Quantum Information Processing (2020) 19:295
https://doi.org/10.1007/s11128-020-02793-4

Quantum direct communication protocols using discrete-time quantum walk

S. Srikara[1] · C. M. Chandrashekar[2,3]

Received: 14 April 2020 / Accepted: 30 July 2020

Abstract
The unique features of quantum walk, such as the possibility of the walker to be in superposition of the position space and get entangled with the position space, provide inherent advantages that can be captured to design highly secure quantum communication protocols. Here we propose two quantum direct communication protocols, a quantum secure direct communication protocol and a controlled quantum dialogue (CQD) protocol using discrete-time quantum walk on a cycle. The proposed protocols are unconditionally secure against various attacks such as the intercept-resend attack, the denial of service attack, and the man-in-the-middle attack. Additionally, the proposed CQD protocol is shown to be unconditionally secure against an untrusted service provider and both the protocols are shown more secure against the intercept resend attack as compared to the qubit-based LM05/DL04 protocol.

Keywords Quantum direct communication · Quantum dialogue · Quantum walk

1 Introduction

The research in quantum cryptography, which first started with the BB84 quantum key distribution (QKD) protocol [1], was later followed up with the design and the study of various novel QKD schemes [2–4]. These protocols were designed to securely generate a secret key between two parties, which would then be used to encode the message via a one-time pad. Most of the research in quantum cryptography was concentrated on QKD, until during 2002-2005, when few new protocols were introduced [5–9]. These protocols were called quantum secure direct communication (QSDC) protocols. In

✉ C. M. Chandrashekar
chandru@imsc.res.in

1 Indian Institute of Science Education and Research, Pune 411008, India

2 The Institute of Mathematical Sciences, C. I. T. Campus, Taramani, Chennai 600113, India

3 Homi Bhabha National Institute, Training School Complex, Anushakti Nagar, Mumbai 400094, India

2002, the first QSDC protocol was proposed in the form of a deterministic key that could transmit the secret message [5,6]. In 2003, the standard form of QSDC without the requirement of a key was proposed [7] and in 2004 and 2005 a single photon-based protocol called DL04 was proposed [8]. Recently, the device-independent QSDC protocol [10] and measurement device-independent QSDC protocol [11,12] have also been proposed. In 2004, a two-way quantum direct communication protocol was introduced, called the quantum dialogue (QD) [13]. Unlike QSDC protocols where communication is just one way, in QD protocols both the parties interact with each other, i.e. communication is two ways. This quantum dialogue protocol was extended to a controlled quantum dialogue protocol (CQD), in which a third party provides the quantum services for communication [14]. The QSDC, QD and the CQD protocols have shown that an unconditionally secure quantum communication can be achieved even without a key. With the reporting of experimental realisation of QSDC protocols [15–17], its significance for practical use is being highlighted.

In 1993, the concept of quantum walks was introduced [18]. Quantum walks are the quantum analogues of classical random walks. Unlike classical random walks where the walker is at just one deterministic position at a given time, in quantum walks, the walker can be at multiple positions at the same time, i.e. in a superposition of position space. The tossed quantum coin that decides the movement of the walker can also be at a superposition of head and tails. These unique features of quantum walks can help to traverse multiple positions faster, a feature that has been exploited in the design of various quantum search algorithms [19]. Quantum walks have also been used for studying and describing various quantum phenomena [20,21] and also in the study and design of quantum networks [22]. Surprisingly, the usage of quantum walks for cryptography and secure communication has largely been unexplored, except for a few designs of QKD protocols [23] and public-key cryptosystems [24]. In this work, we delve into an unexplored cryptographic potential of quantum walks, which is the quantum direct communication. Using the discrete-time quantum walk on a cycle, we propose two new protocols for QSDC and CQD and show the unconditional security they provide against various attacks such as the intercept-resend attack, the denial of service attack and the man-in-the-middle attack. We also show that the proposed CQD protocol provides unconditional security against an untrusted service provider and both the protocols are more secure against the intercept resend attack as compared to the qubit-based LM05/DL04 protocol [8,9].

This paper is structured as follows: In Sect. 2, we introduce the preliminary concepts of discrete-time quantum walk on a cycle required to understand the protocols proposed in Sect. 3. In Sect. 4, we discuss the security of the proposed protocols against various attacks. In Sect. 5, we conclude with our remarks. In the "Appendix," we provide relevant background details that can be referred to if required.

2 Discrete-time quantum walk on a cycle preliminaries

Quantum walks are a quantum analogue of the classical random walks. In discrete-time quantum walk on an N-cycle, the walker moves along N discrete points on a cycle [25], which are represented by N-dimensional quantum states $|x\rangle$, orthogonal to each other and belonging to the Hilbert space H_p where

$$H_p = span\left\{|x\rangle, x \in \{0, 1, 2, ..., N-1\}\right\}.$$

.

During each step of the discrete-time quantum walk, the walker moves one position either to his left or to his right based on the result ($|0\rangle$ or $|1\rangle$) of the quantum coin, which is given by a two-dimensional quantum state $|c\rangle$ belonging to the Hilbert space H_c where

$$H_c = span\{|0\rangle, |1\rangle\}.$$

If the walker is in a superposition of the coin state, it will move to both left and right simultaneously, creating a state which is in superposition in position space. Thus, the initial state of the walker starting at position x_{in} and with an initial coin state $|c_{in}\rangle$ can be considered to be in a superposition of the two allowed basis states given by

$$|\Psi_{in}\rangle = |x_{in}\rangle \otimes |c_{in}\rangle = |x_{in}\rangle|c_{in}\rangle \quad ; \quad |x_{in}\rangle \in H_p \quad ; \quad |c_{in}\rangle \in H_c. \tag{1}$$

The dynamics of the walker during each step of the walk is governed by the action of the unitary operator, a composition of a quantum coin operation on the coin space followed by a conditioned position shift operation on the complete Hilbert space [26–28],

$$U = U(\theta, \xi, \zeta) = S\left(I_p \otimes R_c\right). \tag{2}$$

Here I_p is the identity operator on position space and the quantum coin operation R_c is given by

$$R_c = R_c(\theta, \xi, \zeta) = \begin{bmatrix} e^{i\xi}\cos\theta & e^{i\zeta}\sin\theta \\ e^{-i\zeta}\sin\theta & e^{-i\xi}\cos\theta \end{bmatrix}. \tag{3}$$

In simpler cases, when $\zeta = \xi = 0$ or fixed to a specific value, $R_c(\theta, \xi, \zeta) = R_c(\theta)$ is the coin operator on the coin space. The shift operator on $H = H_p \otimes H_c$, which shifts the position of the walker in the direction which is determined by the coin state, is given by

$$S = \sum_{x=0}^{N-1}(|x-1(\bmod N)\rangle\langle x| \otimes |0\rangle\langle 0| + |x+1(\bmod N)\rangle\langle x| \otimes |1\rangle\langle 1|). \tag{4}$$

The state after t steps of the walk on an $N-$cycle, in general, will be in the form,

$$|\Psi_t\rangle = U^t|\Psi_{in}\rangle = \sum_{x=1}^{N}|x\rangle \otimes \left(\alpha_{x,t}|0\rangle + \beta_{x,t}|1\rangle\right), \alpha_{x,t}\ \beta_{x,t} \in \mathbb{C}\,\forall\, x, t \tag{5}$$

and the probability of finding the walker at any position x after t steps of the walk will be $P(x,t) = |\alpha_{x,t}|^2 + |\beta_{x,t}|^2$. In addition to the quantum walk evolution operator, we will also define the translation operator and measurement operator which will be needed for QSCD and CQD protocols. The translation operator T defined on the space H_p is given as:

$$T(y) = \sum_{x=0}^{N-1} |x + y(\bmod N)\rangle\langle x| \tag{6}$$

and the measurement operator M is defined on the entire space H in the form given by

$$M = M_p \otimes M_c$$

where

$$M_p = \sum_{x=0}^{N-1} |x\rangle\langle x| \qquad \text{and} \qquad M_c = \sum_{c=0}^{1} |c\rangle\langle c|. \tag{7}$$

Note that $[T(y), U] = 0$, i.e. $T(y)$ and U commute with each other [24].

3 The protocols

The extent of the spread of the discrete-time quantum walk in position space is mainly governed by the parameter θ in the quantum coin operation [27,28]. Therefore, in this paper, we will keep only the coin parameter θ as a variable parameter while keeping the parameters ξ and ζ constant throughout the protocols. Here we first present the encoding scheme, and then, we present the protocols for QSDC and CQD. The schematic representation of the protocols for QSDC and CQD is presented in Fig. 1 and Fig. 2, respectively. In both the figures, the "random path switcher" is a device that switches the path of the quantum channel to move a particular state into encoding the message or into checking eavesdropping, similar to using a physical lever that is used for changing the railway tracks. For example, for linear and quantum optical implementations of quantum walks [29], various optical switches [30–32] coupled with a quantum random number generator [33] can be used as a random path switcher.

3.1 Encoding of the message

The message m (or a part m of the total message) is encoded on a discrete-time quantum walk state $|\phi\rangle = \sum_i |x_i\rangle|c_i\rangle$ by applying the translation operator $T(m)$ on $|\phi\rangle$, resulting in the state $T(m) \otimes I_c|\phi\rangle = \sum_i |x_i + m(\bmod N)\rangle|c_i\rangle$.

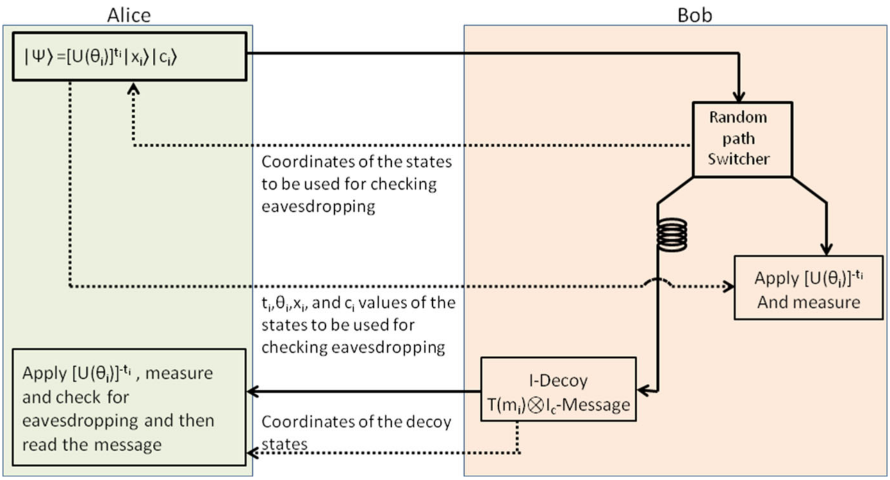

Fig. 1 Schematic diagram of the discrete-time quantum walk-based QSDC protocol. The bold arrow lines represent quantum channels, whereas the dotted arrow lines represent classical channels

3.2 Discrete-time quantum walk-based QSDC protocol

1. Alice prepares n discrete-time quantum walk states. To prepare n quantum walk states, Alice randomly chooses $3n$ integers $\{t_1, t_2, ..., t_n\}$, $\{x_1, x_2, ..., x_n\}$ and $\{c_1, c_2, ..., c_n\}$ such that $x_i \in \{0, 1, 2, ..., N-1\}$, $c_i \in \{0, 1\}$ and $t_i \in \mathbb{N} \cup \{0\}$ $\forall i \in \{1, 2, ..., n\}$ and n random real numbers $\{\theta_1, \theta_2, ..., \theta_n\}$ such that $\theta_i \in [0, 2\pi]$. Thus, she prepares n discrete-time quantum walk states $[U(\theta_i)]^{t_i}|x_i\rangle|c_i\rangle = U^{t_i}|x_i\rangle|c_i\rangle$ $\forall i \in \{1, 2, ..., n\}$ and sends these states to Bob. (In the rest of this and the next protocol, we will refer to $[U(\theta_i)]$ as U).
2. On receiving the walk states from Alice, Bob randomly chooses $n/2$ of them for checking eavesdropping and classically sends their corresponding coordinates i to Alice. Alice classically sends to Bob the corresponding values of t_i, x_i, c_i, and θ_i. Bob applies the corresponding operation U^{-t_i} on those states, measures them, and checks the measurement result with the value of x_i and c_i. If the error is within a tolerable limit, he continues to step 3. Otherwise, the protocol is aborted and they will start the protocol all over again.
3. Out of the remaining $n/2$ walk states, Bob chooses $n/4$ of them for encoding the message. On each of those $n/4$ states, Bob codes a part of his message m_i by applying the translation operator $T(m_i) \otimes I_c$. He does nothing to the other $n/4$ states (let us call them decoy states). He then sends all the $n/2$ states back to Alice.
4. Once Alice confirms the receiving of the states, Bob classically sends the coordinates of the decoy states to Alice. Alice applies the corresponding operator U^{-t_i} on the decoy states and checks for eavesdropping just like how Bob does it in step 2.
5. Once no eavesdropping is confirmed, Alice then applies U^{-t_i} on the remaining $n/4$ message states and measures them to obtain the message sent by Bob.

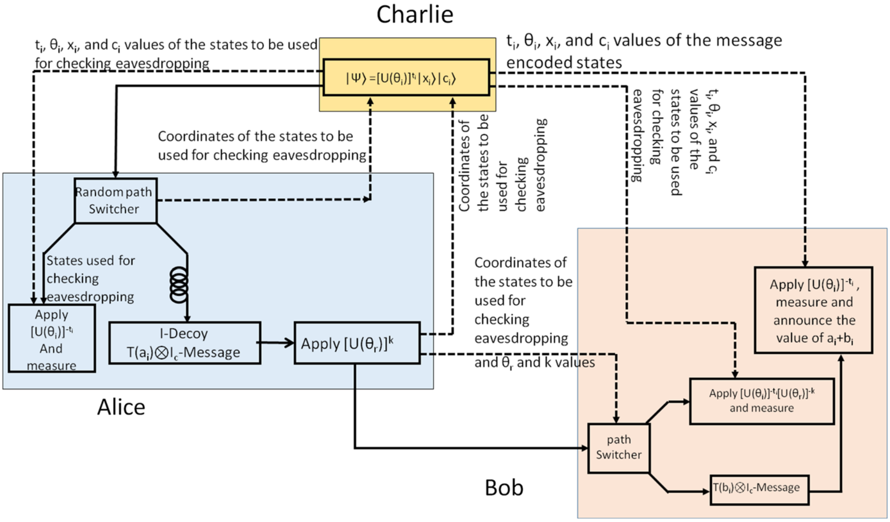

Fig. 2 Schematic diagram of the discrete-time quantum walk-based CQD protocol. The bold arrow lines represent quantum channels, whereas the dotted arrow lines represent classical channels

3.3 Discrete-time quantum walk-based CQD protocol

1. Charlie prepares n discrete-time quantum walk states. To prepare n quantum walk states, Charlie randomly chooses $3n$ integers $\{t_1, t_2, ..., t_n\}$, $\{x_1, x_2, ..., x_n\}$ and $\{c_1, c_2, ..., c_n\}$ such that $x_i \in \{0, 1, 2, ..., N-1\}$, $c_i \in \{0, 1\}$ and $t_i \in \mathbb{N} \cup \{0\}$ $\forall i \in \{1, 2, ..., n\}$ and n random real numbers $\{\theta_1, \theta_2, ..., \theta_n\}$ such that $\theta_i \in [0, 2\pi]$. He prepares n quantum walk states $[U(\theta_i)]^{t_i}|x_i\rangle|c_i\rangle = U^{t_i}|x_i\rangle|c_i\rangle \quad \forall i \in \{1, 2, ..., n\}$ and sends these states to Alice.
2. On receiving the walk states, Alice randomly chooses $n/2$ of them for checking eavesdropping and classically sends their corresponding coordinates i to Charlie. Charlie classically sends to Alice the corresponding values of t_i, x_i, c_i, and θ_i. Alice applies the operation U^{-t_i} on those states and measures them and checks the measurement result with the value of x_i and c_i. If the error is within a tolerable limit, Alice continues to step 3. Otherwise, the protocol is aborted and they restart the protocol from the beginning.
3. Out of the remaining $n/2$ walk states, Alice chooses $n/4$ of them for encoding the message. On each of those $n/4$ states, Alice encodes a part of her message a_i by applying the translation operator $T(a_i)$. She does nothing to the other $n/4$ states (let us call them decoy states). She then chooses a random integer k and coin parameter θ_r, applies $[U(\theta_r)]^k$ on all the $n/2$ states, and sends the states to Bob.
4. Once Bob confirms the receiving of the states, Alice publicly announces the values of θ_r and k and the coordinates of the decoy states. Charlie, upon receiving the announcement, sends the t_i, x_i, c_i, and θ_i values of the decoy states to Bob. Bob then applies the corresponding operator $U^{-t_i}[U(\theta_r)]^{-k}$ on the decoy states and checks for the presence of Eve just like how Alice does it in step 2.

5. Meanwhile, Bob encodes his message b_i on the remaining message states by applying the translation operator $T(b_i)$. Once he confirms the absence of eavesdropping, Charlie sends the t_i, x_i, θ_i, and c_i values of the message states to Bob. Bob applies the operator $U^{-t_i}[U(\theta_r)]^{-k}$ on the message states, measures them, and publicly announces the measurement results $a_i + b_i$. Alice and Bob subtract a_i and b_i, respectively, from their results to obtain each others' messages.

Compared to LM05/DL04 protocols (see "Appendix") which can transfer one bit per quantum state, the discrete-time quantum walk protocol on a coin and position Hilbert space presented above can transfer more number of bits per quantum state allowing for faster transmission of message. In addition to this, the security advantage is discussed below.

4 Security

In this section, we analyse the security of our protocol against various attacks, namely the intercept-resend attack, the denial of service attack, man-in-the-middle attack, and the attack by an untrusted Charlie.

4.1 Intercept-and-resend attack

In this attack, Eve intercepts the quantum channel and tries to extract information from the incoming state by measuring it. Then, she re-prepares the appropriate state (based on the information she receives) and sends it to the receiver. Our protocols are robust against this attack. This is because the discrete-time quantum walk states are usually superposition states where the position and the coin Hilbert spaces are usually entangled. Hence, Eve cannot determine the incoming state by measurement alone. Instead of directly measuring the state, Eve can apply U^{-t_i} and then measure the state. But this attack also cannot be performed by Eve because the value of t_i will be only known to Alice at the time of attack. If Eve attempts to perform this attack, she will raise the error during the eavesdropping checking of the control mode states and hence will be caught.

4.1.1 Mutual information between Alice and Eve

In practical scenarios, Alice can choose her parameters t_i, x_i, c_i, and θ_i only from a finite set or a finite range of values. Hence, the amount of mutual information I_{AE} gained between Alice and Eve during the intercept-resend attack is dependent upon the size of these sets and ranges. The higher the mutual information, the more will be known by Eve about the state sent by Alice, thus making the protocol less secure. Let us consider a practical scenario where Alice can choose:

- t_i from the set T containing $n(T)$ integers (from 0 to $n(T) - 1$)
- x_i from the set $X = \{0, 1, 2, ..., N - 1\}$ (set of N values), N being the dimension of the position space

- c_i from the set $C = \{0, 1\}$ (set of 2 values)
- θ_i from the range $R_\theta = [\theta_{min}, \theta_{max}]$

Let us say that for a particular round of transmission, Alice chooses the values $t_A \in T$, $x_A \in X$, $c_A \in C$, and $\theta_A \in R_\theta$ and prepares the state $|\psi_A\rangle = [U(\theta_A)]^{t_A}|x_A\rangle|c_A\rangle$. Now Eve can perform the intercept-resend attack in two ways,

1. directly measure the incoming state to obtain the position and coin values x_E and c_E, respectively (let us call this strategy IR1) , or
2. randomly choose the values $t_E \in T$, $x_E \in X$, $c_E \in C$, and $\theta_E \in R_\theta$ and perform the operation $[U(\theta_E)]^{-t_E}|\psi_A\rangle$ and then measure the position and coin values of the resulting state in order to obtain the values x_E and c_E, respectively (let us call this strategy IR2).

Let us now examine IR2. We can consider t_A, x_A, c_A, t_E, x_E, c_E, θ_A, and θ_E as uniformly distributed random variables, where t_A, x_A, c_A, t_E, x_E, c_E are discrete and θ_A and θ_E are continuous. Now, for IR2, the mutual information I_{AE_2} between Alice and Eve is given by,

$$I_{AE_2} = \sum_{t_E \in T} \sum_{x_E \in X} \sum_{c_E \in C} \sum_{t_A \in T} \sum_{x_A \in X} \sum_{c_A \in C} \int_{\theta_A=\theta_{min}}^{\theta_{max}} \int_{\theta_E=\theta_{min}}^{\theta_{max}} p(t_A, x_A, c_A, t_E, x_E, c_E, \theta_A, \theta_E) log_2 \frac{p(t_A, x_A, c_A, t_E, x_E, c_E, \theta_A, \theta_E)}{p(t_A)p(x_A)p(c_A)p(t_E)p(x_E)p(c_E)p(\theta_A)p(\theta_E)} d\theta_A d\theta_E, \tag{8}$$

where $p(a_1, a_2, ..., a_n)$ is the joint probability distribution mass function of the random variables $a_1, a_2, ..., a_n$ where $a_i \in \{t_A, x_A, c_A, t_E, x_E, c_E, \theta_A, \theta_E\}$.
For IR1, the mutual information I_{AE_1} between Alice and Eve is given by,

$$I_{AE_1} = \sum_{x_E \in X} \sum_{c_E \in C} \sum_{t_A \in T} \sum_{x_A \in X} \sum_{c_A \in C} \int_{\theta_A=\theta_{min}}^{\theta_{max}} p(t_A, x_A, c_A, x_E, c_E, \theta_A) log_2 \frac{p(t_A, x_A, c_A, x_E, c_E, \theta_A)}{p(t_A)p(x_A)p(c_A)p(x_E)p(c_E)p(\theta_A)} d\theta_A. \tag{9}$$

The above formulas of I_{AE_1} and I_{AE_2} contain 1 and 2 integrals, respectively. Due to lack of access to good computing power to calculate I_{AE_1} and I_{AE_2}, we modify the protocol for the purpose of analysis of this attack, by keeping all the coin parameters, including θ constant and publicly known throughout the protocol, thus reducing the number of secret parameters and avoiding the integrals. Now, the revised formulas for I_{AE_1} and I_{AE_2} will be

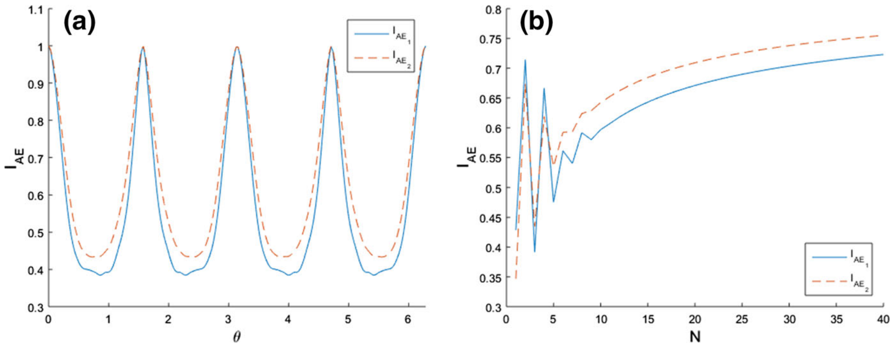

Fig. 3 **a** Mutual information I_{AE} vs coin parameter θ for $N = 3, n(T) = 7$. **b** Mutual information I_{AE} vs the cycle length N for $n(T) = 7, \theta = \frac{\pi}{4}$. The variation of I_{AE} with θ is periodic with period $\frac{\pi}{2}$ with the peaks at even multiples of $\frac{\pi}{4}$ and minimum at odd multiples of $\frac{\pi}{4}$. The variation of I_{AE} with N is fluctuating in the beginning, but later steadily increases. For both the plots, the coin parameters ζ and ξ were set to a fixed value $\frac{\pi}{4}$

$$I_{AE_2} = \sum_{t_E \in T} \sum_{x_E \in X} \sum_{c_E \in C} \sum_{t_A \in T} \sum_{x_A \in X} \sum_{c_A \in C} p(t_A, x_A, c_A, t_E, x_E, c_E) log_2 \frac{p(t_A, x_A, c_A, t_E, x_E, c_E)}{p(t_A)p(x_A)p(c_A)p(t_E)p(x_E)p(c_E)} \tag{10}$$

and

$$I_{AE_1} = \sum_{x_E \in X} \sum_{c_E \in C} \sum_{t_A \in T} \sum_{x_A \in X} \sum_{c_A \in C} p(t_A, x_A, c_A, x_E, c_E) log_2 \frac{p(t_A, x_A, c_A, x_E, c_E)}{p(t_A)p(x_A)p(c_A)p(x_E)p(c_E)} \tag{11}$$

where

$$p(t_A, x_A, c_A, t_E, x_E, c_E) = \frac{‘1}{2N[n(T)]^2} (\langle x_E | \langle c_E | U^{-t_E} U^{t_A} | x_A \rangle | c_A \rangle)^2, \tag{12}$$

$$p(t_A, x_A, c_A, x_E, c_E) = \frac{‘1}{2N[n(T)]} (\langle x_E | \langle c_E | U^{t_A} | x_A \rangle | c_A \rangle)^2 \tag{13}$$

and

$$p(a_i) = \sum_{a_1, , a_2, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n} p(a_1, a_2, \ldots, a_n) \tag{14}$$

where $a_j \in \{t_A, x_A, c_A, t_E, x_E, c_E\}$ and $U = U(\theta)$ where θ is the publicly known coin parameter throughout the protocol. We can see that I_{AE_1} and I_{AE_2} are a function of $n(T)$ and N and also depend on the fixed coin parameter θ.

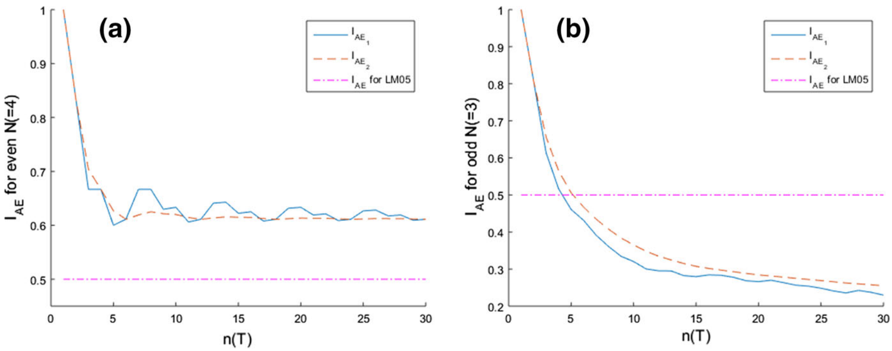

Fig. 4 Mutual information I_{AE} vs $n(T)$ for **a** $N = 4$ and **b** $N = 3$. The dash-dotted line (magenta coloured in online and colour-printed versions) represents the I_{AE} for one channel of the LM05/DL04 protocol, which is the same as the I_{AE} for the BB84 protocol. In both the figures, I_{AE} decreases with $n(T)$, thus increasing security of the protocol with increase in $n(T)$. For both the plots, the coin parameters θ, ζ, and ξ were set to a fixed value $\frac{\pi}{4}$

In Fig. 3(a), we can see that I_{AE} is at its lowest when θ is an odd multiple of $\frac{\pi}{4}$ and is at its highest ($I_{AE} = 1$) when θ is an even multiple of $\frac{\pi}{4}$. Hence, for θ equal to even multiples of $\frac{\pi}{4}$, the security of the protocol will be compromised. This is consistent with the discrete-time quantum walk dynamics, for θ being even multiples of $\frac{\pi}{4}$, the walk will either be localised around the origin or will be ballistic without being in superposition of more than two position space at a time [27,28]. We can infer that the degree of spread of the walker in position space gives an enhanced security to the protocol. In Fig. 3(b), we can see that for odd N, I_{AE} increases with increase in N, whereas for even N, I_{AE} initially decreases with N, but then increases. In Fig. 4, we see that I_{AE} decreases with $n(T)$ and its value is greater for even N than for odd N. In fact, for odd N, the I_{AE} drops much below 0.5 (which is the I_{AE} value for the LM05/DL04 protocol (see "Appendix")) for large $n(T)$ and in fact is less than 0.25 for $n(T) > 25$. From Fig. 4(b) and Fig. 3, we can see that $I_{AE_2} > I_{AE_1}$, implying that that IR2 is a better strategy for Eve than IR1 for odd N. This shows that for an odd, low value of N, and a high value of $n(T)$, and θ being an odd multiple of $\frac{\pi}{4}$, our discrete-time quantum walk protocols are more secure against the intercept-resend attack than the LM05/DL04 protocol (whose $I_{AE} = 0.5$), even with the modification that the coin parameters remain constant and publicly known throughout the protocol.

4.2 Denial of service attack

Instead of trying to extract information from the incoming state, Eve can rather perform a denial-of-service attack, i.e. she can just stop the incoming state from going forward and can instead prepare and send a random discrete-time quantum walk state. This attack also cannot be performed by Eve because if she does so, she introduces an added error and noise into the channel, and, hence the eavesdropping checking performed by the sender and the receiver at each quantum channel will detect Eve.

4.3 Man-in-the-middle attack

Let us consider the QSDC protocol. In this attack, Eve initially puts the incoming state from Alice into her quantum memory. Then, she sends her own walk state to Bob. Bob, assuming that Alice may have sent this state, encodes his message on this state and sends it back to Alice. Eve intercepts that channel also and reads the message. She then encodes the message onto Alice's state which she had earlier stored in her quantum memory and sends it back to Alice, thus being able to read the message. Eve can perform a similar kind of attack in the CQD protocol to obtain the message of one of the two communicating parties. In both cases of this attack, Eve will be detected by the communicating parties during eavesdropping checking. Hence, both our protocols are unconditionally secure against this attack.

4.4 Attack by an untrusted Charlie

Let us consider the QDC protocol. In this attack, Charlie intercepts the Alice–Bob channel, applies U^{-t_i} on the incoming state, and obtains Alice's message by measuring the state. Then, he re-prepares the state and sends it to Bob. Then, when Bob encodes his message b_i and announces the value $a_i + b_i$, Charlie can then get Bob's message as well. But our QDC protocol is robust against this attack because as Alice applies an additional $[U(\theta_r)]^k$ to the states, Charlie will not know the value of θ_r or k and hence he cannot apply $[U(\theta_r)]^{-k}$ to retrieve the state.

5 Conclusion

The unique features of a discrete-time quantum walk such as spreading the quantum state in the superposition of position space and entanglement generation between the position and the coin states have an immense unexplored potential for quantum security for communication and cryptographic protocols. In this work, we have explored its potential for providing cryptographic security by proposing two new protocols, a one-way two-party quantum secure direct communication (QSDC) protocol and a two-way three-party controlled quantum dialogue (CQD) protocol. We have shown that the proposed protocols are unconditionally secure against various attacks, such as the intercept-resend attack, the denial of service attack, and the man-in-the-middle attack. The CQD protocol, in particular, is shown to be secure against an attack by an untrusted Charlie. Also, for the intercept-resend attack, the mutual information gained between Alice and Eve is shown to be much lower for the proposed protocols as compared to the qubit-based protocols such as the LM05/DL04 protocol [8,9], thus making the proposed protocols more secure than the LM05/DL04 against this attack. Also, unlike the qubit-based protocols which transfer just one bit per state, the proposed protocols can transfer multiple bits per state [33], which can possibly lead to advantages such as the faster transmission of messages and a lower requirement of resources (both subject to practical/experimental conditions). These direct communication schemes could potentially lead to secure feasible solutions for many social and economic problems such as the socialist millionaire problem [34], quantum E-commerce [35], quantum voting [36], and the work towards finding these potential solutions are to be attempted in the future.

Acknowledgements SS and CMC would like to thank Department of Science and Technology, Government of India, for the Ramanujan Fellowship Grant No.:SB/S2/RJN-192/2014. We also acknowledge the support from Interdisciplinary Cyber Physical Systems (ICPS) programme of the Department of Science and Technology, India, Grant No.:DST/ICPS/QuST/Theme-1/2019/1.

Appendix

LM05/DL04 protocol

This qubit-based protocol was introduced in [8,9]. In this protocol, the encoding rules for the message sender are as follows:

To encode the bit 0, do nothing to the incoming qubit.

To encode the bit 1, apply the operator $iY = ZX$ on the incoming qubit. The transformations are as follows:

$$\begin{aligned} iY|0\rangle &= -|1\rangle \\ iY|1\rangle &= |0\rangle \\ iY|\pm\rangle &= \pm|\mp\rangle \end{aligned}$$

The protocol is as follows:

1. Alice chooses n random qubits from the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and sends them to Bob.
2. Out of these n qubits received from Alice, Bob randomly chooses $n/2$ of them and classically sends their coordinates to Alice.
3. Alice publicly announces the states of the $n/2$ qubits which Bob chose in step 2. Bob measures each of the $n/2$ qubits in their corresponding bases and checks for eavesdropping. If the error is within a tolerable limit, then the protocol continues to step 4. Else, the protocol is discarded and they start all over again.
4. Among the remaining $n/2$ qubits, Bob randomly chooses $n/4$ of them and encodes the message in them according to the encoding rules above and does nothing to the remaining $n/4$ qubits. He sends all these $n/2$ qubits back to Alice.
5. After Alice confirms receiving the $n/2$ qubits, Bob sends the coordinates of the qubits on which he did not encode the message. Alice uses these qubits to check for eavesdropping just like how Bob does it in step 3.
6. After confirming no eavesdropping, Alice measures the remaining qubits in their respective bases to obtain the message sent by Bob.

Mutual information

Let us take two random variables, say x and y. The mutual information I_{XY} between two random variables x and y is the decrease in uncertainty of one random variable when the value of the other random variable is observed, measured, or determined. If x and y are discrete, the formula for I_{XY} is given by [37]

$$I_{XY} = \sum_{x}\sum_{y} p(x, y) log_2 \frac{p(x, y)}{p(x)p(y)} \tag{15}$$

where $p(x, y)$ is the joint probability mass function and $p(x)$ and $p(y)$ are the individual probability mass functions.
If x and y are continuous, then the formula for I_{XY} is given by

$$I_{XY} = \int_{x}\int_{y} p(x, y) log_2 \frac{p(x, y)}{p(x)p(y)} dxdy \tag{16}$$

where $p(x, y)$ is the joint probability density function and $p(x)$ and $p(y)$ are the individual probability density functions.

There can also be a case where one of the random variables is discrete and the other is continuous. For example, if x is discrete and y is continuous, then the formula for I_{XY} becomes

$$I_{XY} = \sum_{x}\int_{y} p(x, y) log_2 \frac{p(x, y)}{p(x)p(y)} dy \tag{17}$$

where $p(x)$ is the probability mass function of x, $p(y)$ is the probability density function of y, and $p(x, y)$ is a function that is a probability density-mass function that is discrete in x and continuous in y.

This concept of mutual information can also be generalised to $r = mn > 2$ random variables $\{x_1, x_2, ..., x_m\}$ and $\{y_1, y_2, ..., y_n\}$ where x_i are discrete and y_i are continuous. The generalised mutual information I_{mutual} is given by [37]

$$I_{mutual} = \sum_{x_1, x_2, ..., x_n} \int_{y_1, ..., y_n} p(x_1, x_2, ..., x_m, y_1, y_2, ..., y_n) log_2 \frac{p(x_1, x_2, ..., x_m, y_1, y_2, ..., y_n)}{p(x_1)p(x_2)...p(x_m)p(y_1)p(y_2)...p(y_n)} dy_1 dy_2 ... dy_n. \tag{18}$$

Mutual information for the intercept-resend attack for the LM05/DL04 protocol

Let us consider the first transmission from Alice to Bob. In this transmission, Alice first selects either of the four states and prepares them and sends them to Bob. Eve intercepts this channel before the state reaches Bob and randomly chooses a basis for each incoming state and measures the state in that basis. Let $a, e \in \{0, 1, +, -\}$. Let the probability of Alice sending the qubit a and Eve receiving the qubit e be $p(a, e)$.

For example, the probability $p(0,0)$ is

$$p(0,0) = \overset{probability\ of\ Alice\ choosing\ 0}{\frac{1}{4}} \times \overset{probability\ of\ Eve\ choosing\ the\ computational\ Z\ basis}{\frac{1}{2}} \times \overset{probability\ of\ Eve\ getting\ 0}{1} = \frac{1}{8}. \tag{19}$$

Similarly,

$$p(0,1) = \frac{1}{4} \times \frac{1}{2} \times 0 = 0, \tag{20}$$

$$p(0,+) = \frac{1}{4} \times \frac{1}{2} \times \frac{1}{2} = \frac{1}{16}, \tag{21}$$

$$p(0,-) = \frac{1}{4} \times \frac{1}{2} \times \frac{1}{2} = \frac{1}{16}, \tag{22}$$

and similar probabilities for $p(1,e)$, $p(+,e)$, and $p(-,e)$, where $e \in \{0,1,+,-\}$.

Hence, the mutual information I_{AE} for the LM05/DL04 protocol is given by

$$\begin{aligned} I_{AE} &= \sum_a \sum_e p(a,e) log_2 \frac{p(a,e)}{p(a)p(e)} \\ &= 4\left(\frac{1}{8} log_2 \frac{\frac{1}{8}}{\frac{1}{16}} + \frac{1}{16} log_2 \frac{\frac{1}{16}}{\frac{1}{16}} + \frac{1}{16} log_2 \frac{\frac{1}{16}}{\frac{1}{16}}\right) = 0.5. \end{aligned} \tag{23}$$

(We can see that for all a and e, $p(a) = p(e) = \frac{1}{4}$. Hence, $p(a)p(e) = \frac{1}{16}$).

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. arXiv preprint arXiv:2003.06557 (2020)
2. Bennett, Charles H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**(21), 3121 (1992)
3. Ekert, Artur K.: Quantum cryptography based on bell's theorem. Phys. Rev. Lett. **67**(6), 661 (1991)
4. Lo, Hoi-Kwong, Chau, Hoi Fung: Is quantum bit commitment really possible? Phys. Rev. Lett. **78**(17), 3410 (1997)
5. Bostrom, Kim, Felbinger, Timo: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. **89**(18), 187902 (2002)
6. Long, G.L., Liu, X.S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A **65**, 032302 (2002)
7. Deng, Fu-Guo, Long, Gui Lu, Liu, Xiao-Shu: Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys. Rev. A **68**, 042317 (2003)
8. Deng, Fu-Guo, Long, Gui Lu: Secure direct communication with a quantum one-time pad. Phys. Rev. A **69**, 052319 (2004)
9. Lucamarini, Marco, Mancini, Stefano: Secure deterministic communication without entanglement. Phys. Rev. Lett. **94**(14), 140501 (2005)
10. Zhou, Lan, Sheng, Yu-Bo, Long, Gui-Lu: Device-independent quantum secure direct communication against collective attacks. Sci. Bull. **65**, 12 (2020)

11. Niu, P.H., Zhou, Z.R., Lin, Z.S., Sheng, Y.B., Yin, L.G., Long, G.L.: Measurement-device-independent quantum communication without encryption. Sci. Bull. **63**, 1345 (2018)
12. Zhou, ZengRong, Sheng, YuBo, Niu, PengHao, Yin, LiuGuo, Long, GuiLu, Hanzo, Lajos: Measurement-device-independent quantum secure direct communication. Sci. China Phys. Mech. Astron. **63**, 230362 (2020)
13. Nguyen, Ba An: Quantum dialogue. Phys. Lett. A **328**(1), 6–10 (2004)
14. Thapliyal, Kishore, Pathak, Anirban: Applications of quantum cryptographic switch: various tasks related to controlled quantum communication can be performed using bell states and permutation of particles. Quantum Inf. Process. **14**(7), 2599–2616 (2015)
15. Jian-Yong, Hu, Bo, Yu., Jing, Ming-Yong, Xiao, Lian-Tuan, Jia, Suo-Tang, Qin, Guo-Qing, Long, Gui-Lu: Experimental quantum secure direct communication with single photons. Light Sci. Appl. **5**, e16144 (2016)
16. Zhang, Wei, Ding, Dong-Sheng, Sheng, Yu-Bo, Zhou, Lan, Shi, Bao-Sen, Guo, Guang-Can: Quantum secure direct communication with quantum memory. Phys. Rev. Lett. **118**, 220501 (2017)
17. Zhu, Feng, Zhang, Wei, Sheng, Yubo, Huang, Yidong: Experimental long-distance quantum secure direct communication. Sci. Bull. **62**, 1519 (2017)
18. Aharonov, Yakir, Davidovich, Luiz, Zagury, Nicim: Quantum random walks. Phys. Rev. A **48**(2), 1687 (1993)
19. Santha, M.: Quantum walk based search algorithms, vol. 31–46 (2008)
20. Chawla, Prateek, Ambarish, C.V., Chandrashekar, C.M.: Quantum percolation in quasicrystals using continuous-time quantum walk. J. Phys. Commun. **3**(12), 125004 (2019)
21. Badhani, H., Chandrashekar, C.M.: Gravitationally induced entanglement between two quantum walkers. arXiv preprint arXiv:1907.06953 (2019)
22. Yang, Yuguang, Yang, Jiajie, Zhou, Yihua, Shi, Weimin, Chen, Xiubo, Li, Jian, Zuo, Huijuan: Quantum network communication: a discrete-time quantum-walk approach. Sci. China Inf. Sci. **61**(4), 042501 (2018)
23. Vlachou, Chrysoula, Krawec, Walter, Mateus, Paulo, Paunkovic, Nikola, Souto, Andre: Quantum key distribution with quantum walks. Quantum Inf. Process. **17**(11), 288 (2018)
24. Vlachou, Chrysoula, Rodrigues, J., Mateus, Paulo, Paunkovic, N., Souto, Andre: Quantum walk public-key cryptographic system. Int. J. Quantum Inf. **13**(07), 1550050 (2015)
25. Banerjee, Subhashish, Srikanth, R., Chandrashekar, C.M., Rungta, Pranaw: Symmetry-noise interplay in quantum walk on an n-cycle. Phys. Rev. A **78**(5), 052316 (2008)
26. Kempe, Julia: Quantum random walks: an introductory overview. Contemp. Phys. **44**(4), 307–327 (2003)
27. Meyer, D.A.: From quantum cellular automata to quantum lattice gases. J. Stat. Phys. **85**(5–6), 551–574 (1996)
28. Chandrashekar, C.M., Srikanth, R., Laflamme, R.: Optimizing the discrete time quantum walk using a SU(2) coin. Phys. Rev. A **77**(3), 032326 (2008)
29. Wang, Jingbo, Manouchehri, Kia: Physical Implementation of Quantum Walks. Springer, Berlin (2013)
30. Little, M.J., et al.: 2D optical switch. U.S. Patent No. 6,396,976 (28 May 2002)
31. Donald, D.K.: Thermal optical switches for light. U.S. Patent No. 6,212,308 (3 Apr. 2001)
32. Dorn, R., Kersten, P., Rehm, W., Wischmann, W.: Optical switch. U.S. Patent No. 5,319,492 (7 Jun. 1994)
33. Sarkar, Anupam, Chandrashekar, C.M.: Multi-bit quantum random number generator from a single qubit quantum walk. Sci. Rep. **9**(1), 12323 (2019)
34. Saxena, A., Thapliyal, K., Pathak, A.: Continuous variable controlled quantum dialogue and secure multiparty quantum computation. arXiv preprint arXiv:1902.00458 (2019)
35. Thapliyal, Kishore, Pathak, Anirban: Quantum e-commerce: a comparative study of possible protocols for online shopping and other tasks related to e-commerce. Quantum Inf. Process. **18**(6), 191 (2019)
36. Thapliyal, Kishore, Sharma, Rishi Dutt, Pathak, Anirban: Protocols for quantum binary voting. Int. J. Quantum Inf. **15**(01), 1750007 (2017)
37. Ince, R.A.A., Panzeri, S., Schultz, S.R.: Summary of information theoretic quantities. arXiv preprint arXiv:1501.01854 (2015)