International Journal of Applied Research

ISSN Print: 2394-7500
ISSN Online: 2394-5869
Impact Factor: 5.2
IJAR 2017; 3(7): 1340-1347
www.allresearchjournal.com
Received: 10-06-2017
Accepted: 17-07-2017

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

Orthogonal states based secure quantum communication without actual transmission of qubits

Vandana Vanegal

Abstract

In majority of protocols of secure quantum communication (such as, BB84, B92, etc.), the unconditional security of the protocols are obtained by using conjugate coding (two or more mutually unbiased bases). Initially all the conjugate-coding-based protocols of secure quantum communication were restricted to quantum key distribution (QKD), but later on they were extended to other cryptographic tasks (such as, secure direct quantum communication and quantum key agreement). In contrast to the conjugate-coding-based protocols, a few completely orthogonal-state-based protocols of unconditionally secure QKD (such as, Goldenberg-Vaidman (GV) and N09) were also proposed. 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.

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

Introduction

Quantum cryptography is now 30 years old as it was first introduced in 1984 when Bennett and Brassard [1] proposed the first protocol of quantum key distribution (QKD) which is now known as BB84 protocol. This pioneering work drew con-siderable attention of the entire cryptography community as it was successful in achieving unconditional security, a much desirable feat that is never achievable in the classical cryptography. To be precise, all the classical cryptographic protocols including the widely used RSA protocol are secure only under some assumptions, whereas quantum cryptographic protocols are unconditionally secure. Due to this existing feature of QKD, Bennett and Brassard's initial proposal was followed by a large number of alternate protocols of QKD [2, 4]. The applicability of early protocols of quantum cryptography [1-4] were limited to QKD. However, it was soon realized that quantum states can be employed for other cryptographic tasks, too. For example, quantum states can be used for quantum secret sharing (QSS) of classical secrets [5], deterministic secure quantum communication (DSQC) [6, 13], quantum secure direct communication (QSDC) [14, 17], quantum dialogue [18, 19], quantum key agreement (Ref. 20 and references therein), etc. Reviews on these topics, present challenges and future prospects of secure quantum communication can be found in Refs [21, 24].

The unconditional security of the existing protocols are usually claimed to be obtained using different approaches and different quantum resources like, single particle states [1, 3, 15, 17, 25], entangled state [2], teleportation [8], entanglement swapping [9], rearrangement of order of particles [11, 26], etc. Although these protocols differ with each other with respect to the procedure followed and the quantum resources used, the security of all these protocols of secure quantum communication essentially arises from the use of conjugate coding (i.e., from the quantum non-commutativity or equivalently from the use of two or more mutually unbiased bases (MUBs)) as in all these protocols the existence of an eavesdropper is traced by measuring verification qubits in 2 or more MUBs. Thus all these protocols may be viewed as conjugate-coding-based protocols of quantum communication; alternatively these protocols may be referred to as BB84-type protocols of quantum communication. The existence of such a large number of conjugate-coding-based protocols of quantum communication leads to a fundamental question: Is conjugate coding essential for unconditionally secure quantum communication?

The answer is "no". Specifically, it is possible to design protocols of secure quantum communication using orthogonal states alone. Thus we can design protocols of secure quantum communication using orthogonal states for encoding of information, decoding of information and eavesdropping check i.e., using a single basis for implementation of the entire protocol without involving any use of two or more MUBs or conjugate coding. First such orthogonal-state-based protocol was reported in 1995 by Goldenberg and Vaidman [4] and subsequently a few other orthogonal-state-based protocols of QKD were reported [27, 28, 29]. However, till recent past activities on orthogonal-state based protocols of quantum communication were limited to QKD and theoretical studies alone. Only recently a set of exciting experiments on orthogonal-state-based protocols of quantum communication have been reported [30, 33]. Further, new orthogonal-state-based protocols are proposed for quantum cryptographic tasks be- yond QKD [20, 34, 44]. These orthogonal-state-based proposals can be broadly classified in two classes: i. GV-type protocols which are analogous to the original GV-protocol and in which transmission of qubits that carry secret information through the quantum channel is allowed, but the information is protected from the eavesdropping by geographically separating an orthogonal state into two or more quantum pieces that are not simultaneously accessible to Eve and ii. $N0_9$-type protocols or counterfactual protocol that use interaction free measurement and circumvents the transmission of information carrying qubits through the quantum channel. GV-type protocols are mostly investigated by the present authors and their collaborators [20, 23, 34, 35, 36]. Specifically, we have shown that it is feasible to construct orthogonal-state-based protocols of QKA [20], QSDC and DSQC [34, 35, 36]. Practically, we have established that all the secure quantum communication tasks that can be performed using two or more MUBs can also be achieved by using single basis. Similarly, much progress has recently been made in designing of counterfactual (i.e., $N0_9$-type) protocols. For example, in 2013, Salih *et al.* have claimed to design a counterfactual protocol of direct quantum communication [37]. The claim was subsequently criticized by Vaidman [45] and the criticism lead to a very interesting debate on the issue [46]. Further, recently Salih has also proposed counter- factual protocols for transportation of an unknown qubit[41] and tripartite quantum cryptography [44], Guo *et al*. have proposed protocol of counterfactual entanglement distribution [42], Guo *et al*. proposed protocol of counterfactual information transfer [39], Sun and Wen have proposed a modified $N0_9$ protocol [38] which is more efficient than the actual $N0_9$ protocol and some of the present authors proposed protocols of counterfactual certificate authentication [40] and semi-counterfactual QKD [47]. These exciting developments of recent past motivated us to briefly review these recent achievements with specific attention to works of our group. Here we will briefly review a set of existing orthogonal-state-based protocols and describe a trick that helps us to transform BB_{84}-type protocols into Goldenberg- Vaidman (GV) type[4] protocols, which uses only orthogonal states for encoding, decoding and error checking, as was done in the original GV protocol of QKD. Subsequently, we will describe two orthogonal-state-based protocols of quantum communication introduced by us and briefly describe how they can be extended. These two orthogonal-state-based protocols are fundamentally different from conjugate- coding-based (BB84-type) protocols as their security does not depend on non-commutativity. Consequently, they are very important from the foundational perspective.

The trick that can transform BB_{84}-type protocols into GV-type protocol requires the rearrangement of orders of particles or *permutation of particles* (PoP). As PoP plays a very crucial role in our protocol, it would be apt to note that this technique was first introduced by Deng and Long in 2003, while they proposed a protocol of QKD based on this technique [48]. Subsequently, a DSQC protocol based on the rearrangement of orders of particles was proposed by Zhu *et al.* [11] in 2006. However, it was shown to be insecure under a Trojan-horse attack by Li *et al.* [7]. In Ref. [7], Li *et al*. had also provided an improved version of Zhu *et al*. protocol that is free from the above mentioned Trojan-horse attack. Thus we may consider Li *et al*. protocol as the first unconditionally secure protocol of DSQC based on PoP. Recently, many PoP based protocols are proposed (See [23] and references therein). Specifically, many such PoP-based protocols of quantum communication have been proposed in recent past. For example, Banerjee and Pathak [49], Shukla, Banerjee and Pathak [50], Yuan *et al.* [13] and Tsai *et al.* [26] have recently proposed PoP-based protocols of direct secure quantum communication. In what follows, we will see that PoP provides us a useful tool for the generalization of the original GV protocol into corresponding multipartite version.

A chronological history of protocols of orthogonal-state-based secure quantum communication and their experimental verification

1995: All the protocols of quantum cryptography proposed until 1995 were based on non-orthogonal states and security of those protocols arose directly or indirectly through non-commutativity, but in 1995, Goldenberg and Vaidman[4] proposed a completely orthogonal-state-based protocol of QKD, where the security arises due to duality (for single particle). This was the birth of orthogonal-state-based protocol of quantum cryptography. Interestingly, the fact that GV protocol is fundamentally different from the BB84-type protocol was questioned by Peres [51]. However, Goldenberg and Vaidman successfully defended their work[52] and established the fact that this orthogonal-state-based protocol is fundamentally different from the conventional BB84-type protocol. In the next section we have briefly de- scribed this protocol and have shown that the protocol uses a slightly modified Mach-Zehnder interferometer (See Fig. 1a).

1997: Koashi and Imoto [29] generalized the GV protocol and proposed a protocol similar to GV protocol, but does not require random sending time.

1998: Mor [53] showed that it is not always possible to clone orthogonal states. Specifically, an orthogonal state cannot be cloned if the full state cannot be accessed at the same time. Using this idea, Mor provided a clear and innovative explanation of the origin of security of GV protocol.

1999: Four years after the introduction of first orthogonal-state-based QKD protocol (i.e., GV protocol), Guo and Shi [28] proposed the second orthogonal- state-based protocol of QKD using the concept of interaction-free measurement or quantum interrogation [54], an idea that was introduced earlier by Elitzur and Vaidman in context of a very interesting hypothetical situation in which some of the active bombs can be separated from the inactive ones without directly observing the active bombs (i.e., without sending any photon to the isolated active bombs which blasts when receives a photon, whereas inactive bombs does not show any response on receiving a pho- ton). Actually, the bombs are placed in the lower arm of a Mach-Zehnder interferometer and a single photon is sent through the input port (See Fig. 1b). With 50% probability the single photon travels through the upper arm of the interferometer. Even in these 50% cases, if we have an active bomb (thus a detector) in the lower arm, the interference is destroyed as we obtain the which path information, and consequently in half of these incidents (i.e., 25% of the total) the detector present at the output port of the interferometer that does not click in absence of any detector in the lower arm would click. As a consequence we will be able to detect 25% of the active bombs without blasting them. Thus, in brief, the presence of the obstacle (active bomb) disrupts the destructive interference that would otherwise occur and thereby reveal its presence. Guo and Shi modified the idea and in their protocol Alice (Bob) randomly inserts an absorber in upper (lower) arm of the interferometer (See Fig. 1c). Form the clicks of the upper detector which does not click in absence of the detector, Bob knows that one of the absorber was present in one of the arm. In these cases he discloses that his upper detector has been clicked. As Alice (Bob) knows whether she (he) has inserted the absorber, using the observation of Bob she (he) can conclude whether Bob (Alice) has inserted the absorber or not and subsequently use this to form a key using a pre-decided rule: presence of Alice's (Bob's) absorber implies bit value 0 (1). Anyway, Guo and Shi's effort was the first step towards orthogonal-state-based counterfactual QKD and in recent years interaction-free measurement is frequently used as a tool for the designing of counterfactual quantum cryptographic protocols.

2009: A protocol of counterfactual QKD (orthogonal-state-based) was proposed by Noh in 2009 [27] using the Elitzur and Vaidman's idea of interaction-free measurement. This protocol of QKD is now known as N09 protocol or counterfactual protocol. This protocol led to many subsequent counterfactual protocols of secure quantum communication. The beauty of this protocol and other counterfactual protocols is that a secure key is distributed (or other cryptographic task is achieved) without transmitting a particle that carries secret information through the quantum channel. Interestingly, in GV, Koashi-Imoto and Guo-Shi protocols Mach-Zehnder interferometer was used, but in this protocol a Michelson interferometer is used (See Fig. 1d)[a].

2010: Sun and Wen [38] improved the original N09 protocol by providing analogous counterfactual protocol with higher frequency. In the same year, Avella *et al*. experimentally implemented GV protocol [30]. To the best of our knowledge this was the first ever experimental demonstration of orthogonal-state- based protocol of QKD.

2011: Experimental realization of N09 protocol was reported shortly after realization of GV protocol. Precisely, in 2011, Ren *et al*. reported experimental realization of N09 protocol [31].

2012: Soon after Ren *et al*.'s work two more groups reported experimental realization of N09 protocol. Specifically, Brida *et al*. [32] and Liu *et al*. [33], independently implemented this protocol of counterfactual quantum communication. In theoretical front, some of the present authors generalized the single particle GV protocol to multipartite case [35] and showed that GV- type protocol can be used for secure direct communication and established that while in GV the encoding states are perfectly indistinguishable, in the bi-partite case, they are partially distinguishable, leading to a qualitatively different kind of information-vs-disturbance trade-off and also options for Eve in the two cases. Further, generalizing the idea we had also established that GV-type protocol of DSQC, QSDC and QKD can be realized using arbitrary quantum states [34]. Essential ideas that lead to these multipartite GV-type protocols will be explained briefly in the next section.

2013: While the above counterfactual protocols are probabilistic, H. Salih *et al*. proposed a protocol for counterfactual direct quantum communication [37]. This work of Salih *et al*., led to an interesting debate and whether the protocol is counterfactual for only one of the two bit values has been controversial [45]. This protocol efficiently uses chained quantum Zeno effect and an arrangement of sequence of Mach-Zehnder interferometers, where each of the Mach-Zehnder interferometer essentially uses Elitzur and Vaidman setup for interaction free measurement. In the same year, Zhang *et al*. proposed a counterfactual protocol of private database queries [43] which also uses a similar setup of sequence of Mach-Zehnder interferometer. Further, the applicability of GV-type orthogonal-state-based protocols of secure quantum communication was extended by some of the present authors to quantum key agreement (QKA) where Alice and Bob contribute equally to the final shared key and none of them can control the final key [20].

2014: 2014 is the most active year in the history of orthogonal-state-based secure quantum communication. In this year many interesting results appeared. Here we list a few of them: (i) Guo *et al*. proposed a protocol of counter- factual quantum-information transfer [39], (ii) Guo *et al*. proposed a counterfactual protocol of entanglement distribution [42], (iii) Salih proposed a multiparty (tripartite) scheme of counterfactual quantum communication [44] and (iv) some of the present authors proposed a scheme for counterfactual quantum certificate authorization [40].

In the above chronological review we have seen that majority of the interesting developments in orthogonal-state-based secure quantum communication happened in last few years. The development is expected to continue and it is expected to play important role in practical realization of secure quantum communication and also in our understanding of quantum mechanics in general and origin of security in quantum mechanics and post-quantum theories in particular. Keeping these facts in mind, in the next section we briefly review role of no-cloning theorem in realization of orthogonal-state-based protocols and also briefly describe a few orthogonal-state- based GV-type protocols of secure quantum communication.

Orthogonal-state-based protocol of DSQC

The protocol in general works as follows:

Step1:

Aliceprepares|ψi⊗N.Shekeepsthefirstmqubitsofeach|ψiwith herselfand prepares a sequence PB with the remaining l qubits. Thus, PB is a sequence of N*l* qubits.

Step2: Alice communicates PB to Bob in a non-clonable manner. To communicate PB in nonclonable manner Alice prepares |ψ+i⊗N*l* 2 as decoy (checking) qubits and concatenates the qubits into PB to obtain a longer sequence P0 B, which has total 2Nl qubits. Subsequently, Alice applies a random permutation operator Π2Nl on P0 B to obtain a new sequence P00 B = Π2NlP0 B and sends that to Bob.

Step3: Alice discloses Π2Nl (which includes the coordinates of the Bell pairs) after receiving authentic acknowledgment of receipt of all the qubits from Bob.

Step4: Bob reorders the sequence and measures the transmitted Bell pairs (that are prepared as decoy qubits) in the Bell basis to determine if they are in the state |ψ+i. If the error detected by Bob is within at olerable limit, they continue to the next step. Otherwise, they discard the protocol and restart from Step1.

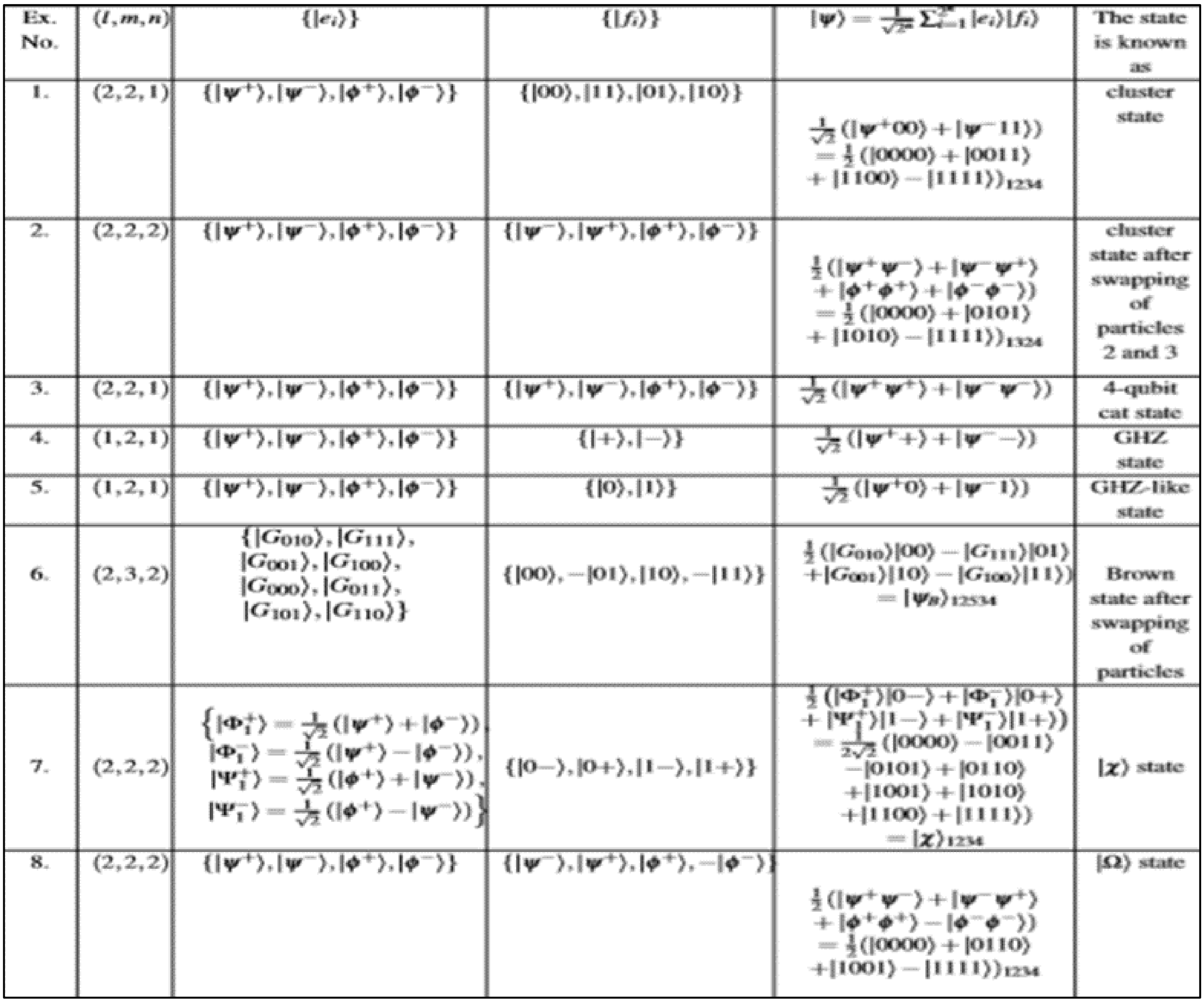
Step5: Alice encodes her n-bit message as follows: She encodes 0_10_2···0n, 0_10_2···1n,···, 1_11_2···1n as |e1i,|e2i,···,|eni, respectively and combines the encoded state with |ψi. Now, if Alice encodes a secret message j then the complete state of the system is as follows |ψ1i= 1 √2n 2n ∑ i=1|eji|eii|fii, whose first 2m qubits are with Alice and the last l qubits are with Bob.

Step6: Alice performs entanglement swapping operation as described above and announces her measurement outcomes.

Step7: Bob measure shis qubits in {|fii}basis. From his measurement outcomes and from the announcement of Alice, he can decode the information encoded by Alice.

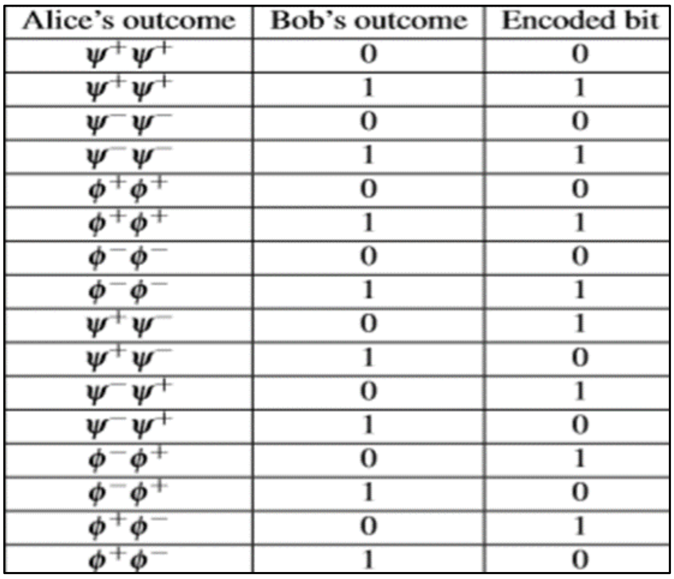
Role of no-cloning and randomness in secure communication and how to transform BB84-type protocols to GV-type protocols**.** It is well known that unknown quantum states cannot be cloned and several proofs of no-cloning theorem are provided using unitary evolution [53], no-signaling [55], linearity [56]. 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 measurement. 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 nonorthogonal 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.

Table 1: Interesting quantum states of the form (6.1) Here,|Gijki = |0i|ji|ki + (−1) I | 1 i|j⊕1i|k⊕1i, i, j,k∈{0,1}is a GHZ state.



Ex. No.	(l,m,n)	$\{\|e_i\rangle\}$	$\{\|f_i\rangle\}$	$\|\psi\rangle = \frac{1}{\sqrt{2^n}}\sum_{i=1}^{2^n}\|e_i\rangle\|f_i\rangle$	The state is known as
1.	(2,2,1)	$\{\|\psi^+\rangle,\|\psi^-\rangle,\|\phi^+\rangle,\|\phi^-\rangle\}$	$\{\|00\rangle,\|11\rangle,\|01\rangle,\|10\rangle\}$	$\frac{1}{\sqrt{2}}(\|\psi^+00\rangle+\|\psi^-11\rangle) = \frac{1}{2}(\|0000\rangle+\|0011\rangle + \|1100\rangle-\|1111\rangle)_{1234}$	cluster state
2.	(2,2,2)	$\{\|\psi^+\rangle,\|\psi^-\rangle,\|\phi^+\rangle,\|\phi^-\rangle\}$	$\{\|\psi^-\rangle,\|\psi^+\rangle,\|\phi^+\rangle,\|\phi^-\rangle\}$	$\frac{1}{2}(\|\psi^+\psi^-\rangle+\|\psi^-\psi^+\rangle + \|\phi^+\phi^+\rangle+\|\phi^-\phi^-\rangle) = \frac{1}{2}(\|0000\rangle+\|0101\rangle + \|1010\rangle-\|1111\rangle)_{1324}$	cluster state after swapping of particles 2 and 3
3.	(2,2,1)	$\{\|\psi^+\rangle,\|\psi^-\rangle,\|\phi^+\rangle,\|\phi^-\rangle\}$	$\{\|\psi^+\rangle,\|\psi^-\rangle,\|\phi^+\rangle,\|\phi^-\rangle\}$	$\frac{1}{\sqrt{2}}(\|\psi^+\psi^+\rangle+\|\psi^-\psi^-\rangle)$	4-qubit cat state
4.	(1,2,1)	$\{\|\psi^+\rangle,\|\psi^-\rangle,\|\phi^+\rangle,\|\phi^-\rangle\}$	$\{\|+\rangle,\|-\rangle\}$	$\frac{1}{\sqrt{2}}(\|\psi^+ +\rangle+\|\psi^- -\rangle)$	GHZ state
5.	(1,2,1)	$\{\|\psi^+\rangle,\|\psi^-\rangle,\|\phi^+\rangle,\|\phi^-\rangle\}$	$\{\|0\rangle,\|1\rangle\}$	$\frac{1}{\sqrt{2}}(\|\psi^+0\rangle+\|\psi^-1\rangle)$	GHZ-like state
6.	(2,3,2)	$\{\|G_{010}\rangle,\|G_{111}\rangle, \|G_{001}\rangle,\|G_{100}\rangle, \|G_{000}\rangle,\|G_{011}\rangle, \|G_{101}\rangle,\|G_{110}\rangle\}$	$\{\|00\rangle,-\|01\rangle,\|10\rangle,-\|11\rangle\}$	$\frac{1}{2}(\|G_{010}\rangle\|00\rangle-\|G_{111}\rangle\|01\rangle + \|G_{001}\rangle\|10\rangle-\|G_{100}\rangle\|11\rangle) = \|\Psi_B\rangle_{12534}$	Brown state after swapping of particles
7.	(2,2,2)	$\{\|\Phi_1^+\rangle=\frac{1}{\sqrt{2}}(\|\psi^+\rangle+\|\phi^-\rangle), \|\Phi_1^-\rangle=\frac{1}{\sqrt{2}}(\|\psi^+\rangle-\|\phi^-\rangle), \|\Psi_1^+\rangle=\frac{1}{\sqrt{2}}(\|\phi^+\rangle+\|\psi^-\rangle), \|\Psi_1^-\rangle=\frac{1}{\sqrt{2}}(\|\phi^+\rangle-\|\psi^-\rangle)\}$	$\{\|0-\rangle,\|0+\rangle,\|1-\rangle,\|1+\rangle\}$	$\frac{1}{2}(\|\Phi_1^+\rangle\|0-\rangle+\|\Phi_1^-\rangle\|0+\rangle + \|\Psi_1^+\rangle\|1-\rangle+\|\Psi_1^-\rangle\|1+\rangle) = \frac{1}{2\sqrt{2}}(\|0000\rangle-\|0011\rangle -\|0101\rangle+\|0110\rangle +\|1001\rangle+\|1010\rangle +\|1100\rangle+\|1111\rangle) = \|\chi\rangle_{1234}$	$\|\chi\rangle$ state
8.	(2,2,2)	$\{\|\psi^+\rangle,\|\psi^-\rangle,\|\phi^+\rangle,\|\phi^-\rangle\}$	$\{\|\psi^-\rangle,\|\psi^+\rangle,\|\phi^+\rangle,-\|\phi^-\rangle\}$	$\frac{1}{2}(\|\psi^+\psi^-\rangle+\|\psi^-\psi^+\rangle + \|\phi^+\phi^+\rangle-\|\phi^-\phi^-\rangle) = \frac{1}{2}(\|0000\rangle+\|0110\rangle +\|1001\rangle-\|1111\rangle)_{1234}$	$\|\Omega\rangle$ state

Table 2: Relation between Alice’s outcomes, Bob’s outcome and the encoded information.



Alice’s outcome	Bob’s outcome	Encoded bit
$\psi^+\psi^+$	0	0
$\psi^+\psi^+$	1	1
$\psi^-\psi^-$	0	0
$\psi^-\psi^-$	1	1
$\phi^+\phi^+$	0	0
$\phi^+\phi^+$	1	1
$\phi^-\phi^-$	0	0
$\phi^-\phi^-$	1	1
$\psi^+\psi^-$	0	1
$\psi^+\psi^-$	1	0
$\psi^-\psi^+$	0	1
$\psi^-\psi^+$	1	0
$\phi^-\phi^+$	0	1
$\phi^-\phi^+$	1	0
$\phi^+\phi^-$	0	1
$\phi^+\phi^-$	1	0

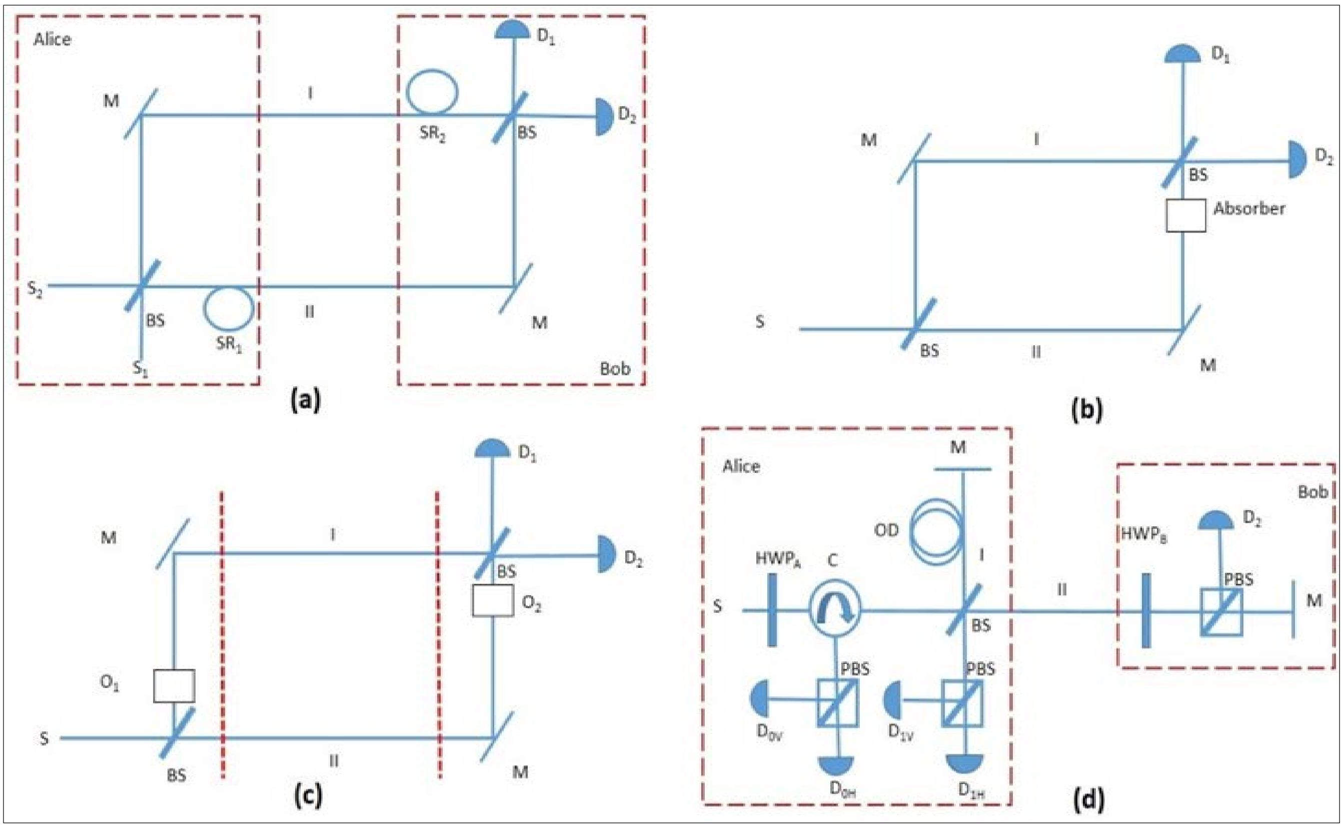


Fig 1: (a) A schematic diagram of a modified Mach-Zehnder interferometer that can be used to implement GV protocol [4] if the symmetric beam spliters used as 50:50, otherwise (i.e., if the symmetric beam splitters are not 50:50) the same device implements Koashi-Imoto protocol [29]. Here SR$_i$ denotes a delay. (b) A schematic diagram of a Mach-Zehnder interferometer that can be used to implement Elitzur and Vaidman's idea of interaction-free measurement or quantum interrogation [54]. Here the absorber is an active bomb that blasts when receives a photon. (c) A schematic diagram of Mach-Zehnder interferometer that can be used to realize orthogonal-state- based protocol of Guo-Shi [28] which uses interaction-free measurement. Here O$_1$ and O$_2$ are the obstacles that are randomly inserted by Alice and Bob, respectively. (d) A schematic diagram of the experimental setup used in [24, 32] to implement N0$_9$ protocol [27] of counterfactual QKD. In all the diagrams BS, M, C, PBS, HWP, D and OD represent beam splitter, mirror, circulator, polarizing beam splitter, half wave plate, detector and optical delay, respectively.

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|a\rangle - |b\rangle)$$

where $|a\rangle$ and $|b\rangle$ are two localized wave packets. Further, $|\psi_0\rangle$ and $|\psi_1\rangle$ represent bit values 0 and 1, respectively. Alice sends wave packets $|a\rangle$ and $|b\rangle$ to Bob by using two different arms of a Mach-Zehnder interferometer as shown in the Fig. 1 a. Alice sends Bob either $|\psi_0\rangle$ or $|\psi_1\rangle$, but $|a\rangle$ is always sent first and $|b\rangle$ is delayed by time τ. Here traveling time (θ) of wave packets from Alice to Bob is shorter than τ. Thus $|b\rangle$ enters the communication channel only after $|a\rangle$ is received by Bob. Consequently, both the wave packets $|a\rangle$ and $|b\rangle$ (i.e., the entire superposition) are never found simultaneously in the transmission channel. This geographic separation between $|a\rangle$ and $|b\rangle$ restricts Eve from measuring the state communicated by Alice in $\{|\psi_0\rangle, |\psi_1\rangle\}$ basis. In fact, this geographic separation method compels Eve to measure the state communicated by Alice either in $\{|a\rangle, |b\rangle\}$ 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 $|a\rangle$ by τ and recreates the superposition state sent by Alice after he receive $|b\rangle$ (cf. Fig. 1 a). In order to restrict Eve to perform the similar operation (i.e., to delay $|a\rangle$ till the arrival of $|b\rangle$) Alice and Bob need to perform following tests:

1. Alice and Bob compare the receiving time t_r with the sending time t_s for each state to ensure that Eve cannot delay $|a\rangle$ and wait for $|b\rangle$ to reach her so that she can do a measurement in $\{|\psi_0\rangle, |\psi_1\rangle\}$. Specifically, Alice and Bob checks that $t_r = t_s + \theta + \tau$. This test ensures that Eve cannot delay a wave packet, but it does not stop her from replacing a wave packet by a fake wave packet. The following test detects such an attack.
2. Alice and Bob look for changes in the data by comparing a portion of the transmitted bits with the same portion of the received bits. It is important to note that sending time in GV protocol must be random. Otherwise, Eve can prepare a fake state in $|\psi_0\rangle$ and send the fake $|a\rangle$ to Bob at the known arrival time. Eve can keep the original $|a\rangle$ and the fake $|b\rangle$ wave packets with her till the arrival of original $|b\rangle$. When $|b\rangle$ arrives then she measures the original state. If the measurement yields $|\psi_0\rangle$ then she sends the fake wave packet $|b\rangle$ to Bob. Otherwise, she corrects the phase of the fake wave packet and sends $-|b\rangle$ to Bob. If we assume that the time required for Eve's measurement is negligible, then following this procedure Eve can obtain the key without being detected. Interestingly, this requirement of random sending time can be circumvented just by replacing the 50:50 beam spliters present in the GV setup (cf. Fig. 1 a) by identical

beam splitters having *R f*= *T*, where *R* and *T* are reflectivity and transmissivity, respectively. This small change in GV setup (1 a) turns it into Koashi-Imoto [29] protocol.

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].

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

In the present work we have briefly present the recent developments on orthogonal- state-based protocols of secure quantum communication. We have classified the recently proposed orthogonal-state-based protocols into two sub-classes: GV-type and Counterfactual. GV-type protocols are discussed with relatively more detail and it is explicitly shown that by using a GV-type subroutine where Bell states are used as decoy qubits we can convert any conjugate coding based protocol with orthogonal-state-based encoding and decoding into GV-type completely orthogonal- state-based protocol. Thus in principle, every task that can be done using conjugate coding can also be done using orthogonal states alone. As examples, we have explicitly shown here how PP and DLL protocols can be converted to corresponding GV-type protocols. Further, since earlier proposals of orthogonal-state-based protocols are experimentally implemented recently, we may hope that ideas presented in this work and our more detailed related works [20, 34, 35, 36] will be implemented soon and this type of protocols would draw much more attention of cryptography community because of their fundamentally different nature.

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 nonorthogonal 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. A 1999;59:1829-1834.
6. Liu J, Liu Y-M, Cao H-J, Shi S-H, Zhang Z-J, *et al.* Revisiting quantum secure direct communication with W state. Chin. Phys. Lett 2006;23:2652-2655.
7. Li X-H, Deng F-G, Li C-Y, Liang Y-J, Zhou P, Zhou H-Y, *et al.* Determinis- tic 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. J. B 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 H-J, Song H-S. Quantum secure direct communication with W state. Chin. Phys. Lett 2006;23:290-292.
13. Yuan H, Song J, Zhou J, Zhang G, Wei X-f. 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, *et al.* 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 2014. In Press, 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 G-l, Deng F-g, Wang C, Li X-h, Wen K, Wang W-y, *et al.* 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, Brida G, *et al.* Review on

recent groundbreaking experiments on quantum communication with orthogonal states. Quantum Matter 2013;2:153-166.

25. Cai, Q-y, Li B-w. 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 T-G. Counterfactual quantum cryptography. Phys. Rev. Lett 2009;103:230501.
28. Guo G-C, Shi B-S. 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, *et al*. 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:l247-252.
33. Liu Y, Ju L, Liang X-L, Tang S-B, Tu G-L S, 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. Ar 2012;14:1209.4304.
36. Shukla C, Pathak A. Direct quantum communication without actual transmission of the message qubits. Quant. Info. Process. 2014. In Press, 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 Q-Y. Counterfactual quantum key distribution with high efficiency. Phys. Rev. A 2010;82:52318.
39. Guo Q, Cheng L-Y, Chen L, Wang H-F, Zhang S. Counterfactual quantum- information transfer. arXiv: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. Ar 2014;14:1404.2200.
42. Guo Q, Cheng L-Y, Chen L, Wang H-F, Zhang S. Counterfactual entangle- ment distribution without transmitting any particles. Optics express 2014;22:8970-8984.
43. Zhang J-L, Guo F-Z, Gao F, Liu B, Wen Q-Y. Private database queries based on counterfactual quantum key distribution. Phys. Rev. A 2013;88:022334.
44. Salih H. Tripartite counterfactual quantum cryptography. Ar 2014;14:1404.5540.
45. Vaidman L. Comment on “Protocol for direct counterfactual quantum communication”. Phys. Rev. Lett. 2014;112:208901.
46. Salih H, Li Z-H, 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 F-G, 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 F-G, Long GL, Liu X-S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys. Rev. A 2003;68:042317.