**ISSN Print:** 2394-7500
**ISSN Online:** 2394-5869
**Impact Factor:** 5.2
IJAR 2017; 3(8): 818-825
www.allresearchjournal.com
Received: 23-06-2017
Accepted: 26-07-2017

**Vandana Vanegal**
Research Scholar, Department of Physics, CCS University Meerut, Utter Pradesh, India

**Correspondence**
**Vandana Vanegal**
Research Scholar, Department of Physics, CCS University Meerut, Utter Pradesh, India

# Secure quantum communication with orthogonal states based actual transmission of qubits

**Vandana Vanegal**

## Abstract

We have seen that secure and efficient quantum communication is possible using arbitrary, orthogonal multi-partite quantum state. The orthogonal-state-based protocols described in the previous chapter are extremely interesting as they are fundamentally different from the existing conjugate-coding-based BB84-type protocols. In this chapter, we aim to propose another orthogonal-state-based protocol of DSQC. More precisely, the obstacles are placed in the lower arm of a Mach-Zehnder interferometer and a single photon is sent through the input port. The presence of the obstacle disrupts the destructive interference that would otherwise occur, thereby revealing the presence of the obstacle. This type of interaction-free measurements is referred to as counterfactual and aquantum cryptographic protocol that uses interaction-free measurement to avoid the transmission of information carrying qubits over the quantum channel accessible to Eve is referred to as a counterfactual protocol. However, till the recent past orthogonal-state-based protocols were only a theoretical concept and were limited to QKD. Only recently, orthogonal-state-based protocols of QKD are experimentally realized and extended to cryptographic tasks beyond QKD. This paper aims to briefly review the orthogonal-state-based protocols of secure quantum communication that are recently introduced by our group and other researchers. The protocol is shown to be unconditionally secure. Interestingly, it is found that the protocol is not maximally efficient. The proposed orthogonal-state-based protocol may have many useful applications in experimental quantum cryptography, as it provides a wide choice of quantum states that can be generated with nowadays technology.

**Keywords:** Quantum communication using orthogonal states, DSQC, QSDC, QKD, quantum cryptography

## Introduction

We have seen that secure and efficient quantum communication is possible using arbitrary, orthogonal multi-partite quantum state. The orthogonal-state-based protocols described in the previous chapter are extremely interesting as they are fundamentally different from the existing conjugate-coding-based BB84-type protocols. In this chapter, we aim to propose another orthogonal-state-based protocol of DSQC. Similar to the protocols of the previous chapter, the protocol presented here is a GV-type [5] protocol of DSQC, which uses only orthogonal states for encoding, decoding and error checking, as was done in the original GV protocol of QKD. We mentioned that GV protocol was introduced in 1995, but for a few years, it remained isolated as the only orthogonal-state-based protocol of QKD. In 1999, Guo and Shi [26] introduced an interesting orthogonal-state-based protocol of QKD using interaction-free measurement or quantum interrogation [49]. The idea of interaction-free measurement was introduced earlier by Elitzur and Vaidman in the context of a hypothetical situation in which obstacles placed in the arm of a Mach-Zehnder interferometer can be detected even without a particle physically interacting with it. More precisely, the obstacles are placed in the lower arm of a Mach-Zehnder interferometer and a single photon is sent through the input port. The presence of the obstacle disrupts the destructive interference that would otherwise occur, thereby revealing the presence of the obstacle. This type of interaction-free measurements is referred to as counterfactual and quantum cryptographic protocol that uses interaction-free measurement to avoid the transmission of information carrying qubits over the quantum channel accessible to Eve is referred to as a counterfactual protocol. In 2009, a decade after the work of Guo and Shi, another orthogonal-state-based protocol along the same line was proposed by T.-G. Noh using the idea of counter factuality.

This protocol of Noh is known as N09 protocol [25] or counterfactual protocol. We have already mentioned that orthogonal-state-based protocols are important because they are fundamentally different from the conjugate-coding-based $BB_{84}$-type protocols. Interestingly, importance of orthogonal-state-based protocols are not limited to foundational aspects only, they are also of practical importance as they are experimentally realizable [28–31]. To be precise, recently, GV protocol is experimentally realized [28]. A set of successful implementations of N09 protocol is also reported [30, 31]. The foundational importance and the recent experimental achievements have motivated us to investigate the power of orthogonal-state-based protocols from various aspects. The foundational importance and the recent experimental achievements have also motivated others to employ counter factuality to propose a protocol of direct quantum communication. To be precise, recently, Salih *et al.* [35] have provided a very interesting protocol of direct counter factual quantum communication using chained quantum Zeno effect. Although, Salih *et al*. had not made any effort to make their protocol secure, the protocol is extremely interesting as the authors claimed that direct quantum communication between Alice and Bob is possible without actual transmission of particles between them. This claim, which is equivalent to counter factuality, is criticized by Vaidman [40], who argued that the actual measurement of the presence of the qubits in the transmission channel contradicts the claim of Salih *et al.* These recent developments in orthogonal-state-based quantum communication motivated us to investigate the possibility of designing a protocol of DSQC under the condition that transmission of particles is allowed, but the transmission of information encoded qubits is not allowed. This condition, which does need counter factuality, maybe viewed as a weaker version of the condition imposed by Salih *et al.* and it may be referred to as the weak condition. Remaining within this weak condition, in this chapter, we propose an entanglement swapping-based DSQC protocol which may be realized using various quantum states of a specific form. In the protocol proposed in this paper, PoP plays an important role. In all the protocols of secure direct quantum communication that are described so far, the qubits on which Alice encodes a message travel through the quantum channel. In contrast, no such transmission happens in recently proposed Zhang *et al.* [91] protocol of secure direct quantum communication and Salih *et al.* [35] protocol of direct quantum communication. Extending their ideas [35, 91], we aim to show that there exists a class of quantum states that may be used to implement GV-type protocol of DSQC that would be free from the transmission of information encoded qubits. In this paper, we present such a protocol.

## General form of the quantum state

We are interested to design a protocol of DSQC that can transmit an n-bit message using the quantum states of the form

|ψi= 1 √2n 2n ∑ i=1|eii|fii,

Where, {|eii}is a basis set inC2m : m≥n and each of the basis vectors is an m-qubit maximally entangled state (consequently, m≥2), and {|fii} is a basis set in C2l : l ≥n≥1. It is not essential for the basic elements of {|fii} to be in an entangled state. Thus, |ψi is an m+l qubit state. Since {|eii} and {|fii} are basis sets, i6 = i0 implies that |ψi is an entangled state. In general, we demand |eii as maximally entangled m-qubit state. However, for the convenience of proof, we restrict ourselves to a specific case where |eii is an m-qubitcat state. Now, we assume that the quantum state |ψi is prepared by Alice. She keeps first m-qubits with herself and sends the remaining l qubits to Bob in a non-clonable manner. By non-clonable manner, we mean that Alice sends the qubits to Bob in such a way that Eve cannot clone the state |fii. Theterm 'non-clonable manner' will be explained below. Further, imagine that Alice has prepared another cat state |eji of the same dimension. The combined state |eji⊗|ψi can be expressed as follows

|ψ1i= 1 √2n 2n ∑ i=1|eji|eii|fii=|eji 1 √2n 2n ∑ i=1|eii|fii!.

In what follows, we will see that Alice encodes a secret j by creating |eji. Thus, the index j corresponds to a secret bit string indexed by j. From (6.2), it is clear that in |ψ1i the first m qubits (i.e., the qubits of |eji) are separable from the rest of the qubits. Consequently, any measurement on the rest of the qubits will not reveal any information about the state of the first m qubits. Let us see what happens if we allow Alice to perform entanglement swapping among first 2m qubits of this combined state (6.2). Specifically, we are interested to see the effect of entanglement swapping on|eji|eii. To do so, Alice may follow the following prescription. She takes first p= m 2 qubits from both the cat states (i.e., from|ejiand|eii) if m is even; otherwise, she takes p = m−1 2 qubits from both |ejiand|eii. Thus, Alice has a set of 2p qubits (this set is referred to as first set) and another set of 2(m−p) qubits (this set is referred to as second set). Before we proceed further, the notations used here can be made more precise using the convention used in [145]. Following [145], we can express an m-qubit cat state in general as follows

|ei = 1 √2 m ∏ k=1|uki±m ∏ k=1|uc ki!,

Where, the symbol uk stands for binary variable ∈{0,1} with uc k = 1−uk. The state of our interest is a finite superposition of products of two cat states. Let each of these cat states be labeled by q, where q = 1, 2 and the kth particle of the lth cat state is labeled by k(l). This summarizes the notations used here. Now, it is straightforward to recognize that the set of all states of 2 p qubits forms a complete or the normal basis set, and using the notation described here, the elements of such a basis set can be expressed as follows

|ψ(2p)i=2 ∏ q=1p ∏ k=1|uk(q)i±2 ∏ q=1p ∏ k=1|uc k(q)i

Now, we assume that Alice performs a projective measurement on the first set of qubits using cat basis of 2p dimension. The measurement on this basis implies that we operate |ψ(2p)ihψ(2p)|on|ψ1i. The operation would collapse the first set of qubits into one of the cat states in 2p dimension. Remaining (2m−2p) qubits of |eji|eii will be projected to a (2m−2p) cat state of the form [145]

|ψ(2m−2p)i=2 ∏ q=1m ∏ k=p+1|uk(q)i±2 ∏ q=1 m ∏ k=p+1|uc k(q)i.

The structure of (6.2) would ensure that the initial entanglement present between |eii and |fii (more precisely between first m particles and last l particles of |ψi) is now transferred between the (2m−2p) particles of |ψ(2m−2p)I and l particles of |fii. Now, if we consider a protocol in which Alice sends the last l qubits (i.e., qubits of|fii) to Bob and measures the first 2p qubits in 2p-qubit cat basis and the remaining (2m−2p) qubits of her possession in (2m−2p)-qubit cat basis and announces the outcomes, then Bob will be able to infer what was |eji (equivalently, the secret encoded by Alice which is indexed by j) by measuring his qubits in {|fii} basis and using the outcomes of Alice's measurement. Thus, it leads to a protocol of direct quantum communication. At a first glance, any protocol designed along the above line of arguments does not appear to be secure as {|fii} is orthogonal and measurement outcomes of Alice are public knowledge. Conventionally, orthogonal states can be perfectly measured and thus cloned. A measurement by Eve in {|fii} basis will destroy the entanglement, but Alice and Bob will not be able to trace Eve if they apply the above idea without using any strategy for eavesdropping check. Further, if Eve is allowed to measure the states communicated by Alice in {|fii} basis, then she is also capable to clone the states [48] and the protocol would fail. However, it is possible to design strategy in which orthogonal states are communicated in such a way that Eve does not have access to the basis set in which the communicated states are basis elements (i.e., the basis set in which the communicated states are perfectly measurable). This restriction on the basis sets available to Eve implies no-cloning [48] and when orthogonal states are communicated using such a strategy, then we say that the states are communicated in a non-clonable manner. To communicate the orthogonal states of {|fii} basis in a non-clonable manner, we need to ensure that Eve does not have access to {|fii} basis. This is possible in several ways. For example, non-clonable communication is possible if the physical realizations of all the states in {|fii} basis are such that they may be visualized as superposition of two or more pieces that can be geographically separated. For example, in the original GV protocol [5], orthogonal states |φ0i= |ai+|bi √2 and |φ1i= |ai−|bi √2 are used to communicate bit values 0 and 1, respectively, but Alice sends the states in such a way that the components |ai and |bi are realized by spatiotemporally separated wave packets, so that |bi is guaranteed to leave Alice's site only after |ai has arrived at Bob's site. This strategy implies that Eve does not have simultaneous access to |ai and |bi and as a consequence, Eve cannot perform a measurement in n|ai+|bi √2, |ai−|bi √2 obasis. Eve's in ability to perform a measurement in n|ai+|bi √2, |ai−|bi √2 o basis implies that she can neither perform a perfect measurement nor perform cloning operation [48]. Thus, in the GV protocol, orthogonal states are communicated in a non-clonable manner. We are not interested to follow the original GV idea to communicate |fii in a non-clonable manner as GV idea requires strict time checking which difficult to achieve experimentally. We [32] and Yadav *et al*. [33] have recently generalized the GV idea and have suggested another strategy of non-clonable communication of orthogonal states by using the fact that entangled states are nothing but superposition in tensor product space. In our procedure, strict time checking is not required. To be precise, Alice can concatenate a set of decoy qubits prepared in Bell states (say Alice prepares |ψ+i⊗N 2 =|00i+|11i √2 ⊗N 2) with an N-qubit string that she wants to transmit to Bob and randomly rearrange the particle ordering i.e., apply PoP technique and thus restrict the basis available to Eve. PoP will ensure that Eve cannot clone, or measure the decoy qubits as she does not know which qubits are mutually entangled. Further, Eve will not be able to selectively clone, or measure non-decoy qubits as after application of PoP, she has no way to isolate decoy qubits from the other qubits. As perfect measurement by Eve is not possible due to unavailability of {|fii} basis, any measurement and/or cloning attempt by Eve will leave a signature that can be traced by measuring and comparing the decoy qubits. In summary, Alice can always communicate last l qubits of (6.1) to Bob in a non-clonable manner and that in turn ensures protection against measurement and resend attack and CNOT (Cloning) attack. Above facts lead us to a protocol of DSQC using entanglement swapping where actual transmission of the information encoded particles are not required.

Role of no-cloning and randomness in secure communication and how to transform BB84-type protocols to GV-type protocols**.** It is well known that unknown quantum states cannot be cloned and several proofs of no-cloning theorem are provided using unitary evolution [53], no-signaling [55], linearity [56]. A closer look into these proofs reveals that there exist fine differences among these proofs and those differences lead to a fundamental question: What nonclassical resources are required for the existence of no-cloning theorem in a the- ory *T*. Recently, we have shown that no-cloning theorem should hold in any theory possessing uncertainty and disturbance on measurement [57]. Thus we can construct post-quantum theories with no-cloning. Without going into detail of those theories, let us try to follow a simpler argument that can give us a general perception of no- cloning theorem. To begin with let us try to address another simple question: What distinguishes a completely stochastic classical theory from the quantum mechanics? Clearly, in a completely stochastic classical theory the outcomes of measurement are always probabilistic whereas in quantum mechanics we can have a deterministic outcome if the state to be measured is part of the basis set used for the measure- ment. For example, if we measure |0*)* in *{*|0*),* |1*)}* basis we will always get |0*)* (thus the outcome is deterministic as the state is part of the basis), but if we measure |0*)* in *{*|+*),* |−*)}* basis we will have probabilistic outcome. We may say that the *{*|0*),* |1*)}* basis is *special basis* as it leads to deterministic outcome. We may now generalize the idea and say that for measurement of a state a particular basis set will be referred to as special basis if the state can be perfectly measured in that basis. It is easy to recognize that existence of special basis implies perfect measurement and thus complete information of the state being measured. This information implies that the state is known and thus can be cloned. In contrast, absence of special basis implies no-cloning. As the elements of any basis set are orthogonal to each other, two non-orthogonal states cannot be part of the same basis set and thus cannot be cloned. However, this viewpoint does not demand that the orthogonal states can always be cloned. Specifically, by using geographical separation among the components of a superposition state we can make it non-clonable. In a completely different language this viewpoint was elaborated by Mor [53] in 1998. Of course Mor's work appeared after the GV protocol, but it helped us to understand and generalize GV protocol. Let us elaborate this point by briefly describing GV protocol.

### *Goldenberg-Vaidman (GV) protocol*

Let us consider two orthogonal states

$$^{2}|\psi_0) = \sqrt{2}\,(|a) + |b))$$

Where, $|a)$ and $|b)$ are two localized wave packets. Further, $|\psi_0)$ and $|\psi_1)$ represent bit values 0 and 1, respectively. Alice sends wave packets $|a)$ and $|b)$ to Bob by using two different arms of a Mach-Zehnder interferometer as shown in the Fig. 1 a. Alice sends Bob either $|\psi_0)$ or $|\psi_1)$, but $|a)$ is always sent first and $|b)$ is delayed by time $\tau$. Here traveling time ($\theta$) of wave packets from Alice to Bob is shorter than $\tau$. Thus $|b)$ enters the communication channel only after $|a)$ is received by Bob. Consequently, both the wave packets $|a)$ and $|b)$ (i.e., the entire superposition) are never found simultaneously in the transmission channel. This geographic separation between $|a)$ and $|b)$ restricts Eve from measuring the state communicated by Alice in $\{|\psi_0), |\psi_1)\}$ basis. In fact, this geographic separation method compels Eve to measure the state communicated by Alice either in $\{|a), |b)\}$ basis or in some suitably constructed positive-operator valued measure (POVM). Thus the geographic separation ensures unavailability of special basis and thus implies no-cloning and security of GV protocol. This is how one can look at the security of GV protocol using the concept of special basis or the idea of Mor [53]. Although the special basis is not available to Eve, it is available to Bob as Bob delays $|a)$ by $\tau$ and recreates the superposition state sent by Alice after he receives $|b)$. Alice and Bob compare the receiving time $t_r$ with the sending time $t_s$ for each state to ensure that Eve cannot delay $|a)$ and wait for $|b)$ to reach her so that she can do a measurement in $\{|\psi_0), |\psi_1)\}$. Specifically, Alice and Bob checks that $t_r = t_s + \theta + \tau$.

In the above we have already seen that it is possible to separate two pieces of orthogonal state and that leads to unavailability of special basis and thus no- cloning and orthogonal-state-based QKD. In what follows we will show that validity of GV-type protocol is not limited to single particle case and QKD, it can be easily generalized to multipartite case and to design protocols of DSQC and QSDC. Before we describe an orthogonal-state-based protocol of secure direct quantum communication, we wish to note that GV in its original form is a protocol of QKD only and it cannot be directly used for secure direct quantum communication. Keeping this in mind, let us first describe a conjugate coding based protocol of secure direct quantum communication. The protocol is popularly known as ping-pong (PP) protocol 15 and is described in the following section.

### *Ping-pong and modified ping-pong protocols*

Ping-pong (PP) protocol which was introduced by Bostr¨om and Felbinger in 2002 [15] is a protocol of QSDC and it may be described briefly as follows [23]:

**PP1** Bob prepares $n$ copies of the Bell state $|\psi^+) \equiv \sqrt{1}\ (|00) + |11))_{AB}$ (i.e.,$|\psi^+)\otimes n$), and transmits all the first qubits of the Bell pairs to Alice, keeping all the second particles with himself.

**PP2** Alice randomly selects a set of $\underline{n}$ qubits from the string$_2$ received by her as a verification string, and applies the BB84 subroutine[b] on the verification string to detect eaves dropping. If sufficiently few errors are found, they proceed to the next step; else, they return to the previous step.

**PP3** Alice randomly selects half of the unmeasured qubits as verification string for the return path and encodes her message in the remaining $\frac{n}{4}$ qubits using following rule: Alice does nothing to encode 0 on a message qubit, and applies an $X$ gate to encode 1. After completion of the encoding operation, she sends all the $\underline{n}$ $_2$ qubits of her possession to Bob.

**PP4** Alice discloses the coordinates of the verification qubits after receiving authenticated acknowledgment of receipt of all the qubits from Bob. Bob applies the BB84 subroutine on the verification qubits and computes the error rate. If sufficiently few errors are found, they proceed to the next step; else, they return to PP1. [b]BB$_{84}$ subroutine means eavesdropping is checked by following a procedure similar to that adopted in the original BB84 protocol. Specifically, BB84 subroutine implies that Alice (Bob) randomly selects half of the qubits received by her (him) to form a verification string. She (He) measures verification qubits randomly in $\{0,\ 1\}$ or $\{+,\ -\}$ basis and announces the measurement outcome, position of that qubit in the string and the basis used for the particular measurement. Bob (Alice) also measures the corresponding qubit using the same basis (if needed) and compares his (her) results with the announced result of Alice (Bob) to detect eavesdropping.

**PP5** Bob performs Bell-state measurements on the remaining Bell pairs, and de- codes the message. If in PP3 Alice has encoded 0 then Bob will obtain $|\psi^+)$ (the same as he had sent) in PP5, otherwise he will receive $|\varphi^+)$. Since $|\psi^+)$ and $|\varphi^+)$ are orthogonal a Bell measurement will deterministically distinguish $|\psi^+)$ and $|\varphi^+)$ and consequently decode the message encrypted by Alice. This two-way protocol is referred to as the ping-pong protocol as the travel qubit moves from Bob to Alice and comes back just like a table tennis (ping-pong) ball which moves back and forth between two sides of the table. It is easy to observe that in the original PP protocol full power of dense coding is not used. Alice could have used $I$, $X$, $iY$ and $Z$ to encode 00, 01, 10 and 11 respectively and that would have increased the efficiency of ping-pong protocol. This is so because the same amount of communication would have successfully carried two bits of classical information. This fact was first formally included in a modified PP protocol proposed by Cai and Li in 2004 [25]. In fact, in principle any entangled state can be used to design a ping-pong type protocol for QSDC.

Here it is interesting to observe that in the above version of PP protocol (and in CL protocol) encoding and decoding of information is done by using orthogonal states alone. However, the eavesdropping checking is done with the help of BB$_{84}$ subroutine. Thus to convert PP protocol into an orthogonal-state-based protocol we would require to replace BB$_{84}$ subroutine $_2$ by a GV-type subroutine for eaves-dropping check. While describing the role of special basis on the origin of security of GV protocol, we have already mentioned that if we can visualize an orthogonal state as superposition of two quantum pieces that are geographically separable then the orthogonal state can be transmitted in such a way that Eve can neither clone it nor measure it without disturbing. In addition, we may note that an entangled state is a superposition in tensor product space. Now just consider a simple situation that Alice prepares a product of two Bell states say $|\psi^+)\otimes 2 = |\psi^+\psi^+)_{1234}$ and randomly changes the sequence of the particles and sends them to Bob over a channel. Now Eve knows that two Bell states are sent and she has to do a Bell measurement to know which Bell state is sent, but she does not know which particle is entangled to which particle. Consequently, any wrong choice of partner particles would lead to entanglement swapping (say∉if Eve does Bell measurement on 13 and/or 24 that would lead to entanglement swapping). Now consider that at a later time, when Bob informs Alice that he has received 4 qubits then Alice discloses the actual sequence of the transmitted qubits and Bob uses that data to rearrange the qubits in his hand into the original sequence and perform Bell measurement on them. Clearly, attempts of eavesdropping will leave detectable traces through the entanglement swapping and whenever Bob's Bell measurement would yield any result other than $|\psi^+)$ they will know there exists a Eve. Clearly, this new eavesdropping checking subroutine is of GV-type as it uses orthogonal states only and as it geographically separates two quantum pieces of an orthogonal state. Further, PoP technique applied here actually ensures that the special basis (Bell basis in this case) is not available with Eve when the particles are in the channel, but after Alice's disclosure of the actual sequence of the qubit, Bob obtains access to the special basis. Once we understand the essence of this strategy, we may generalize it to develop a GV-type subroutine as follows:

1. To communicate a sequence $A$ of $n$ message qubits, Alice creates an additional sequence $D$ of $n$ decoy qubits prepared as $|\psi^{\otimes} 2\,)$.
2. She concatenates $D$ with $A$ to obtain a new sequence $P$ of $2n$ qubits and applies a permutation operator $\Pi_{2n}$ on $P$ to yield $P^j = \Pi_{2n}P$.
3. After receiving authenticated acknowledgment from Bob that he has received all the $2n$ qubits sent to him, Alice discloses the actual sequence of the decoy qubits only (she does not disclose the sequence of message qubits) so that Bob can perform Bell measurement on partner particles (original Bell pairs) and reveal any effort of eavesdropping through the disturbance introduced by Eve's measurements.

As the message qubits are also randomized and as Alice does not disclose the actual sequence till she knows that eavesdropping has not happened. Above subroutine for eavesdropping checking which we referred to as GV subroutine can be used to convert any BB84-type protocol of secure quantum communication that utilizes orthogonal states for encoding and decoding. For example, PP [15], Cai-Li [25] and DLL [58] protocol can be converted easily into GV-type protocol. This idea is extensively discussed in our recent publications [20, 34, 35, 36]. For the completeness of the present paper we elaborate this point here by explicitly describing a GV-type version of PP protocol which we referred to as PP $^{GV}$. More detail about this protocol can be found at Refs [23, 35].

### *PP$^{GV}$ protocol*

2 In what follows we briefly describe the PP$^{GV}$ protocol introduced by Yadav, Srikanth and Pathak [35]. We can convert PP protocol to PP$^{GV}$ protocol by modifying steps PP1, PP2 and PP4 of PP protocol described above as follows: PP$^{GV}$1 Bob prepares the state $|\psi^+)\otimes n$. He keeps half of the second qubits of the Bell pairs with himself. On the remaining $\underline{3n}$ qubits he applies a random permutation operation $\Pi$ 3$n$ and transmits them to Alice. $n$ of the transmitted qubits are Bell pairs and the remaining $\underline{n}$ are the partner particles of the particles which remained with Bob.

**PP$^{GV}$2:** After receiving Alice's authenticated acknowledgment; Bob announces $\Pi_n$ $\Pi$ 3$n$, the coordinates of the transmitted Bell pairs. Alice measures them in the Bell basis to determine if they are each in the state $|\psi^+)$. If the error detected by Alice is within the tolerable limit, they continue to the next step. Otherwise, they discard the protocol and restart from PP$^{GV}$1.

**PP$^{GV}$4:** Alice discloses the coordinates of the verification qubits after receiving Bob's authenticated acknowledgment of receipt of all the qubits. Bob combines the qubits of verification string with their partner particles already in his possession and measures them in the Bell basis to compute the (return trip) error rate.

The other steps in PP remain the same. Briefly, security in PP$^{GV}$ and CL$^{GV}$ arises as follows. The reordering has the same effect as time control and time randomization in GV. Eve is unable to apply a 2-qubit operation on legitimate partner particles to determine the encoding in spite of their orthogonality. Any correlation she generates by interacting with individual particles will diminish the observed correlations between Alice and Bob because of restrictions on shareability of quantum correlations [35]. It is not our purpose⊿to discuss the security of the protocol in detail here. Interested readers may found detailed discussions on the security of PP$^{GV}$ in Refs [34, 35]. The PP$^{GV}$ protocol of Yadav, Srikanth and Pathak was the first ever orthogonal-state-based protocol of QSDC.

PP protocol described above is a two way protocol in the sense that the qubits travel in both the direction (i.e., from Alice to Bob and Bob to Alice). However, it is possible to modify them into one-way protocols. A very interesting one-way protocol known as DLL protocol was introduced by Deng, Long and Liu in 2003 [58]. This protocol can be obtained by modifying CL protocol. In what follows we will describe DLL protocol and subsequently modify that to a GV-type protocol which we refer to as DLL$^{GV}$. A relatively detailed description of this protocol can be found at Ref [23]. Before we describe DLL protocol we may note that after PP1, Alice and Bob share entanglement. To share an entanglement it is not required to be created by Bob as in PP protocol, even Alice can create an entangled state and send a qubit to Bob. Let us modify the first step of PP protocol and see what happens.

### DLL protocol

**DLL1:** Alice prepares the state $|\psi^+)\otimes n$, where $|\psi^+) \equiv \sqrt{1}$ $(|00) + |11))_{AB}$, and transmits all the second qubits (say B) of the Bell pairs to Bob, keeping the other half (A) with herself.

**DLL2:** Bob randomly chooses a set of $\underline{n}$ qubits from the string received by him to form a verification string, on which the BB84 subroutine to detect eavesdrop- ping is applied. If sufficiently few errors are found, they proceed to the next step; else, they return to DLL1.

**DLL3:** Alice randomly chooses half of the qubits in her possession to form the verification string for the next round of communication, and encodes her mes4sage in the remaining $n$qubits. To encode a 2-bit key message, Alice applies one of the four Pauli operations *I, X, iY, Z* on her qubits. Specifically, to encode 00, 01, 10 and 11 she applies *I, X, iY* and *Z*, respectively. After the encoding operation, Alice sends all the qubits in her possession to Bob.

**DLL4:** Alice discloses the coordinates of the verification qubits after receiving authenticated acknowledgment of receipt of all the qubits from Bob. Bob applies a BB84 subroutine to the verification string and computes the error rate.

**DLL5:** If the error rate is tolerably low, then Bob decodes the encoded states via a Bell-state measurement on the remaining Bell pairs. DLL protocol described in this way helps us to illustrate the symmetry among PP, CL and DLL protocols. This is a one-way two-step QSDC protocol. DLL protocol looks similar to PP protocol with dense coding (i.e., CL protocol). However, there is a fundamental difference between a two-way protocol and a two-step one-way protocol which uses the same resources and encoding operations. The difference lies in the fact that in a two-way protocol home qubit always remains at sender's port but in a one-way two-step protocol both the qubits travel through the channel. At this specific point we observe a symmetry between DLL protocol and GV protocol. Here the superposition is broken into two pieces in such a way that the entire superposed (entangled) state is never available in the transmission channel but only the entire superposition (i.e., the superposed state or entangled state) contains meaningful information. Visualization of this intrinsic symmetry helps us to generalize DLL protocol to obtain an orthogonal version of GV protocol.

### The modified DLL protocol (DLL$^{GV}$)

Based on the reasoning analogous to the one used for turning PP to PP$^{GV}$, we may propose the following GV-like version of DLL, which may be called DLL$^{GV}$ in accordance with the recent work of Yadav, Srikanth and Pathak [35]. As before, we retain the steps of DLL, replacing only steps DLL1, DLL2 and DLL4 as follows 23, 35.

**DLL$^{GV}$1:** Alice prepares the state $|\psi^+)\otimes n$. She keeps half of the first qubits of the Bell pairs with herself. On the remaining 3*n* qubits she applies a random permutation operation Π 3*n* and transmits them to Bob; *n* of the transmitted qubits are Bell pairs while the remaining $n$ are the entangled partners of the particles remaining with Alice.

**DLL$^{GV}$2:** After receiving Bob's authenticated acknowledgment, Alice ann6unces $\Pi_n$ Π 3*n*, the coordinates of the transmitted Bell pairs. Bob measures them in the Bell basis to determine if they are each in the state $|\psi^+)$. If the error detected by Bob is within a tolerable limit, they continue to the next step. Otherwise, they discard the protocol and restart from DLL$^{GV}$1.

**DLL$^{GV}$4:** Same as PP$^{GV}$4, except that the return 'trip' is replaced by Alice's second onward communication. So two-way protocols of QSDC are now converted to one-way protocols. But still we need two steps. This motivates us to ask: Do we always need at least two steps for secure direct quantum communications? Apparently it looks so because if we send both the qubits of an entangled pair together then Eve may perform Bell measurement and find out the message. Even if Eve is detected afterward it would not be of any use because she has already obtained the message. However, using rearrangement of particle order (PoP) we can restrict Eve from measuring in Bell (special) basis and circumvent this problem. We have already used PoP in implementing PP$^{GV}$, CL$^{GV}$ and DLL$^{GV}$. Using PoP a one-step one-way protocol of DSQC is already provided by us in Ref [34]. However, due to space restriction we do not elaborate the one-step one-way orthogonal-state-based protocol here.

We end-up this section by drawing your attention to the fact that in all the existing protocols information splitting is done in such a way that Eve does not get access to the special basis. Thus unavailability of special basis leads to no-cloning and thus to secure quantum communication and in the above described orthogonal-state-based protocol we have primarily ensured unavailability of special basis by geographically separating a quantum state into two pieces and avoiding Eve's simultaneous access to both the pieces.

### Conclusions

It is shown that DSQC is possible without actual transmission of message string and the task can be performed with any member of a set of quantum states having generic form. The proposed protocol is based on Bose *et al.*'s idea of generalized entanglement swapping [145], and it is a GV-type orthogonal-state-based protocol of DSQC. We have also elaborated the working of the protocol by considering a special case where the initial state is a GHZ-like state. The protocol is different from most of the conventional DSQC protocols for the following three reasons: (1) It is an orthogonal-state-based protocols and except our recent proposals and the proposal. All other existing protocols of DSQC are based on conjugate coding. (2) In the proposed protocol, actual information encoded quantum state never propagates through the transmission channel. (3) The security of conventional QSDC and DSQC protocols, like that of BB84-class QKD protocols is based on conjugate coding, the security of the GV-type DSQC protocol proposed here is based on monogamy of entanglement. The present work provides a protocol of DSQ2C that is similar to the protocol of Salih *et al.* in the sense that it's an orthogonal-state-based protocol of quantum2 communication and the message qubits are not transmitted. However, in contrast to Salih *et al.*'s protocol the present protocol is secure and it does not employ counter factuality. The state described here and the proposed protocol is much more general. However, a protocol is useful only if it can be implemented using the quantum states that can be generated experimentally using the contemporary facilities. The protocol is shown to be unconditionally secure. Interestingly, it is found that the protocol is not maximally efficient.

### References

1. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, 1984, 175-179.
2. Ekert AK. Quantum cryptography based on Bell's Theorem. Phys. Rev. Lett 1991;67:661-663.

3. Bennett CH. Quantum cryptography using any two non-orthogonal states. Phys. Rev. Lett 1992;68:3121-3124.
4. Goldenberg L, Vaidman L. Quantum cryptography based on orthogonal states. Phys. Rev. Lett 1995;75:1239-1243.
5. Hillery M, Buzek V, Bertiaume A. Quantum secret sharing. Phys. Rev 1999;A59:1829-1834.
6. Liu J, Liu YM, Cao HJ, Shi SH, Zhang ZJ. Revisiting quantum secure direct communication with W state. Chin. Phys. Lett 2006;23:2652-2655.
7. Li XH, Deng FG, Li CY, Liang YJ, Zhou P, Zhou HY. Deterministic secure quantum communication without maximally entangled states. J Korean Phys. Soc 2006;49:1354-1359.
8. Yan FL, Zhang X. A scheme for secure direct communication using EPR pairs and teleportation. Euro. Phys. JB 2004;41:75-78.
9. Man ZX, Zhang ZJ, Li Y. Deterministic secure direct communication by using swapping quantum entanglement and local unitary operations. Chin. Phys. Lett 2005;22:18-21.
10. Hwang T, Hwang CC, Tsai CW. Quantum key distribution protocol using dense coding of three-qubit W state. Euro. Phys. J. D 2011;61:785-790.
11. Zhu AD, Xia Y, Fan QB, Zhang S. Secure direct communication based on secret transmitting order of particles. Phys. Rev. A 2006;73:022338.
12. Cao HJ, Song HS. Quantum secure direct communication with W state. Chin. Phys. Lett 2006;23:290-292.
13. Yuan H, Song J, Zhou J, Zhang G, Wei Xf. High-capacity deterministic secure four-qubit W state protocol for quantum communication based on order re-arrangement of particle pairs. Int. J Theo. Phys 2011;50:2403-2409.
14. Long GL, Liu XS. Theoretically efficient high-capacity quantum-key- distribution scheme. Phys. Rev. A 2002;65:032302.
15. Bostrom K, Felbinger T. Deterministic secure direct communication using entanglement. Phys. Rev. Lett 2002;89:187902.
16. Degiovanni IP, Berchera IR, Castelletto S, Rastello ML, Bovino FA, Colla AM. Quantum dense key distribution. Phys. Rev. A 2004;69:032310.
17. Lucamarini M, Mancini S. Secure deterministic communication without entanglement. Phys. Rev. Lett. 2005;94:140501.
18. An NB. Quantum dialogue. Phys. Lett. A 2004;328:6-10.
19. Shukla C, Kothari V, Banerjee A, Pathak A. On the group-theoretic structure of a class of quantum dialogue protocols. Phys. Lett. A 2013;377:518-527.
20. Shukla C, Alam N, Pathak A. Protocols of quantum key agreement solely us- ing Bell states and Bell measurement. Quant. Info. Process. In Press, 2014. DOI: 10.1007/s11128-014-0784-0.
21. Gisin N, Ribordy G, Tittel W, Zbinden H. Quantum cryptography. Rev. Mod. Phys 2002;74:145-195.
22. Long Gl, Deng Fg, Wang C, Li Xh, Wen K, Wang W.-y. Quantum se- cure direct communication and deterministic secure quantum communication. Front. Phys. China 2007;2:251-271.
23. Pathak A. Elements of quantum computation and quantum communication. CRC Press, Boca Raton, USA, 2013.
24. Traina P, Gramegna M, Avella A, Cavanna A, Carpentras D, Degiovanni IP. Review on recent groundbreaking experiments on quantum communication with orthogonal states. Quantum Matter 2013;2:153-166.
25. Cai Qy, Li Bw. Improving the capacity of the Bostr¨om-Felbinger protocol. Phys. Rev. A 2004;69:054301.
26. Tsai CW, Hsieh CR, Hwang T. Dense coding using cluster states and its application on deterministic secure quantum communication. Eur. Phys. J. D 2011;61:779-783.
27. Noh TG. Counterfactual quantum cryptography. Phys. Rev. Lett 2009;103:230501.
28. Guo GC, Shi BS. Quantum cryptography based on interaction-free measure- ment. Phys. Lett. A 1999;256:109-112.
29. Koashi M, Imoto N. Quantum cryptography based on split transmission of one-bit information in two steps. Phys. Rev. Lett. 1997;79:2383-2386.
30. Avella A, Brida G, Degiovanni IP, Genovese M, Gramegna M, Traina P. Experimental quantum-cryptography scheme based on orthogonal states. Phys. Rev. A 2010;82:062309.
31. Ren M, Wu G, Wu E, Zeng H. Experimental demonstration of counterfactual quantum key distribution. Laser Phys. 2011;21:755-760.
32. Brida G, Cavanna A, Degiovanni IP, Genovese M, Traina P. Experimental realization of counterfactual quantum cryptography. Laser Phys. Lett. 2012;9:247-252.
33. Liu Y, Ju L, Liang XL, Tang SB, Tu GLS, Zhou L et al. Experimental demonstration of counter- factual quantum communication. Phys. Rev. Lett 2012;109:030501.
34. Shukla C, Pathak A, Srikanth R. Beyond the Goldenberg-Vaidman protocol: Secure and efficient quantum communication using arbitrary, orthogonal, multi-particle quantum states. Int. J Quant. Info. 2012;10:1241009.
35. Yadav P,, Srikanth R, Pathak A. Generalization of the Goldenberg-Vaidman QKD protocol. arXiv: 2012;1209:4304.
36. Shukla C, Pathak A. Direct quantum communication without actual transmission of the message qubits. Quant. Info. Process. In Press, 2014, DOI: 10.1007/s11128- 014-0792-0. (2013).
37. Salih H, Li ZH, Al-Amri M, Zubairy MS. Protocol for direct counterfactual quantum communication. Phys. Rev. Lett 2013;110:170502.
38. Sun Y, Wen QY. Counterfactual quantum key distribution with high efficiency. Phys. Rev. A 2010;82:52318.
39. Guo Q, Cheng LY, Chen L, Wang HF, Zhang S. Counterfactual quantum- information transfer. arXiv: 2014;1404:6401.
40. Shenoy A, Srikanth R, Srinivas T. Counterfactual quantum certificate authorization. Phys. Rev. A 2014;89:052307.
41. Salih H. Protocol for counterfactually transporting an unknown qubit. arXiv: 2014;1404:2200.
42. Guo Q, Cheng LY, Chen L, Wang HF, Zhang S. Counterfactual entangle- ment distribution without

transmitting any particles. Optics express 2014;22:8970-8984.

43. Zhang JL, Guo FZ, Gao F, Liu B, Wen QY. Private database queries based on counterfactual quantum key distribution. Phys. Rev. A 2013;88:022334.
44. Salih H. Tripartite counterfactual quantum cryptography. arXiv: 2014;1404:5540.
45. Vaidman L. Comment on “Protocol for direct counterfactual quantum communication”. Phys. Rev. Lett 2014;112:208901.
46. Salih H, Li ZH, Al-Amri M, Zubairy MS, Salih et al. Reply. Phys. Rev. Lett 2014;112:208902.
47. Shenoy A, Srikanth R, Srinivas T. Semi-counterfactual cryptography, Europhys. Lett 2013;103:60008.
48. Deng FG, Long GL. Controlled order rearrangement encryption for quan- tum key distribution. Phys. Rev. A 2003;68:042315.
49. Banerjee A, Pathak A. Maximally efficient protocols for direct secure quantum communication. Phys. Lett. A 2012;376:2944-2950.
50. Shukla C, Banerjee A, Pathak A. Improved protocols of secure quantum communication using W states. Int. J Theor. Phys 2013;52:1914-1924.
51. Peres A. Quantum cryptography with orthogonal states?. Phys. Rev. Lett. 1996;77:3264.
52. Goldenberg L, Vaidman L. Goldenberg and Vaidman Reply. Phys. Rev. Lett 1996;77:3265.
53. Mor T. No cloning of orthogonal states in composite systems. Phys. Rev. Lett 1998;80:3137-3140.
54. Elitzur AC, Vaidman L. Quantum mechanical interaction-free measurements. Found. Phys 1993;23:987-997.
55. Gisin N. Quantum cloning without signaling. Phys. Lett. A 1998;242:1-3.
56. Wootters WK, Zurek WH. A single quantum cannot be cloned. Nature 1982;299:802-803.
57. Aravinda S, Yadav P, Srikanth R, Pathak A. Post-quantum cryptography. Communicated.
58. Deng FG, Long GL, Liu XS. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys. Rev. A 2003;68:042317.