DESIGN AND ANALYSIS OF QUANTUM COMMUNICATION PROTOCOLS

Synopsis submitted in fulfillment for the requirements of the Degree of

Doctor of Philosophy

by

CHITRA SHUKLA

Department of Physics and Materials Science and Engineering

JAYPEE INSTITUTE OF INFORMATION TECHNOLOGY

A-10, SECTOR-62, NOIDA, INDIA

November, 2014

SYNOPSIS

1 Introduction

In modern society, communication plays a crucial role. Everyday knowingly or unknowingly, we use a large number of communication devices and protocols. For example, we use the internet, mobile phone, ATM cards, etc. Until now, we mostly use communication devices and protocols based on the laws of classical physics. Interestingly, in the last three decades a considerable progress has been observed in quantum communication. Specifically, several communication tasks that are impossible in the classical world, have been realized using quantum mechanical resources. For example, we may mention (i) unconditionally secure quantum key distribution (QKD) [1], (ii) dense coding [2] and (iii) quantum teleportation (QT) [3]. These schemes have no classical analogue. The basic protocols of quantum communication tasks were proposed between 1984 to 1993. For example, in 1984, Bennett and Brassard [1] proposed the first protocol of QKD which is now known as BB84 protocol, in which a sender (Alice) creates a random sequence of bits (i.e., a key) and then distributes it to a distant receiver (Bob) by quantum means. The idea of dense coding, which is also known as "Superdense coding" was first proposed by Bennett et al. [2] in 1992. In this process, a sender (Alice) can communicate two classical bits of information to the receiver (Bob) by sending only one qubit of information with the condition that Alice and Bob must share a prior entanglement. Subsequently, in 1993, Bennett et al. introduced the QT scheme [3] in which a sender (Alice) can communicate (transmit) an unknown quantum state to a distant receiver (Bob) by using two bits of classical communication and an entangled state already shared by the sender (Alice) and the receiver (Bob). Since the publications of these pioneering and fundamental works, several new protocols of quantum communication have been proposed [4]-[39]. Some of these protocols (such as protocols of teleportation, quantum information splitting (QIS), dense coding, etc.) do not require security, whereas the other protocols (such as protocols of QKD, deterministic secure quantum communication (DSQC), quantum secure direct communication (QSDC), quantum dialogue (QD) and quantum secret sharing (QSS), etc.) require security. Most of the protocols of secure quantum communication are unconditionally secure. Usually the security of these protocols is obtained using conjugate coding (i.e., using our inability to simultaneously measure a quantum state in two or more mutually unbiased bases (MUBs)). Most of the existing protocols of QKD and other cryptographic tasks belong to this class [1], [4]-[14]. However, it is possible to obtain security of the protocols solely using orthogonal states (i.e., without using conjugate coding or two or more MUBs). In this type of protocols, encoding, decoding and eavesdropping checking are performed only using orthogonal states. These protocols are fundamentally different from the conjugate-coding-based protocols. In what follows, we refer to these protocols as orthogonal-state-based protocols [15]-[21].

Till 2010, there was no experimental realization of the orthogonal-state-based protocols and such protocols available till then [15]-[17], [22] were applicable to QKD only. This thesis work was started at that time with an intention to design orthogonal-state-based protocols for cryptographic tasks other than QKD. A large number of experimental realization [23]-[26] of orthogonal-state-based QKD protocols were also reported between 2010-2012 (i.e., during the initial phase of this thesis work). These experiments further motivated us to look into the possibility of orthogonal-state-based realization of quantum cryptographic tasks beyond QKD. The thesis is mostly focused on this task and we have reported orthogonal-state-based protocols of QKD, DSQC and QSDC using arbitrary orthogonal multi-partite quantum states (cf. our publication [18]), orthogonal-state-based protocols of quantum key agreement (QKA) using 4-qubit $|\Omega\rangle$ and 4-qubit cluster states (cf. our publication [20]) and orthogonal-state-based protocols of DSQC using entanglement swapping (cf. our publication [19]). Although, the proposed thesis is focused on orthogonal-state-based protocols of secure quantum communication, but it is not limited to that. Specifically, in Chapter 2 of the proposed thesis, we have discussed bidirectional controlled state teleportation (BCST) and in Chapter 3, we have described the generalized structure of hierarchical QIS (HQIS), probabilistic HQIS and hierarchical quantum secret sharing (HQSS).

The proposed thesis has 9 chapters. In the first chapter, a basic introduction to the subject is provided and the aim and achievements of the thesis work are clearly mentioned. Major part of this chapter will be published as a review paper [27]. In Chapters 2-8, we have discussed several aspects of quantum communication and results reported in these chapters are already published as Refs. [11, 12], [18]-[20], [28]-[30]. Finally, the thesis is concluded in Chapter 9, where we have also discussed the limitations of the present work and scope of the future works. In the following sections, the contents of each chapter are briefly described.

2 Chapter 1: Introduction

This chapter provides an introduction to the work reported in this thesis and to the various topics that are discussed in the present thesis (such as QKD, QIS, CT, HQSS, etc.). In this chapter, we have discussed what motivated us for the present study and how to convert a conjugate-coding-based protocol of quantum communication into an orthogonal-state-based protocol for the same communication task. This trick of replacing a BB84 subroutine by a GV subroutine is used in the rest of the chapters to design a bunch of useful orthogonal-state-based protocols. Majority of the observations discussed in this chapter will be published as [27].

3 Chapter 2: Bidirectional controlled teleportation by using 5-qubit states: A generalized view

In this chapter, we have shown that there exists a class of 5-qubit quantum states that can be used for BCST. It is also shown that almost all the reported cases of BCST [31]-[33] are the special cases of the proposed class of 5-qubit quantum states. Further, we have shown that one can, in principle, construct infinitely many 5-qubit quantum states for this purpose. We have also shown that the idea can be extended to bidirectional controlled probabilistic state teleportation. Some potential applications of the proposed scheme and its modified versions are also discussed in relation to the implementation of quantum remote control and quantum cryptography. Thus, this chapter provides a very general perspective to the BCST schemes. The work reported in this chapter is published as [28]. Interestingly, it is possible to construct protocols of controlled bidirectional remote state preparation (RSP) and the same 5-qubit quantum state can be used for that purpose. We have shown this in Ref. [34], but the results related to controlled bidirectional RSP are not included in the present thesis.

4 Chapter 3: Hierarchical quantum communication

In this chapter, a general method to study the HQIS is proposed and the same is used to systematically investigate the possibility of realizing HQIS using different classes of 4-qubit entangled states that are not connected by stochastic local operations and classical communication (SLOCC). Explicit examples of HQIS using 4-qubit cluster state, 4-qubit $|\Omega\rangle$ state and 8-qubit cluster state are provided. Further, the proposed HQIS scheme is generalized to introduce two new aspects of hierarchical quantum communication. To be precise, schemes of probabilistic HQIS and HQSS are introduced by modifying the proposed HQIS scheme. A number of practical situations where hierarchical quantum communication would be of use, are also discussed. The results reported in this chapter are published as [29, 30].

5 Chapter 4: Improved protocols of secure quantum communication using W states

This chapter aims to discuss a set of protocols of quantum communication that use W states. In 2011, Hwang et al. [13] and Yuan et al. [35] proposed two efficient protocols of secure quantum communication using 3-qubit and 4-qubit symmetric W states, respectively. These two dense coding based protocols are generalized and their efficiencies are considerably improved. Simple bounds on the qubit efficiency of DSQC and QSDC protocols are obtained and it is shown that dense coding is not essential for designing of maximally efficient DSQC and QSDC protocols. This fact is used to design maximally efficient protocols of DSQC and QSDC using 3-qubit and 4-qubit W states. Protocols reported in this chapter are conjugate-coding-based. However, it is straightforward to replace the BB84 subroutine used here by the GV subroutine to obtain the equivalent orthogonal-state-based protocol. The results reported in this chapter are published as [11].

6 Chapter 5: Beyond the Goldenberg-Vaidman protocol: Secure and efficient quantum communication using arbitrary, orthogonal, multi-particle quantum states

In this chapter, we have shown that the maximally efficient protocols for secure direct quantum communications can be constructed using any arbitrary orthogonal basis. This establishes that no set of quantum states (e.g., GHZ states, W states, Brown states or cluster states) has an advantage over the others, barring the relative difficulty in physical implementation. The work provides a wide choice of states for experimental realization of secure direct quantum communication protocols. We have also shown that this protocol can be generalized to a completely orthogonal-state-based protocol of GV-type. The security of the proposed GV-type protocol essentially arises from the duality and monogamy of entanglement. This stands in contrast to protocols that employ non-orthogonal states, like BB84 protocol, where the security essentially comes from the non-commutativity in the observable algebra. The results reported in this chapter are published as [18].

7 Chapter 6: Orthogonal-state-based deterministic secure quantum communication without actual transmission of the message qubits

This chapter describes another orthogonal-state-based protocol of DSQC that utilizes the advantage of entanglement swapping. Recently, an orthogonal-state-based protocol of direct quantum communication without actual transmission of particles is proposed by Salih et al. [36] using chained quantum Zeno effect. The counterfactual condition (claim) of Salih et al. is weaken here to the extent that transmission of particles is allowed, but transmission of the message qubits (the qubits on which the secret information is encoded) is not allowed. Remaining within this weaker (non-counterfactual) condition, an orthogonal-state-based protocol of DSQC is proposed using entanglement swapping, where actual transmission of the message qubits is not required. Further, it is shown that there exists a large class of quantum states that can be used to implement the proposed protocol. The security of the proposed protocol originates from monogamy of entanglement. As the protocol can be implemented without using conjugate coding, its security is independent of non-commutativity. The results reported in this chapter are published as [19].

8 Chapter 7: On the group-theoretic structure of a class of quantum dialogue protocols

In this chapter, a sufficient condition for implementation of the QD protocol is obtained and it is shown that the set of unitary operators used for the purpose must form a group under multiplication. A generalized protocol of QD is obtained using the sufficient condition. Further, several examples of possible groups of unitary operators and quantum states that may be used for implementation of QD are systematically generated. As examples, it is shown that GHZ state, GHZ-like state, W state, 4 and 5-qubit cluster states, $|\Omega\rangle$ state, Brown state, Q_4 state and Q_5 state can be used to implement QD protocol. It is also shown that if a quantum system is found to be suitable for QD then that can provide solution of the socialist millionaire problem, too. The works reported in this chapter are published in Ref. [12].

9 Chapter 8: Protocols of quantum key agreement solely using Bell states and Bell measurement

This chapter describes two protocols of QKA that solely use Bell state and Bell measurement. The first protocol of QKA proposed here is designed for two-party QKA, whereas the second protocol is designed for multi-party QKA. The proposed protocols are also generalized to implement QKA using a set of multi-partite entangled states (e.g., 4-qubit cluster state and $|\Omega\rangle$ state etc.). The security of these protocols arises from the monogamy of entanglement. This is in contrast to the existing protocols of QKA where security arises from the use of non-orthogonal state (non-commutativity principle). Further, it is shown that all the quantum systems that are useful for implementation of QD and most of the protocols of secure direct quantum communication can be modified to implement protocols of QKA. The results reported in this chapter are published as [20].

10 Chapter 9: Conclusions and scope of future works

The thesis is summarized in this chapter. To be precise, in the present work, we have designed several new protocols of quantum communication and have analyzed their efficiency and security. In addition, we have also improved some of the existing protocols of secure quantum communication in terms of their efficiency and security. More interestingly, almost all the works reported here are general in nature in the sense that many other results can be obtained as special cases of it. In brief, we can conclude the present work with the following three major points describing the summary of the present work:

1. **Generalized structure of the quantum communication protocols:** We have generalized the protocols in such a way that the intrinsic symmetry of the existing protocols are revealed and used. Interestingly, many authors have been proposed several aspects of secure and insecure quantum communication using specific quantum states, but we have established that no quantum state is special, and these protocols can be designed with a large class of quantum states. Our generalized approach provides a wide choice of quantum states that can be used by the experimentalists interested in the experimental implementation of the protocols.

2. **Orthogonal-state-based quantum cryptography:** The security of the majority of the existing protocols of secure quantum communication is obtained by using conjugate coding, i.e., by using non-orthogonal quantum states (i.e., using two or more MUBs).

For example, in BB84 protocol, security arises due to quantum non-commutativity. Contrary to the conjugate-coding-based protocols, a few completely orthogonal-state-based protocols of unconditionally secure QKD (such as, GV and Noh (N09)) were also known. However, we have generalized the idea and proposed the completely orthogonal state-based-protocols of QKD, QKA, DSQC and QSDC.

3. **Notion of probabilistic hierarchical quantum information splitting (PHQIS) and hierarchical quantum secret sharing (HQSS):** We have generalized the idea of HQIS, and then by modifying it, we have proposed two new schemes of PHQIS and HQSS. Importantly, our protocols of PHQIS and HQSS are the first protocols of their kind. In PHQIS scheme, we have shown that HQIS can also be done in the probabilistic way, where the success rate of the scheme is not unity. The proposed schemes of HQSS are very interesting and of much practical importance because HQSS can be used in several realistic situations.

10.1 Limitations and future scope of the works

Limitations of the present work are intrinsically connected with the scope of future works. Specifically, here we list a few aspects of quantum communication which can be addressed in the future using the methodology developed here.

1. Following a similar line of arguments as is adopted in Chapter 3, one can also obtain a scheme for probabilistic HQSS and hierarchical joint remote state preparation.

2. In the secure quantum communication protocols described here, we have assumed that the stations of Alice and Bob are secure. Thus, the unconditional security claimed here is valid under the assumption that Alice's and Bob's ports are safe. This is a limitation of the present work. This is so because, several side channel attacks are proposed in the recent past and it is also shown that it is possible to design quantum device-independent (DI) protocols of QKD [37, 38]. Following similar logic, in the future one can design DI versions of the protocols proposed here.

3. In future, the present study may be extended to study of device independence from a general perspective (including the possibility of obtaining device-independent protocols in post-quantum theory) and to explore the possibility of using Kochen-Specker theorem or Leggett-Garg inequality for designing of the new protocols.

4. In this thesis, we have not discussed the effect of noise on the quantum channels. However, in a recent paper [34] (the work reported in [34] is not part of the present

thesis), we have studied the effect of amplitude damping and phase damping on the protocols of controlled bidirectional RSP. As the general structure of the 5-qubit state used there is same as that of the 5-qubit state used in the BCST, we can easily study the effect of noise on BCST. Further, in addition to the effect of amplitude damping and phase damping noise, effect of other noise models such as generalized amplitude damping, squeezed general amplitude damping, etc., can be investigated in the context of BCST and other protocols discussed here.

5. As a general approach is adopted in this theoretical work and different alternative quantum channels are provided to implement QKD, QKA, DSQC, QSDC, QD, BCST, HQIS, PHQIS and HQSS. We hope the experimental realization of some of the proposals of the present work will be reported in the near future.

Considering the above scope of future works and the possibilities of experimental realization of the present work, we have concluded this thesis with the expectation that the present thesis work will contribute toward future development of quantum communication and some of the theoretical ideas developed here will be used for secure communication in real life.

References

[1] Bennett C.H., Brassard G., *“Quantum Cryptography: Public Key Distribution and Coin Tossing”*, Proc. of the IEEE Int. Conference on Computers, Systems, and Signal Processing, Bangalore, India, pp. 175-179, 1984.

[2] Bennett C.H., Wiesner S.J., *“Communication via One- and Two-Particle Operators on Einstein-Podolsky-Rosen States”,* Phys. Rev. Lett. vol. 69, pp. 2881-2884, 1992.

[3] Bennett C.H., Brassard G., Crépeau C., Jozsa R., Peres A., Wootters W.K., *“Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels”*, Phys. Rev. Lett., vol. 70, pp. 1895-1899, 1993.

[4] Ekert A.K., *“Quantum Cryptography Based on Bell’s Theorem”*, Phys. Rev. Lett., vol. 67, pp. 661-663, 1991.

[5] Bennett C.H., *“Quantum Cryptography using any Two Nonorthogonal States”*, Phys. Rev. Lett., vol. 68, pp. 3121-3124, 1992.

[6] Long G.L., Liu X.S., *“Theoretically Efficient High-Capacity Quantum-Key-Distribution Scheme”*, Phys. Rev. A, vol. 65, pp. 032302, 2002.

[7] Boström K., Felbinger T., *"Deterministic Secure Direct Communication using Entanglement"*, Phys. Rev. Lett., vol. 89, pp. 187902, 2002.

[8] Lucamarini M., Mancini S., *"Secure Deterministic Communication without Entanglement"*, Phys. Rev. Lett., vol. 94, pp. 140501, 2005.

[9] An N.B., *"Quantum Dialogue"*, Phys. Lett. A, vol. 328, pp. 6-10, 2004.

[10] Deng F.-G., Long G.L., Liu X.-S., *"Two-Step Quantum Direct Communication Protocol using the Einstein-Podolsky-Rosen Pair Block"*, Phys. Rev. A, vol. 68, pp. 042317, 2003.

[11] Shukla C., Banerjee A., Pathak A., *"Improved Protocols of Secure Quantum Communication using W States"*, Int. J. Theor. Phys., vol. 52, pp. 1914-1924, 2013.

[12] Shukla C., Kothari V., Banerjee A., Pathak A., *"On the Group-Theoretic Structure of a Class of Quantum Dialogue Protocols"*, Phys. Lett. A, vol. 377, pp. 518-527, 2013.

[13] Hwang T., Hwang C.C., Tsai C.W., *"Quantum Key Distribution Protocol using Dense Coding of Three-Qubit W State"*, Eur. Phys. J. D, vol. 61, pp. 785-790, 2011.

[14] Cao H.-J., Song H.-S., *"Quantum Secure Direct Communication with W State"*, Chin. Phys. Lett., vol. 23, pp. 290-292, 2006.

[15] Goldenberg L., Vaidman L., *"Quantum Cryptography Based on Orthogonal States"*, Phys. Rev. Lett., vol. 75, pp. 1239-1243, 1995.

[16] Noh T.-G., *"Counterfactual Quantum Cryptography"*, Phys. Rev. Lett., vol. 103, pp. 230501, 2009.

[17] Guo G.-C., Shi B.-S., *"Quantum Cryptography Based on Interaction-Free Measurement"*, Phys. Lett. A, vol. 256, pp. 109-112, 1999.

[18] 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. Quantum Inf., vol. 10, pp. 1241009, 2012.

[19] Shukla C., Pathak A., *"Orthogonal-State-Based Deterministic Secure Quantum Communication without Actual Transmission of the Message Qubits"* Quantum Inf. Process., vol. 13, pp. 2099-2113, 2014.

[20] Shukla C., Alam N., Pathak A., *"Protocols of Quantum Key Agreement Solely using Bell States and Bell Measurement"* Quantum Inf. Process., vol. 13, pp. 2391-2405, 2014.

[21] Yadav P., Srikanth R., Pathak A., *"Two-Step Orthogonal-State-Based Protocol of Quantum Secure Direct Communication with the help of Order-Rearrangement Technique"*, Quantum Inf. Process. DOI 10.1007/s11128-014-0825-8, 2014.

[22] Koashi M., Imoto N., *"Quantum Cryptography Based on Split Transmission of One-Bit Information in Two Steps"*, Phys. Rev. Lett., vol. 79, pp. 2383-2386, 1997.

[23] Avella A., Brida G., Degiovanni I.P., Genovese M., Gramegna M., Traina P., *"Experimental Quantum-Cryptography Scheme Based on Orthogonal States"*, Phys. Rev. A, vol. 82, pp. 062309, 2010.

[24] Ren M., Wu G., Wu E., Zeng H., *"Experimental Demonstration of Counterfactual Quantum Key Distribution"*, Laser Phys., vol. 21, pp. 755-760, 2011.

[25] Brida G., Cavanna A., Degiovanni I.P., Genovese M., Traina P., *"Experimental Realization of Counterfactual Quantum Cryptography"*, Laser Phys. Lett., vol. 9, pp. 247-252, 2012.

[26] Liu Y., Ju L., Liang X.-L., Tang S.-B., Tu G.-L. S., Zhou L., Peng C.-Z., Chen K., Chen T.-Y., Chen Z.-B., Pan J.-W., *"Experimental Demonstration of Counterfactual Quantum Communication"*, Phys. Rev. Lett., vol. 109, pp. 030501, 2012.

[27] Shukla C., Banerjee A., Pathak A., Srikanth R., *"Secure Quantum Communication with Orthogonal States"*, submitted to Int. J. Quantum Inf., arxiv:1407.3412v1 (quant-ph), 2014.

[28] Shukla C., Banerjee A., Pathak A., *"Bidirectional Controlled Teleportation by using 5-Qubit States: A Generalized View"*, Int. J. Theor. Phys. vol. 52, pp. 3790-3796, 2013.

[29] Shukla C., Pathak A., *"Hierarchical Quantum Communication"*, Phys. Lett. A, vol. 377, pp. 1337-1344, 2013.

[30] Shukla C., Pathak A., *"Different Useful Aspects of Hierarchical Quantum Communication"*, 13th Asian Quantum Information Science Conference, IMSc, Chennai, India, pp. 167-168, 25-30 August, 2013.

[31] Zha X.-W., Zou Z.-C., Qi J.-X., Song H.-Y., *"Bidirectional Quantum Controlled Teleportation via Five-Qubit Cluster State"*, Int. J. Theor. Phys., vol. 52, pp. 1740-1744, 2013.

[32] Zha X.-W., Song H.-Y., Ma G.-L., *"Bidirectional Swapping Quantum Controlled Teleportation Based on Maximally Entangled Five-Qubit State"*, arxiv:1006.0052 (quant-ph), 2010.

[33] Li Y.-h., Nie L.-p., *"Bidirectional Controlled Teleportation by using a Five-Qubit Composite GHZ-Bell State"*, Int. J. Theor. Phys., vol. 52, pp. 1630-1634, 2013.

[34] Sharma V., Shukla C., Banerjee S., Pathak A., *"Controlled Bidirectional Remote State Preparation"*, arxiv:1409.0833v1 (quant-ph), 2014.

[35] 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 Rearrangement of Particle Pairs"*, Int. J. Theor. Phys., vol. 50, pp. 2403-2409, 2011.

[36] Salih H., Li Z.-H., Al-Amri M., Zubairy M.S., *"Protocol for Direct Counterfactual Quantum Communication"*, Phys. Rev. Lett., vol. 110, pp. 170502, 2013.

[37] Pironio S., Acín A., Brunner N., Gisin N., Massar S., Scarani V., *"Device-Independent Quantum Key Distribution Secure Against Collective Attacks"*, New Journal of Physics, vol. 11, pp. 045021, 2009.

[38] Barrett J., Hardy L., Kent A., *"No Signaling and Quantum Key Distribution"*, Phys. Rev. Lett., vol. 95, pp. 010503, 2005.

[39] Banerjee A., Pathak A., *"Maximally Efficient Protocols for Direct Secure Quantum Communication"*, Phys. Lett. A, vol. 376, pp. 2944-2950, 2012.

LIST OF PUBLICATIONS

Publications in International Journals

1. **Shukla C.**, Banerjee A., Pathak A., *"Bidirectional Controlled Teleportation by using 5-Qubit States: A Generalized View"*, Int. J. Theor. Phys. vol. 52, pp. 3790-3796, 2013. (**Thomson Reuters I.F.** = 1.188, **h index** = 39, h5-index = 26, **Published by** Springer New York, **Indexed in** SCI and SCOPUS).

2. **Shukla C.**, Pathak A., *"Hierarchical Quantum Communication"*, Phys. Lett. A, vol. 377, pp. 1337-1344, 2013. (**Thomson Reuters I.F.** = 1.766, **h index** = 123, h5-index = 49, **Published by** Elsevier, **Indexed in** SCI and SCOPUS).

3. **Shukla C.**, Banerjee A., Pathak A., *"Improved Protocols of Secure Quantum Communication using W States"*, Int. J. Theor. Phys., vol. 52, pp. 1914-1924, 2013. (**Thomson Reuters I.F.** = 1.188, **h index** = 39, h5-index = 26, **Published by** Springer New York, **Indexed in** SCI and SCOPUS).

4. **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. Quantum Inf., vol. 10, pp. 1241009, 2012. (**Thomson Reuters I.F.** = 0.918, **h index** = 22, h5-index = 17, **Published by** World Scientific Publishing Co. Pte Ltd., **Indexed in** SCI and SCOPUS).

5. **Shukla C.**, Pathak A., *"Orthogonal-State-Based Deterministic Secure Quantum Communication without Actual Transmission of the Message Qubits"* Quantum Inf. Process., vol. 13, pp. 2099-2113, 2014. (**Thomson Reuters I.F.** = 2.960, **h index** = 22, h5-index = 22, **Published by** Springer New York, **Indexed in** SCI and SCOPUS).

6. **Shukla C.**, Kothari V., Banerjee A., Pathak A., *"On the Group-Theoretic Structure of a Class of Quantum Dialogue Protocols"*, Phys. Lett. A, vol. 377, pp. 518-527, 2013. (**Thomson Reuters I.F.** = 1.766, **h index** = 123, h5-index = 49, **Published by** Elsevier, **Indexed in** SCI and SCOPUS).

7. **Shukla C.**, Alam N., Pathak A., *"Protocols of Quantum Key Agreement Solely using Bell States and Bell Measurement"* Quantum Inf. Process., vol. 13, pp. 2391-2405, 2014. (**Thomson Reuters I.F.** = 2.960, **h index** = 22, h5-index = 22, **Published by** Springer New York, **Indexed in** SCI and SCOPUS).

8. **Shukla C.**, Banerjee A., Pathak A., Srikanth R., *"Secure Quantum Communication with Orthogonal States"*, submitted to Int. J. Quantum Inf., (arxiv:1407.3412v1 (quant-ph), 2014). (**Thomson Reuters I.F.** = 0.918, **h index** = 22, h5-index = 17, **Published by** World Scientific Publishing Co. Pte Ltd., **Indexed in** SCI and SCOPUS).

Communicated (Not included in the thesis)

1. **Shukla C.**, Banerjee A., Pathak A., *"Protocols and Quantum Circuits for Implementing Entanglement Concentration in Cat state, GHZ-like state and 9 Families of 4-Qubit Entangled States"*, arxiv:1403.6987v1 (quant-ph), 2014.

2. Sharma V., **Shukla C.**, Banerjee S., Pathak A., *"Controlled Bidirectional Remote State Preparation"*, arxiv:1409.0833v1 (quant-ph), 2014.

3. Mishra S., **Shukla C.**, Pathak A., Srikanth R., Venugopalan A., "*A Simplified Hierarchical Dynamic Quantum Secret Sharing Protocol with Added Features"*, arxiv:1409.2037v1 (quant-ph), 2014.

Conference paper

1. **Shukla C.**, Pathak A., *"Different Useful Aspects of Hierarchical Quantum Communication"*, International Conference, 13th Asian Quantum Information Science Conference (AQIS-13), IMSc, Chennai, India, pp. 167-168, Aug. 25-30, 2013. **[Poster Presentation]**

Chitra Shukla

(Research Scholar)

Dr. Amit Verma

Prof. Anirban Pathak

(Supervisors)