

Kak's three-stage protocol of secure quantum communication revisited: Hitherto unknown strengths and weaknesses of the protocol

Kishore Thapliyal* and Anirban Pathak†

Jaypee Institute of Information Technology, A-10, Sector 62. Noida, UP-201307

Abstract

Kak's three-stage protocol for quantum key distribution is revisited with special focus on its hitherto unknown strengths and weaknesses. It is shown that this protocol can be used for secure direct quantum communication. Further, the implementability of this protocol in the realistic situation is analyzed by considering various Markovian noise models. It is found that the Kak's protocol and its variants in their original form can be implemented only in a restricted class of noisy channels, where the protocols can be transformed to corresponding protocols based on logical qubits in decoherence free subspace. Specifically, it is observed that Kak's protocol can be implemented in the presence of collective rotation and collective dephasing noise, but cannot be implemented in its original form in the presence of other types of noise, like amplitude damping and phase damping noise. Further, the performance of the protocol in the noisy environment is quantified by computing average fidelity under various noise models, and subsequently a set of preferred states for secure communication in noisy environment have also been identified.

1 Introduction

In 1984, Bennett and Brassard proposed the first protocol for quantum key distribution (QKD) [1]. It succeeded to draw the attention of the cryptography community immediately as it could provide unconditional security, which is a desired but unachievable feat in the classical world. Because of these interesting features of QKD, the pioneering work of Bennett and Brassard was followed by a large number of protocols for QKD [2–5] and secure direct quantum communication [6–8] (where prior generation of a key is not required) (see [9] for a review). Among these schemes, only a few schemes have been realized experimentally ([10–15] and references therein). Further, almost all the experimentally realized schemes of secure quantum communication are protocols for QKD. Only, recently a few schemes of secure direct quantum communication have been realized experimentally [14–16]. This fact motivated us to look for simple schemes of secure direct quantum communication that can be realized experimentally. During our investigation, we realized that there exists an experimentally implemented scheme for secure quantum communication, which can be viewed as a scheme for secure direct quantum communication, but in the original proposal as well as in the follow-up works, it has been described as a scheme for QKD. Specifically, a three-stage protocol for QKD was proposed by Kak in 2006 [17] and experimentally implemented in 2013 by Mandal et al. [18]. This scheme has certain advantages over the conventional BB84 protocol and its variants. For example, it does not require single photon source and can be implemented using multi-photon pulses [18, 19]. Further, it can be modified to obtain three-stage quantum protocols for other quantum communication tasks. For example, three-stage schemes for quantum oblivious transform [20] has been proposed¹ using Kak's protocol. A quantum signature scheme [22] and a public key cryptography scheme [23] based on Kak's three-stage protocol were also proposed. This protocol is also found useful in quantum handshake [24], intensity-aware [25] and threshold quantum cryptography [26], and in a variant of it where each pulse transmits more than one bit [27]. Attempts have also been made to reduce the number of rounds of quantum communication in the three-stage protocol by proposing single-stage and braided single-stage protocols [28], where Bob is already aware of the unitary operation Alice has applied. However, this 1 stage variant of Kak's protocol fails to qualify as a scheme for QKD as it requires a prior knowledge of the unitary operation which equivalent to a pre-shared key.

All the above mentioned three-stage schemes are interesting in their own merit. However, the effects of noise on those schemes are not rigorously studied. Of course, in Refs. [29, 30] and Ref. [31], it is claimed that effect of collective rotation (CR) noise and uniform distribution of error caused due to different sources of noise on Kak's protocol have been studied, respectively, but these efforts were not mathematically rigorous. Keeping this fact in mind, in the present paper, the effects of different types of noise models (e.g., amplitude damping (AD), phase damping (PD), collective dephasing (CD), CR) on the

*Email: tkishore36@yahoo.com

†Email: anirban.pathak@gmail.com

¹Note that [20] contradicts the well established results of Ref. [21] and the protocol reported [20] is not loophole free.

Kak-type three-stage protocols of secure quantum communication have been studied. Here, we have considered that the noise parameters remain same for each round of travel through the quantum channel for all three-stages of the particular quantum communication process. In what follows, the effect of noise is illustrated by plotting the fidelity of the expected quantum state and the produced quantum state vs decoherence and other relevant parameters. In most of the cases, we have observed that the effect of PD noise is more than that of the AD noise for the same decoherence rate. Very interestingly, it has been observed that Kak's protocol only works under CR noise. It fails under AD, PD, and CD noise. This is so because the Kraus operators of the noise models (except that of CR) do not commute with unitary operators used by Alice and Bob in Kak's three-stage protocol. A similar conclusion holds for other protocols of secure quantum communications that are based on Kak's protocol. Finally, we have tried to propose some methods that may be adapted to circumvent this problem and implement Kak-type three-stage protocols in the presence of noise.

The rest of the paper is organized as follows. In Sec. 2, we briefly discuss the Kak's three-stage protocol and its origin of security and uniqueness in Section 3. Thereafter, the effect of noise on three-stage protocol is studied in the next two sections before concluding in Section 6.

2 Kak's three-stage protocol

To begin with, we briefly describe Kak's original three-stage protocol for QKD [17] which may be summarized in the following steps:

1. Alice prepares a single qubit quantum state $|\psi\rangle \in \{(\alpha|0\rangle + \beta|1\rangle), (\beta|0\rangle - \alpha|1\rangle)\}$. The basis and the corresponding bit values for both orthogonal states has been priorly decided, i.e., for sending a 0 (1) she prepares $\alpha|0\rangle + \beta|1\rangle$ ($\beta|0\rangle - \alpha|1\rangle$).
2. Alice applies a unitary operator $U_A \equiv R(\theta)$ to transform the state $|\psi\rangle$ to $|\psi'\rangle = R(\theta)|\psi\rangle$ and sends the transformed qubit $|\psi'\rangle$ to Bob. Here, the unitary operator used is a rotation operator $R(\theta) = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}$.
3. Bob independently applies a unitary transformation $U_B \equiv R(\phi)$ to transform $|\psi'\rangle$ into $|\psi''\rangle = R(\phi)|\psi'\rangle = R(\phi)R(\theta)|\psi\rangle = R(\theta)R(\phi)|\psi\rangle$ (in the last step we have used the fact that two arbitrary rotation operators commute) and sends it back to Alice.
4. This time Alice applies $U_A^\dagger = U_A^{-1}$ to transform $|\psi''\rangle$ to $|\psi'''\rangle = R(\phi)|\psi\rangle$ and sends the qubit again to Bob.
5. Bob applies $U_B^\dagger = U_B^{-1}$ to obtain $|\psi\rangle$ the state (bit value) Alice wanted to share.

Although Kak introduced the above protocol as a protocol for QKD, it is easy to recognize that Alice is not bound to send a random bit value using this scheme. She can always send a sequence of meaningful bits using this scheme and thus Kak's protocol should be viewed as a protocol of quantum secure direct communication, where a message can be transmitted directly without constructing a prior key. Once we recognize this protocol as a scheme of quantum secure direct communication we can naturally extend it to construct several other schemes of secure quantum communication that are variants of direct communication (for a detail discussion see [32] and references therein). There exist several schemes for secure direct quantum communication [6, 8, 14, 33, 34]. In fact, it is easy to show that famous BB84 scheme can be transformed to a scheme for secure direct quantum communication if one allows Bob to use quantum memory. To be precise, if Bob stores the string of single photons corresponding to message and checking qubits prepared randomly in $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ in a quantum memory until Alice discloses the positions and basis of the checking qubits. Using the same basis Bob performs a measurement of these verification qubits and announces the measurement outcomes, which help Alice in deciding whether to proceed with announcing the basis used to prepare the message qubits when error rate is below the threshold limit. Thus, Alice and Bob can perform a direct communication with no need of key generation. It may be noted that most of the well known protocols for direct secure quantum communication schemes use quantum memory. For example, we may briefly describe ping-pong protocol [6] for direct secure quantum communication as a scheme where Bob prepares a Bell state and sends a qubit to Alice to encode her message keeping another qubit in a quantum memory before measuring both the qubits in Bell basis to extract the secret². Similarly, LM05 protocol [8], Shukla et al.'s protocol [33], recent experimental implementation by Zhang et al. [15] for direct secure quantum communication do use quantum memory. This is the point where the actual strength of Kak's protocol lies. It does not require quantum memory. This is important as quantum memory is a very costly resource

²An alternative definition exists in the literature [34] according to which Kak's scheme should be viewed as a scheme for deterministic QKD since it does not involve block transmission. However, a deterministic QKD scheme can be adapted to perform direct secure quantum communication if the sender encrypts the message with a randomly chosen private key before sending it to the receiver using deterministic QKD and revealing the key only when she ensures the secure transmission of ciphertext.

and so far we do not have any good solution for a reliable quantum register that can store qubits for a reasonable amount of time. To the best of our knowledge, there exists only one proposal for direct secure quantum communication without quantum memory [35]. In the Yang's scheme [35], LM05 protocol [8] of direct secure quantum communication was suitably modified to obtain a scheme for QSDC without quantum memory.

Further, several direct communication schemes have been modified to obtain solutions of various cryptographic tasks, such as controlled [36, 37], asymmetric [38] and multiparty [39] variants of direct communication schemes, quantum e-commerce [40], quantum voting [41], quantum sealed-bid auction [42], quantum private comparison [40, 43]. Therefore, the use of quantum memory plays an instrumental role in the implementation of some of these schemes as well and modified Kak's protocol can help us to circumvent the use of quantum memory in the experimental realization of the above mentioned cryptographic tasks.

3 Nature and origin of security

Schemes for secure quantum communication can be broadly divided into two types, orthogonal-state-based schemes and conjugate-coding-based scheme. Orthogonal state based schemes, such as Goldenberg-Vaidman protocol [5], use the same basis for encoding, decoding and eavesdropping checking. Whereas in the conjugate-coding-based schemes, like BB84 protocol [1], the security comes from non-commutativity and no-cloning theorems. The origin of unconditional security in the quantum domain can also be understood from the splitting of information. Precisely, the sender splits useful information in multiple quantum and classical pieces and ensures all of them remain unavailable to unintended intruders until the secure communication is accomplished. In case of Kak's protocol, the sender prepares a quantum piece (qubit) and withholds a classical information (unitary U_A) until the receiver also composes a classical piece (another unitary U_B) to perform the cryptographic task. As U_A and U_B are not directly used for the encoding, decoding or eavesdropping checking, and as these operations can be done using orthogonal states, this protocol can be implemented as an orthogonal-state-based protocol.

4 Effect of noise

The beauty of the Kak's protocol lies in the fact that U_A and U_B commute, and the original security proof is restricted to the ideal situation, where there is no noise present in the channel between Alice and Bob. However, in any practical implementation of the scheme, it would be impossible to completely circumvent noise. Keeping this in mind, in what follows, we wish to investigate the effect of various types of noise on Kak's protocol and its variants. The effect of noise on Kak's protocol can be studied using Kraus operators for various noise models.

Mathematically, evolution of a single qubit quantum state ρ in the noisy environment can be described using the Kraus operator formalism as [44–47]

$$\rho_k = \sum_i E_i^k \rho (E_i^k)^\dagger, \quad (1)$$

where E_i^k s are the Kraus operator for a specific noise model (displayed as superscript k) under consideration. Before we proceed further, we need to state the Kraus operators for various noise models. In the following subsection, we have listed the Kraus operators for various noise models that are investigated in this work.

4.1 Kraus operators for various noise models

1. AD noise: The spontaneous emission from a high energy state is modeled by the following set of Kraus operators [45–47]:

$$E_0^A = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\eta_A} \end{bmatrix}, \quad E_1^A = \begin{bmatrix} 0 & \sqrt{\eta_A} \\ 0 & 0 \end{bmatrix}, \quad (2)$$

where the decoherence rate η_A such that $0 \leq \eta_A \leq 1$ depends on the interaction between the system and the environment.

2. PD noise: This dephasing noise model is described by the Kraus operators [45, 46]:

$$E_0^P = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\eta_P} \end{bmatrix}, \quad E_1^P = \begin{bmatrix} 0 & 0 \\ 0 & \sqrt{\eta_P} \end{bmatrix}, \quad (3)$$

with the decoherence rate η_P ($0 \leq \eta_P \leq 1$) involves interaction without energy loss.

3. CD noise model: A coherent effect of environment on all the qubits traveling through a channel is studied as collective noise models [48, 49]. This kind of noise model is described by unitary operations, unlike Kraus operators of AD or PD channels. Specifically, collective noise is studied as CD and CR noise models. The effect of CD noise is characterized ([50] and references therein) by $E^D |0\rangle = |0\rangle$ and $E^D |1\rangle = \exp(i\Phi) |1\rangle$. One can easily obtain that $E^D = \begin{bmatrix} 1 & 0 \\ 0 & \exp(i\Phi) \end{bmatrix}$ is a phase gate only. Here, Φ is the noise parameter that remains the same for all the travel qubits at any instant of time. However, it can take different values while independent use of a channel at different times.
4. CR noise model: Similar to the CD noise model, this type of noise ([50] and references therein) is defined to affect as $E^R |0\rangle = \cos \Theta |0\rangle + \sin \Theta |1\rangle$ and $E^R |1\rangle = -\sin \Theta |0\rangle + \cos \Theta |1\rangle$, which can be easily defined due to the application of a unitary rotation $E^R = \begin{bmatrix} \cos \Theta & -\sin \Theta \\ \sin \Theta & \cos \Theta \end{bmatrix}$. Quite similar to the CD noise, here Θ is the noise parameter that may change with time and affects all the travel qubits in the same way.

4.2 Commutativity of the rotation operator used in Kak's protocol and the Kraus operators

Using the open quantum system approach mentioned in Eq. (1), we can summarize the evolution of a single qubit quantum state under the Kak's three-stage protocol in the noisy environment as

$$\rho_k = \sum_{i,j,l} \left((R(\phi))^\dagger E_i^k R((\theta))^\dagger E_j^k R(\phi) E_l^k R(\theta) \right) \rho \left((R(\phi))^\dagger E_i^k R((\theta))^\dagger E_j^k R(\phi) E_l^k R(\theta) \right)^\dagger. \quad (4)$$

Here, $k \in \{\text{AD}, \text{PD}\}$ corresponds to the type of noise model under consideration, and $\rho = |\psi\rangle\langle\psi|$ is the single qubit initial state prepared by Alice. The single qubit state is rotated by an angle θ (ϕ) in the Bloch sphere by Alice's (Bob's) operation in Step 1 (3). Additionally, different i , j , and l in the subscript represent independent effects of noise during Alice-to-Bob, Bob-to-Alice, and Alice-to-Bob travels of single qubit, respectively.

At a first glance, one can easily conclude that the beauty of the Kak's protocol (i.e., commutativity of rotation operators by Alice and Bob) could only be preserved if the rotation operators commute with the Kraus operators for various noise models.

To begin with, let us consider a simple situation in which Kak's protocol is implemented using an AD channel, and in the first two stages of the protocol (i.e., from Alice-to-Bob and Bob-to-Alice journey), noise affects the qubit via E_0^A , in this situation, instead of $|\psi''\rangle = R(\phi)R(\theta)|\psi\rangle = R(\theta)R(\phi)|\psi\rangle$, Alice would receive $|\psi''\rangle = E_0^A R(\phi) E_0^A R(\theta) |\psi\rangle$. Note that Alice would be able to remove her encryption $U_A = R(\theta)$ by applying $U_A^\dagger = U_A^{-1}$ if and only if $R(\theta)$ commutes with E_0^A (i.e., iff $[E_0^A, R(\theta)] = 0$). However, we can easily compute that

$$[E_0^A, R(\theta)] = E_0^A R(\theta) - R(\theta) E_0^A = (1 - \sqrt{1-\eta}) \sin \theta \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \quad (5)$$

For this commutator to vanish, i.e., $[E_0^A, R(\theta)] = 0$, we require either $\eta = 0$ or $\theta = 0$. The former case corresponds to noiseless situation while the latter case corresponds to no rotation applied by Alice in the Bloch sphere in Kak's protocol, i.e., $R(\theta)$ becomes identity and eavesdropper's ignorance becomes zero. These are trivial cases, and the analysis shows that in the above situation Kak's protocol does not work in its original form. The observation can be further strengthened by noting that

$$[E_1^A, R(\theta)] = E_1^A R(\theta) - R(\theta) E_1^A = -\sqrt{\eta} \sin \theta \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad (6)$$

where the results obtained from Eq. (5) remains valid. Hence, it can be summarized that Kak's three-stage protocol fails under AD noise as the rotation operator of Alice operated in the second step of Kak's protocol will not be nullified by the inverse operator of the same rotation operator applied in the fourth step of the protocol.

Similar studies can be performed for other kind of noises, like PD noise. In fact, it is observed that both E_0^P and E_1^P result in the same conclusion as we obtained for the AD noise channel. Similar investigations over the CD and CR noise is quite easy to perform as the effect of noise is characterized using unitary operators in both these cases. Specifically, the CD noise leads to the same result that the rotation operator commutes only in the ideal condition, and in the noisy scenario, for $\Phi = 2n\pi$ with an integer n (as the unitary for CD noise reduces to an identity)³. It would also be worth noting here that CR noise does not affect the protocol as two arbitrary rotation operators always commute with each other. Hence, Kak's protocol would work under CR noise. One such attempt to analyze the Kak's three-stage protocol over CR noise in multi-photon case [29], and it is shown to possess higher error rate tolerance than the single photon case.

³Here, it may be noted that although Kak's protocol in its original form would not work under the CD noise, there are techniques to use logical qubits and thus to exploit the advantage of a decoherence free subspace to realize Kak's protocol in presence of CD noise [50, 51], but no such decoherence free subspace is known for the AD and PD noise.

It is expected that a similar study on the squeezed generalized amplitude damping channel would also lead to the same conclusion as generalized amplitude damping and AD noise channels are only the limiting cases of squeezed generalized amplitude damping channel.

5 Formal investigation on the effect of noise on the Kak's three-stage protocol

The effect of noise can be formally investigated by comparing the quantum state ρ_k produced in the noisy environment with the state $\rho = |\psi\rangle\langle\psi|$ which was expected at the Bob's port after three-stages of quantum communication in the absence of noise. The comparison can be performed using fidelity

$$F = \langle\psi|\rho_k|\psi\rangle, \quad (7)$$

which is the square of the conventional definition of fidelity. In addition, for the convenience of discussion, an arbitrary single qubit quantum state which is to be transmitted by Alice in Step 1 (before application of U_A) to send a bit value "0" can be assumed as $|\psi_1\rangle = \cos\xi|0\rangle + \sin\xi|1\rangle$; whereas Alice has to send an orthogonal state $|\psi_2\rangle = \sin\xi|0\rangle - \cos\xi|1\rangle$ to send a bit value of "1". Therefore, the initial density matrix will be $\rho = |\psi\rangle\langle\psi|$ with $|\psi\rangle \in \{|\psi_1\rangle, |\psi_2\rangle\}$.

In the presence of AD noise (i.e., when the qubit is subjected to AD noise), using Eqs. (2) and (7) a closed form analytic expression of fidelity is computed as

$$F_{AD} = \frac{1}{16} [-\eta(\eta^2 - 3(\sqrt{1-\eta} + 2)\eta + 7\sqrt{1-\eta} + 9) + 4(\sqrt{1-\eta} + 3) - (\eta - 1)(\eta(\eta + 3\sqrt{1-\eta} - 5) - 4\sqrt{1-\eta} + 4)\cos(4\xi)], \quad (8)$$

which is averaged over two possible choices of the initial state by Alice, depending up on the bit value of the message she wishes to send.

Along the same line, a similar study over purely dephasing kind of noise (i.e., PD noise) using Eqs. (3) and (7) led to the following compact expression

$$F_{PD} = \frac{1}{8} \left((-\sqrt{1-\eta}\eta + 3\eta + 4\sqrt{1-\eta} - 4) \sin^2(2\xi) - 3\eta + 8 \right). \quad (9)$$

The fidelity of the quantum state received by Bob over collective noisy channels with that of Alice's initially prepared state is computed as

$$F_{CD} = \frac{1}{32} (6\cos^2(2\theta)\cos(2\Phi) + \sin^2(2\theta)(15\cos(\Phi) + \cos(3\Phi)) + 5\cos(4\theta) + 21) \quad (10)$$

and

$$F_{CR} = \cos^2(3\Theta), \quad (11)$$

for CD and CR channels, respectively.

Note that the choice of state parameter ξ by Alice is a public knowledge (i.e., decided at the beginning of the protocol by Alice and Bob), which is a continuous variable in the domain $\{0, 2\pi\}$. Therefore, before reaching to any conclusion from Eqs. (8) and (9), it would also be imperative to compute the average fidelity by taking into account all possible choices of ξ using

$$F_k^{\text{av}} = \frac{1}{2\pi} \int_0^{2\pi} F_k d\theta. \quad (12)$$

The average fidelity expressions calculated over AD and PD noise channels are

$$F_{AD}^{\text{av}} = \frac{1}{16} \left(4(\sqrt{1-\eta} + 3) - \eta(\eta^2 - 3(\sqrt{1-\eta} + 2)\eta + 7\sqrt{1-\eta} + 9) \right), \quad (13)$$

and

$$F_{PD}^{\text{av}} = \frac{1}{16} (\sqrt{1-\eta} + 3)(4 - \eta), \quad (14)$$

respectively.

Similarly, average fidelity in the case of qubit subjected to CR noise is

$$F_{CD}^{\text{av}} = \frac{1}{64} (15\cos(\phi) + 6\cos(2\phi) + \cos(3\phi) + 42). \quad (15)$$

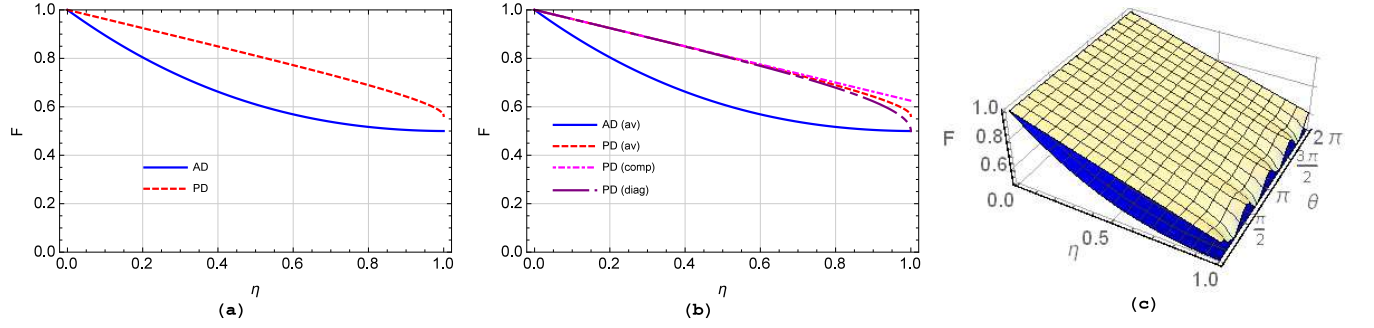


Figure 1: (Color online) Variation of average fidelity as a function of noise parameters of AD and PD noise is shown in (a). In (b), fidelity for the choice of initial states in the computational $\{|0\rangle, |1\rangle\}$ and diagonal $\{|+\rangle, |-\rangle\}$ basis is also shown. In (c), dependence on the choice of initial state is illustrated through a three-dimensional plot where light yellow (dark blue) colored surfaces correspond to fidelity calculated over AD and PD noise models, respectively.

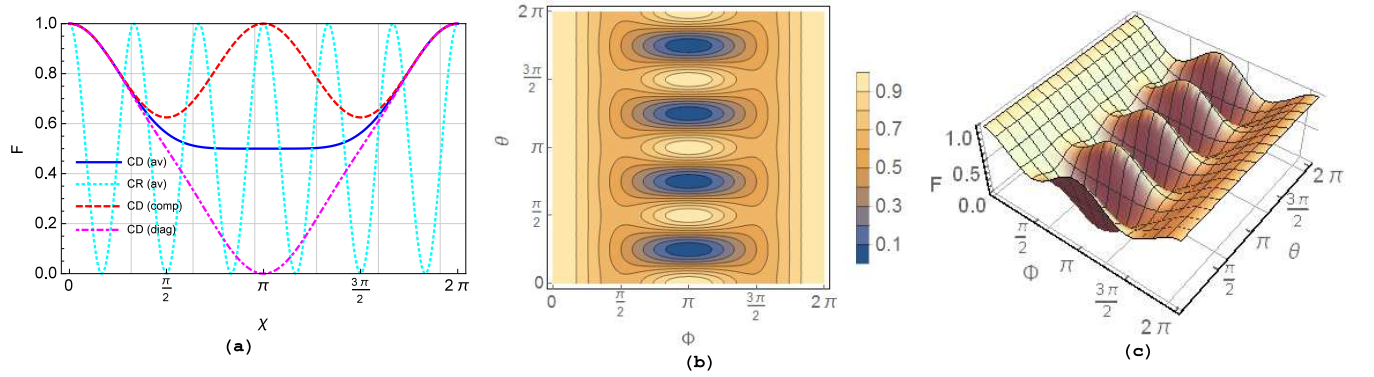


Figure 2: (Color online) Variation of average fidelity as a function of noise parameters, when the qubit is subjected to collective noises. In (a), fidelity for specific choice of initial states in the computational $\{|0\rangle, |1\rangle\}$ and diagonal $\{|+\rangle, |-\rangle\}$ basis is shown along with the average fidelity. Here, the noise parameter $\chi = \Theta (\Phi)$ for CR (CD) noise. In (b) and (c), dependence on the choice of initial state evolving under CD noise is illustrated through a contour and a three-dimensional plots.

Also, from Eq. (11) one can conclude that $F_{CR}^{\text{av}} = F_{CR}$ as the obtained expression for F_{CR} is independent of the choice of the initial state.

Finally, we have established dependence of fidelity (in Eqs. (8) and (9)) on the state parameter, and also shown its variation along with average fidelity (in Eqs. (13) and (14)) in Figure 1. The obtained fidelity and average fidelity over a PD noise channel is always better than that for AD channel (cf. Figure 1 (a) and (c)). Further, in Figure 1 (b), we compare the obtained average fidelity with that of the fidelity for the initial states chosen from the computational $\{|0\rangle, |1\rangle\}$ and diagonal $\{|+\rangle, |-\rangle\}$ basis. It establishes that the computational basis is preferable for the channels with high decoherence rate, while the diagonal basis is the worst choice. The same fact can also be verified from Figure 1 (c). Moreover, the choice of initial state becomes irrelevant in case of AD channels and low decoherence rate PD channels.

A similar study on CR noise shows that fidelity for CR noise is independent of state parameters and is a periodic function of the noise parameter Θ with period $\frac{\pi}{3}$ (cf. dotted (cyan) line in Fig. 2 (a)). Therefore, there are some specific values of the noise parameter for which the state reaches unaffected. This feature can be attributed to the fact that two arbitrary rotation operators commute with each other.

On the contrary, the choice of the initial state plays a very important role in the fidelity that can be obtained over the CD noise as shown in Fig. 2. Specifically, the fidelity over CD channels for the noise parameter $\Phi = \pi$ increases (decreases) to unity (zero) for the choice of computational (diagonal) basis as shown in Fig. 2 (a). Also the average value of the fidelity, as expected, tends to its lowest value 0.5. The dependence of fidelity on the state parameters is also established using a contour and a three-dimensional plots in Fig. 2 (b) and (c).

One can conclude from the study of analyzing the performance of Kak's protocol in various types of noise models that the commutation, which plays the most important role in the three-stage protocol, between the rotation and noise operators (discussed in the previous subsection) epitomizes the whole scenario.

6 Conclusion

We have shown that the three-stage QKD protocol proposed by Kak can work as a scheme for secure direct quantum communication. This provides opportunity to exploit the benefits of single qubit based Kak's protocol in the field of direct communication and their variants as solutions of socioeconomic problems of relevance. However, such a dedicated effort would require serious effort to analyze the feasibility of Kak's protocol under various noise models. The present study has established that Kak's protocol would face serious problems in presence of noise. It's further established that there are certain single qubit states which are preferred over other states for the implementation of Kak's protocol in presence of noise. This is in sharp contrast with the observations made on the basis of the original scheme. Specifically, in the original protocol, presence of noise was not considered and there was no preference about the states to be chosen to represent bit values 0 and 1. Interestingly, in the presence of noise such a choice is found to influence the fidelity and thus the performance of the scheme.

It has also been established that Kak-type protocols properly works only under CR noise. It fails under CD (unless decoherence free subspace is used), AD and PD noise models. Logically, a similar study on the effect of squeezed generalized amplitude damping (SGAD) channel or generalized amplitude damping channel is also expected to yield similar result (failure). In fact, the same result (failure) is expected over the non-Markovian noise channels [52]. The present work can be extended to include the effect of non-Markovian noise by following the prescription provided in Refs. [52]. However, we have restricted us from doing such an exercise as that would only reveal the same limitation of Kak's protocol.

The protocol can work under the effect of CD noise exploiting decoherence free subspaces for encoding using two-qubit entangled logical qubits instead of single qubits (as discussed in Refs. [50, 53] and references therein). However, due to this solution we loose the advantage of single qubit protocols, i.e., a secure protocol without using entanglement. In other words, the use of entangled states would increase the requirement of quantum resources. Further, it may be noted that we have already shown in the recent past that single-qubit-based quantum cryptographic schemes are advantageous when compared to corresponding entangled-state-based counterparts [54] in the presence of noise. Another possible solution, which would work under any kind of noise model up to moderate decoherence, is to use quantum error correction codes ([32] and references therein). In short, a serious investigation on the error correction scheme specifically designed for Kak's protocol and/or a search for suitable decoherence free subspaces may help Kak's protocol to circumvent the limitations pointed out this paper and thus help its implementation in the realistic situation.

Also in view of our recent results [55], that the performance of a quantum cryptographic scheme depends upon the complexity of the task in hand and thus rounds of quantum communication involved in accomplishing the task, the three stage protocol is expected to be more affected when compared to a single- or two-stage quantum cryptographic scheme due to multiple rounds of travel of the single qubit through the noisy channel. Thus, despite of its several advantages, Kak's protocol is not preferable in presence of noise.

Acknowledgment KT thanks CSIR, India for the support provided through Senior Research Fellowship. AP thanks Defense Research & Development Organization (DRDO), India for the support provided through the project number ERIP/ER/1403163 /M/01/ 1603.

References

- [1] Bennett, C. H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. in: International Conference on Computer System and Signal Processing, IEEE, 1984 pp. 175–179 (1984)
- [2] Ekert, A. K.: Quantum cryptography based on Bell's theorem. *Physical Review Letters* **67**, 661 (1991)
- [3] Bennett, C. H., Brassard, G., Mermin, N. D.: Quantum cryptography without Bell's theorem. *Physical Review Letters* **68**, 557 (1992)
- [4] Bennett, C. H.: Quantum cryptography using any two non orthogonal states. *Physical Review Letters* **68**, 3121 (1992)
- [5] Goldenberg, L., Vaidman, L.: Quantum cryptography based on orthogonal states. *Physical Review Letters* **75**, 1239 (1995)
- [6] Boström, K., Felbinger, T.: Deterministic secure direct communication using entanglement. *Physical Review Letters* **89**, 187902 (2002)
- [7] Degiovanni, I., Berchera, I. R., Castelletto, S., et al.: Quantum dense key distribution. *Physical Review A* **69**, 032310 (2004)
- [8] Lucamarini, M., Mancini, S.: Secure deterministic communication without entanglement. *Physical Review Letters* **94**, 140501 (2005)

- [9] Pathak, A., Srikanth, R., et al.: Quantum cryptography: key distribution and beyond. *Quanta* pp. 1–47 (2017)
- [10] Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., Smolin, J.: Experimental quantum cryptography. *Journal of cryptology* **5**, 3–28 (1992)
- [11] Zhao, Y., Qi, B., Ma, X., Lo, H.-K., Qian, L.: Experimental quantum key distribution with decoy states. *Physical Review Letters* **96**, 070502 (2006)
- [12] Schmitt-Manderbach, T., Weier, H., Fürst, M., et al.: Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Physical Review Letters* **98**, 010504 (2007)
- [13] Lo, H.-K., Curty, M., Tamaki, K.: Secure quantum key distribution. *Nature Photonics* **8**, 595 (2014)
- [14] Hu, J.-Y., Yu, B., Jing, M.-Y., et al.: Experimental quantum secure direct communication with single photons. *Light: Science & Applications* **5**, e16144 (2016)
- [15] Zhang, W., Ding, D.-S., Sheng, Y.-B., et al.: Quantum secure direct communication with quantum memory. *Physical Review Letters* **118**, 220501 (2017)
- [16] Cao, Y., Li, Y.-H., Cao, Z., et al.: Direct counterfactual communication via quantum Zeno effect. *Proceedings of the National Academy of Sciences* **114**, 4920–4924 (2017)
- [17] Kak, S.: A three-stage quantum cryptography protocol. *Foundations of Physics Letters* **19**, 293–296 (2006)
- [18] Mandal, S., Macdonald, G., El Rifai, M., et al.: Multi-photon implementation of three-stage quantum cryptography protocol. in: *Information Networking (ICOIN), 2013 International Conference on* pp. 6–11 IEEE (2013)
- [19] Chan, K. W. C., El Rifai, M., Verma, P., Kak, S., Chen, Y.: Security analysis of the multi-photon three-stage quantum key distribution. *International Journal on Cryptography and Information Security* **5**, 3/4 (2015)
- [20] Parakh, A.: A quantum oblivious transfer protocol. in: *SPIE Optical Engineering+Applications* pp. 883204–883204 International Society for Optics and Photonics (2013)
- [21] Lo, H.-K.: Insecurity of quantum secure computations. *Physical Review A* **56**, 1154 (1997)
- [22] Kang, M.-S., Hong, C.-H., Heo, J., Lim, J.-I., Yang, H.-J.: Quantum signature scheme using a single qubit rotation operator. *International Journal of Theoretical Physics* **54**, 614–629 (2015)
- [23] Nikolopoulos, G. M.: Applications of single-qubit rotations in quantum public-key cryptography. *Physical Review A* **77**, 032348 (2008)
- [24] El Rifai, M., Verma, P. K.: An ieee 802.11 quantum handshake using the three-stage protocol. in: *Computer Communication and Networks (ICCCN), 2014 23rd International Conference on* pp. 1–6 IEEE (2014)
- [25] Kak, S., Chen, Y., Verma, P.: iaqc: The intensity-aware quantum cryptography protocol. *arXiv preprint arXiv:1206.6778* (2012)
- [26] Kak, S.: Threshold quantum cryptography. *arXiv preprint arXiv:1310.6333* (2013)
- [27] El Rifai, M., Punekar, N., Verma, P. K.: Implementation of an m-ary three-stage quantum cryptography protocol. in: *Quantum Communications and Quantum Imaging XI* volume 8875 p. 88750S International Society for Optics and Photonics (2013)
- [28] Darunkar, B., Verma, P. K.: The braided single-stage protocol for quantum secure communication. in: *Quantum Information and Computation XII* volume 9123 p. 912308 International Society for Optics and Photonics (2014)
- [29] Wu, L., Chen, Y.: Three-stage quantum cryptography protocol under collective-rotation noise. *Entropy* **17**, 2919–2931 (2015)
- [30] Parakh, A., Van Brandwijk, J.: Correcting rotational errors in three stage qkd. in: *Telecommunications (ICT), 2016 23rd International Conference on* pp. 1–5 IEEE (2016)
- [31] Chitikela, S.: Noise analysis for two quantum cryptography protocols. *arXiv preprint arXiv:1207.7281* (2012)
- [32] Pathak, A.: *Elements of Quantum Computation and Quantum Communication*. Taylor & Francis (2013)

- [33] Shukla, C., Banerjee, A., Pathak, A.: Improved protocols of secure quantum communication using W states. *International Journal of Theoretical Physics* **52**, 1914–1924 (2013)
- [34] Long, G.-l., Deng, F.-g., Wang, C., et al.: Quantum secure direct communication and deterministic secure quantum communication. *Frontiers of Physics in China* **2**, 251–272 (2007)
- [35] Yang, Y.-y.: A quantum secure direct communication protocol without quantum memories. *International Journal of Theoretical Physics* **53**, 2216–2221 (2014)
- [36] Pathak, A.: Efficient protocols for unidirectional and bidirectional controlled deterministic secure quantum communication: different alternative approaches. *Quantum Information Processing* **14**, 2195–2210 (2015)
- [37] Thapliyal, K., Pathak, A.: Applications of quantum cryptographic switch: Various tasks related to controlled quantum communication can be performed using Bell states and permutation of particles. *Quantum Information Processing* **14**, 2599–2616 (2015)
- [38] Banerjee, A., Shukla, C., Thapliyal, K., Pathak, A., Panigrahi, P. K.: Asymmetric quantum dialogue in noisy environment. *Quantum Information Processing* **16**, 49 (2017) doi:10.1007/s11128-016-1508-4
- [39] Banerjee, A., Thapliyal, K., Shukla, C., Pathak, A.: Quantum conference. *arXiv preprint arXiv:1702.00389* (2017)
- [40] Shukla, C., Thapliyal, K., Pathak, A.: Semi-quantum communication: protocols for key agreement, controlled secure direct communication and dialogue. *Quantum Information Processing* **16**, 295 (2017)
- [41] Thapliyal, K., Sharma, R. D., Pathak, A.: Protocols for quantum binary voting. *International Journal of Quantum Information* **15**, 1750007 (2017)
- [42] Sharma, R. D., Thapliyal, K., Pathak, A.: Quantum sealed-bid auction using a modified scheme for multiparty circular quantum key agreement. *Quantum Information Processing* **16**, 169 (2017) doi:10.1007/s11128-017-1620-0
- [43] Thapliyal, K., Sharma, R. D., Pathak, A.: Orthogonal-state-based and semi-quantum protocols for quantum private comparison in noisy environment. *arXiv preprint arXiv:1608.00101* (2016)
- [44] Breuer, H.-P., Petruccione, F.: *The Theory of Open Quantum Systems*. Oxford University Press (2002)
- [45] Nielsen, M. A., Chuang, I. L.: *Quantum computation and quantum information*. Cambridge University Press (2010)
- [46] Preskill, J.: Lecture notes for physics 229: Quantum information and computation. California Institute of Technology **12**, 14 (1998)
- [47] Thapliyal, K., Banerjee, S., Pathak, A., Omkar, S., Ravishankar, V.: Quasiprobability distributions in open quantum systems: Spin-qubit systems. *Annals of Physics* **362**, 261–286 (2015)
- [48] Zanardi, P., Rasetti, M.: Noiseless quantum codes. *Physical Review Letters* **79**, 3306 (1997)
- [49] Bourennane, M., Eibl, M., Gaertner, S., et al.: Decoherence-free quantum information processing with four-photon entangled states. *Physical Review Letters* **92**, 107901 (2004)
- [50] Sharma, R. D., Thapliyal, K., Pathak, A., Pan, A. K., De, A.: Which verification qubits perform best for secure communication in noisy channel? *Quantum Information Processing* **15**, 1703–1718 (2016)
- [51] Li, X.-H., Deng, F.-G., Zhou, H.-Y.: Efficient quantum key distribution over a collective noise channel. *Physical Review A* **78**, 022321 (2008)
- [52] Thapliyal, K., Pathak, A., Banerjee, S.: Quantum cryptography over non-Markovian channels. *Quantum Information Processing* **16**, 115 (2017)
- [53] Boileau, J. C., Gottesman, D., Laflamme, R., Poulin, D., Spekkens, R. W.: Robust polarization-based quantum key distribution over a collective-noise channel. *Physical Review Letters* **92**, 017901 (2004)
- [54] Sharma, V., Thapliyal, K., Pathak, A., Banerjee, S.: A comparative study of protocols for secure quantum communication under noisy environment: Single-qubit-based protocols versus entangled-state-based protocols. *Quantum Information Processing* **15**, 4681–4710 (2016) doi:10.1007/s11128-016-1396-7
- [55] Thapliyal, K., Pathak, A., Banerjee, S.: Quantum cryptography over non-Markovian channels. *Quantum Information Processing* **16**, 115 (2017)