00, 11} or {01, 10}, respectively. So in these two cases $-2 \times \frac{1}{2} \log \frac{1}{2} = 1$ bit of information is gained by Eve without introducing any noise in the channel. However, if she measures $|\phi^-\rangle$ or $|\psi^+\rangle$, she does not get any extra information regarding the communicated bits as each of the 4 strings of two bits are equally probable now. This is why we discard the cases where Eve measures $|\phi^+\rangle$ or $|\psi^-\rangle$ to prevent inherent information leakage.

The existing QD protocols allow this inherent information leakage which is equal to the half of the bits communicated. Explicitly, if Alice and Bob exchange 4 bits of classical information, then the protocols allow 2 bits of information to Eve. If Alice and Bob exchange 2 bits of classical information, then the protocols allow Eve to gain 1 bit of information without any effort. Moreover, setting some positive threshold value for QBER the protocols provide additional information to Eve. As there is no privacy amplification phase, there is no way to discard this information leakage to the adversary.

Contrary to this, in the present protocol there is no inherent information leakage. To gain any information regarding the communication, Eve has to introduce some noise in the channel. Considering the same threshold value of QBER as the existing protocols, our scheme leaks less information and hence offers better security.

5 Usage of symmetric cipher

In this section we explore the advantage for exploiting symmetric cipher in the current QD protocol. Suppose, we want to continue the dialogue for a very long time, say for $T$ times. However, we require $M$-bits security against quantum adversary while $T \gg 2M$. In that case, it is wiser to use the construction of a symmetric cipher to
reduce the ‘cost’ of the protocol. Here, ‘cost’ means the number of qubits used and the number of communications (classical as well as quantum) needed for this protocol.

To generate a $T$-bits key stream using a symmetric cipher, we can exploit a bitstream of smaller length (say, $2M$ bits whose security is reduced to $M$ bits against quantum adversary [39]). This smaller bit string is known as ‘seed.’ The secrecy of the cipher depends on the secrecy of the seed used. In the current protocol, this initial seed is generated between the legitimate parties exploiting BB84 protocol and then both the parties may use a secure stream cipher [40] to generate longer secret key stream at both ends.

For example, consider that we need 128 bits security, but the quantum dialogue may be repeated for 512 times. In this case if we do not use symmetric cipher, we have to generate 2048 bits long stream through BB84. This is because half of the bits which correspond to the measurement results $|\phi^+\rangle$ and $|\psi^-\rangle$ will be discarded and approximately half of the remaining bits will be taken for error estimation. So to initiate the key distribution part, we require approximately 8192 number of qubits (4 times of the key bits). However, if we use symmetric cipher considering the seed of 256 bits (2 times of 128-bits), we need approximately 1024 qubits and hence that much quantum communications. In practice, to generate a finite length key we require far more qubits [24] estimated above.

In this regard, we can recall Table 1 of [24]. Assuming $QBER= 1\%$ and security rate $\epsilon/l = 10^{-14}$, we get the key generation rate ($r$) $= 11.7\%$. From this we can conclude that to generate 2048-bit $\epsilon$-secure key ($b$) approximately 17, 504 raw key bits are required that means we have to start with four times of 17, 504 qubits which is equal to 70, 016 qubits and that amount of quantum communications. On the other hand, to generate 256 bit seed we require approximately 2188 raw key bits. In this case, we start with 8752 qubits and that amount of quantum communications. Hence, in terms of reduction in the cost it will be wiser to choose a symmetric cipher to generate the bit stream $b$.

The existing QKD schemes have the unique property that those are universally composable (UC) [41]. This universally composable security of QKD protocols is well proven [42]. This implies that QKD can be combined with any other UC resulting a composed protocol which is also a UC [43]. That is why, in our current protocol, we can compose BB84 QKD with a symmetric cipher [40] to generate $b$.

6 Discussion and conclusion

In this current draft, we propose a measurement device-independent quantum dialogue protocol. Measurement device-independent quantum key distribution [22] has drawn a huge attention as it can resist the side-channel attacks under certain assumptions. Motivated by the idea of [22], we propose a similar scheme for quantum dialogue.

One may wonder why we would not replace the key distribution part of the protocol by MDI-QKD to provide fully measurement device-independent security. In this regard, we like to mention that BB84 QKD has been proven to be one-sided device independent [44]. In the security analysis in [44] we have to put trust only on the source which emits the entangled pairs. Measurement devices have been treated as
a black box. However, one may replace the BB84 part by MDI-QKD. The security proof remains same for both the cases.

Very recently, the experimental demonstration of QSDC protocol with quantum memory has been reported [19]. Being a subset of QSDC, analyzing the security issues for QD protocols becomes very important.

Our QD scheme does not require quantum memory. As soon as the third party (TP) gets the qubits (one from Alice and one from Bob), she measures those in the Bell basis and announces the measurement results. Depending on the announcement, Alice and Bob come to know the communicated bits by their respective counterparts. Hence, the current protocol is inherently robust against any type of quantum memory attacks which might be carried on the QSDC protocols which require quantum memory.

All the existing QD protocols suffer from inherent information leakage via classical communications about the measurement outcomes [20,21]. We design our protocol in such a way so that it becomes robust against such information leakage. So, for practical implementation, our scheme offers better security over the existing QSDC and QD protocols.

References

1. Shor, P.W.: Algorithms for quantum computation: Discrete Logarithms and Factoring. In: Foundations of Computer Science (FOCS) 1994, pp. 124–134, IEEE Computer Society Press (1994)
2. Bennett, C., Wiesner, S.: Communication via one and two-particle operators on Einstein–Podolsky–Rosen states. Phys. Rev. Lett. 69(20), 2881 (1992)
3. Long, G.L., Liu, X.S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A 65, 032302 (2002)
4. Boström, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. 89, 187902 (2002)
5. Deng, F.G., Long, G.L., Liu, X.S.: Two-step quantum direct communication protocol using the Einstein–Podolsky–Rosen pair block. Phys. Rev. A 68, 042317 (2003)
6. Deng, F.G., Long, G.L.: Secure direct communication with a quantum one-time pad. Phys. Rev. A 69, 052319 (2004)
7. Lucamarini, M., Mancini, S.: Secure deterministic communication without entanglement. Phys. Rev. Lett. 94, 140501 (2005)
8. Wang, C., Deng, F.G., Li, Y.S., et al.: Quantum secure direct communication with high-dimension quantum superdense coding. Phys. Rev. A 71, 044305 (2005)
9. Wang, C., Deng, F.G., Long, G.L.: Multi-step quantum secure direct communication using multi-particle Green–Horne–Zeilinger state. Opt. Commun. 253, 15–20 (2005)
10. Li, X.H., Deng, F.G., Zhou, H.Y.: Improving the security of secure direct communication based on the secret transmitting order of particles. Phys. Rev. A 74, 054302 (2006)
11. Li, X.H., Li, C.Y., Deng, F.G., et al.: Quantum secure direct communication with quantum encryption based on pure entangled states. Chin. Phys. B 16, 2149–2153 (2007)
12. Nguyen, B.A.: Quantum dialogue. Phys. Lett. A 328, 6–10 (2004)
13. Man, Z.X., Zhang, Z.J., Li, Y.: Quantum dialogue revisited. Chin. Phys. Lett. 22, 22–24 (2005)
14. Ji, X., Zhang, S.: Secure quantum dialogue based on single-photon. Chin. Phys. 15, 1418–1420 (2006)
15. Man, Z.X., Xia, Y.J., Nguyen, B.A.: Quantum secure direct communication by using GHZ states and entanglement swapping. J. Phys. B At. Mol. Opt. Phys. 39, 3855–3863 (2006)
16. Banerjee, A., Shukla, C., Thapliyal, K., Pathak, A., Panigrahi, P.K.: Asymmetric quantum dialogue in noisy environment. Quant. Inf. Process. 16, 49 (2017)
17. Shukla, C., Kothari, V., Banerjee, A., Pathak, A.: On the group-theoretic structure of a class of quantum dialogue protocols, semi-quantum communication. Phys. Lett. A 377, 518 (2013)
18. Shukla, C., Thapliyal, K., Pathak, A.: Protocols for key agreement, controlled secure direct communication and dialogue. arXiv:1702.07861
19. Zhang, W., Ding, D.S., Sheng, Y.B., Zhou, L., Shi, B.S., Guo, G.C.: Quantum secure direct communication with quantum memory. Phys. Rev. Lett. **118**, 220501 (2017)

20. Tan, Y.-G., Cai, Q.-Y.: Classical correlation in quantum dialogue. Int. J. Quant. Inf. **6**(2), 325 (2008)

21. Gao, F., Guo, F.-Z., Wen, Q.-Y., Zhu, F.-C.: Revisiting the security of quantum dialogue and bidirectional quantum secure direct communication. Sci. China Ser. G Phys. Mech. Astron. **51**(5), 559–566 (2008)

22. Lo, H.K., Curty, M., Qi, B.: Measurement-device-independent quantum key distribution. Phys. Rev. Lett. **108**, 130503 (2012)

23. Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, vol. 175, 8 (1984)

24. Tomamichel, M., Lim, C.C.W., Gisin, N., Renner, R.: Tight finite-key analysis for quantum cryptography. Nat. Commun. **3**, 634 (2012)

25. Lütkenhaus, N.: Security against individual attacks for realistic quantum key distribution. Phys. Rev. A **61**, 052304 (2000)

26. Lo, H.-K., Ma, X., Chen, K.: Decoy state quantum key distribution. Phys. Rev. Lett. **94**, 230504 (2005)

27. Scarani, V., Acín, A., Ribordy, G., Gisin, N.: Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulses implementations. Phy. Rev. Lett. **92**, 057901 (2004)

28. Wang, X.-B.: Beating the photon-number-splitting attack in practical quantum cryptography. Phy. Rev. Lett. **94**, 230503 (2005)

29. Lütkenhaus, N., Jian, M.: Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. New J. Phys. **4**(1), 44 (2002)

30. https://www.idquantique.com

31. Tang, Z., Liao, Z., Xu, F., Qi, B., Qian, L., Lo, H.-K.: Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. Phys. Rev. Lett. **112**, 190503 (2014)

32. Tomamichel, M., Hänggi, E.: The link between entropic uncertainty and nonlocality. J. Phys. A: Math. Theor. **46**, 055301 (2013)

33. Tomamichel, M., Lim, C.C.W., Gisin, N., Renner, R.: Supplementary material. https://www.nature.com/naturecommunications (2012)

34. Cover, T.M., Thomas, J.A.: Elements of Information Theory. John Willey and Sons Inc., Hoboken (2009)

35. Wootters, W.K., Zurek, W.H.: A single quantum cannot be cloned. Nature **299**, 802–803 (1982)

36. Dieks, D.: Communication by EPR devices. Phys. Lett. A **92**(6), 271–272 (1982)

37. Serfling, R.J.: Probability inequalities for the sum in sampling without replacement. Ann. Stat. **2**, 39 (1974)

38. Wen Lim, C.C., Portmann, C., Tomamichel, M., Renner, R., Gisin, N.: Device-independent quantum key distribution with local bell test. Phys. Rev. X **3**, 031006 (2013)

39. Grover, L. K.: A fast quantum mechanical algorithm for database search. In: Proceedings of the Twenty Eighth Annual ACM Symposium on Theory of Computing, 212–219, ACM, New York, NY, USA (1996)

40. Ruhault, S.: SoK: security models for pseudo-random number generators. IACR Trans. Symm. Cryptol. **2017**(1), 506–544 (2017)

41. Canetti, R.: Universally composable security: a new paradigm for cryptographic protocols. FOCS **136--145**, 2001 (2001)

42. Renner, R.: Security of quantum key distribution, Ph.D. thesis, Swiss Federal Institute of Technology (ETH) Zurich, 2005. Int. J. Quantum Inform., **6** (1), 127, 2008, eprint arXiv:quant-ph/0512258

43. Alleaume, R., et al.: Using quantum key distribution for cryptographic purposes: a survey. Theor. Comput. Sci. **560**, 62–81 (2014)

44. Tomamichel, M., Fehr, S., Kaniewski, J., Wehner, S.: One-sided device-independent QKD and position-based cryptography from monogamy games. Eurocrypt **2013**(7881), 609–625 (2013)