Secure quantum communication beyond QKD

Anirban Pathak

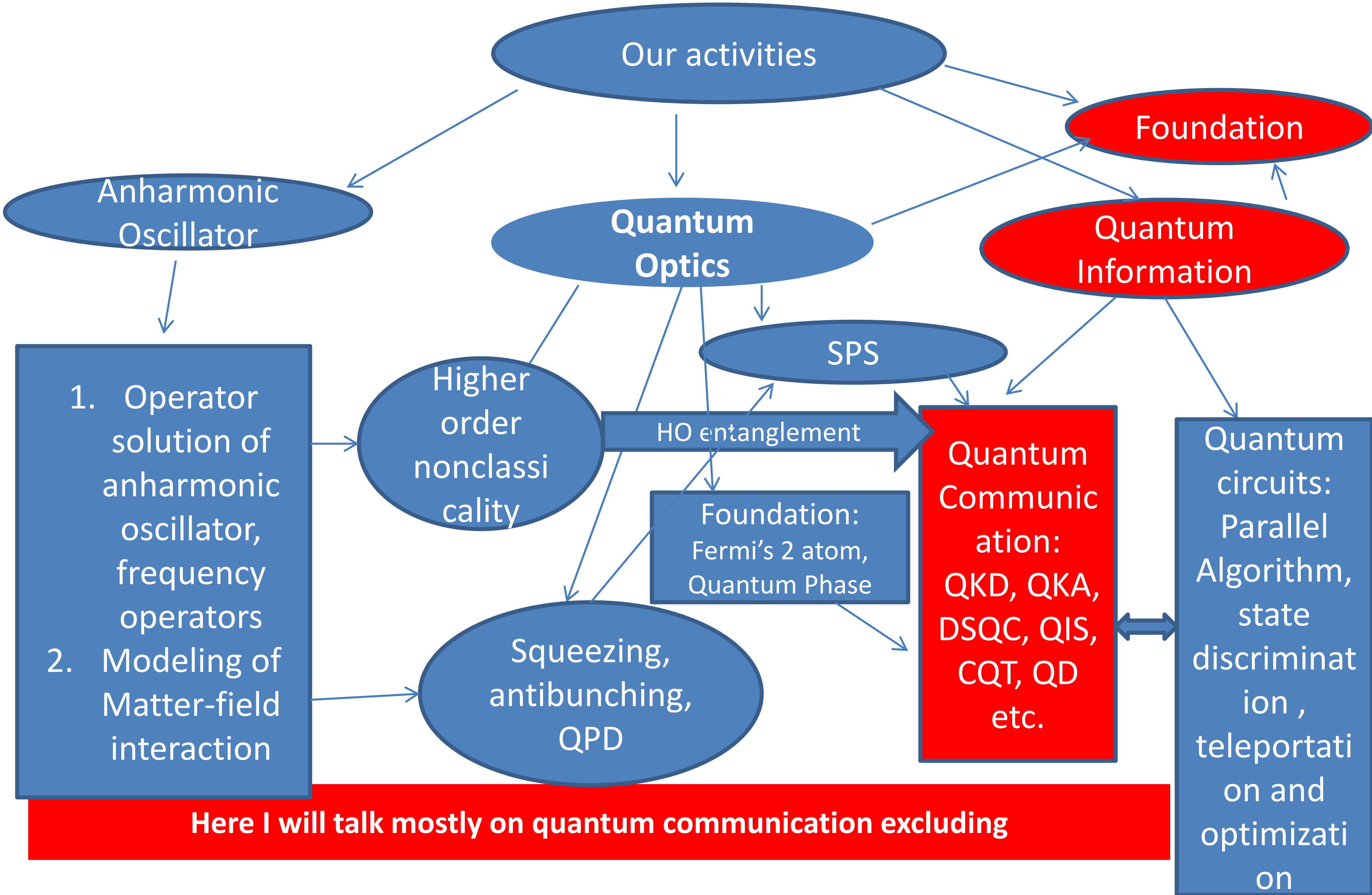
Jaypee Institute of Information Technology, Noida, India

International Program on Quantum Information 2014 (IPQI-14), IOP Bhubaneswar, 24 February, 2014

What do we mean by quantum communication beyond QKD?

- **QKD: Distribution of unconditionally secure key among legitimate users. Usually one user (Alice) prepares and distributed it. Encryption is usually hybrid (classical encryption with quantum key) technology.**
- **Quantum Cryptography Beyond QKD**
  - **Secure direct communication=>DSQC and QSDC (**Maximally efficient protocols for direct secure quantum communication, A. Banerjee and A. Pathak, Phys. Lett A **376** (2012) 2944-2950; Beyond the Goldenberg-Vaidman protocol: Secure and efficient quantum communication using arbitrary, orthogonal, multi-particle quantum states, C. Shukla, A. Pathak and R. Srikanth, Int. J. Quant. Info., **10** (2012) 1241009.)
  - **Quantum dialogue and solution of socialist millionaire problem (**On the group-theoretic structure of a class of quantum dialogue protocols, C. Shukla, V. Kothari, A. Banerjee and A. Pathak, Phys. Lett. A, **377** (2013) 518.)
  - **Quantum cryptographic switch** (The quantum cryptographic switch, N. Srinatha, S. Omkar, R. Srikanth, S. Banerjee and A. Pathak, Quant. Infor. Process. **13** (2014) 59-70.)
  - **Hierarchical quantum communication** (Hierarchical quantum communication, C. Shukla and A. Pathak, Phys. Lett. A **377** (2013) 1337-1344.)
  - **Quantum key agreement (**Orthogonal-state-based protocols of quantum key agreement, C. Shukla, N. Alam and A. Pathak**,** arxiv: 1310.1435 (quant-ph).

We do IT with both bit and qubit



Our activities

Anharmonic Oscillator

Quantum Optics

Foundation

Quantum Information

1. Operator solution of anharmonic oscillator, frequency operators
2. Modeling of Matter-field interaction

Higher order nonclassicality

SPS

HO entanglement

Quantum Communication: QKD, QKA, DSQC, QIS, CQT, QD etc.

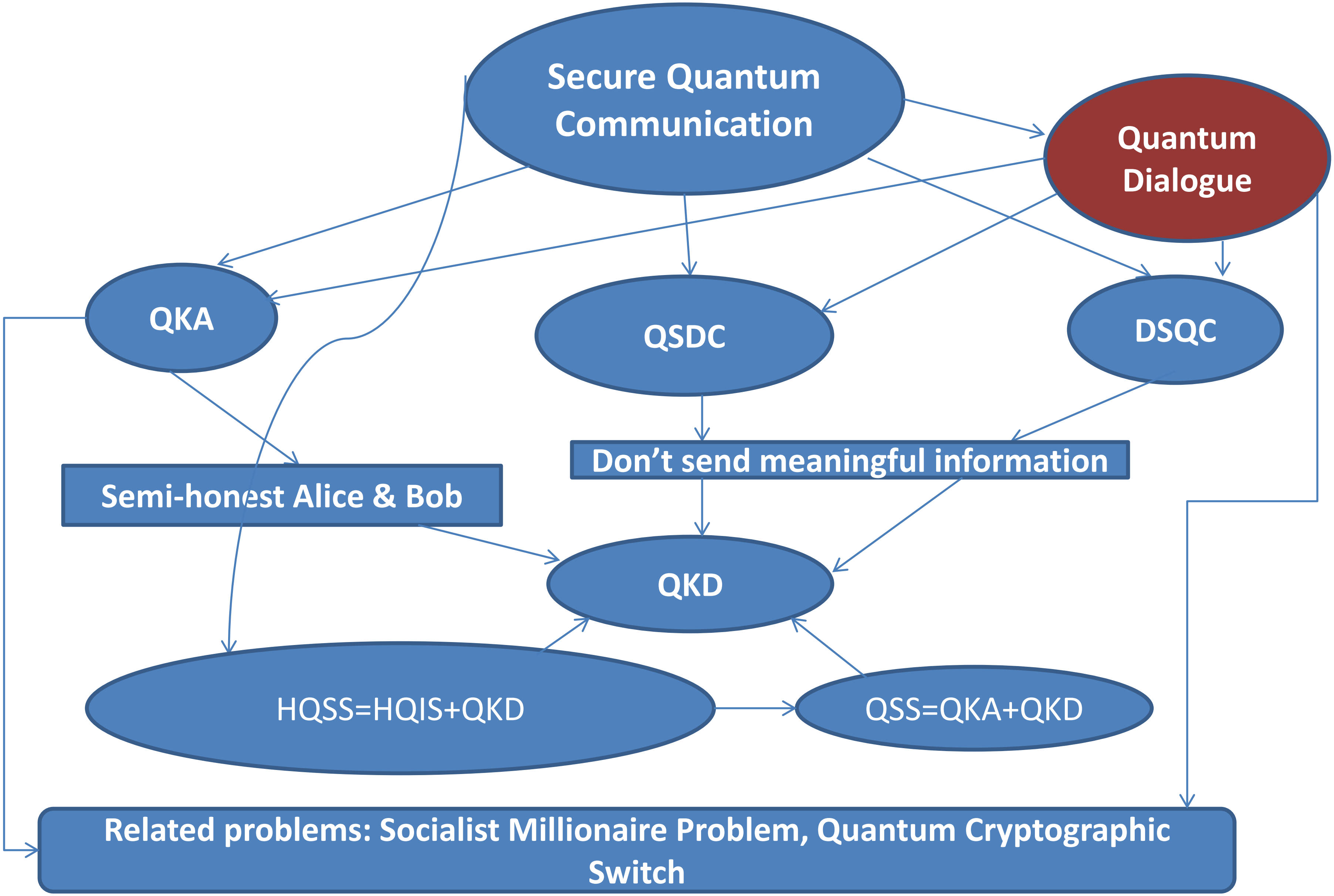
Quantum circuits: Parallel Algorithm, state discrimination , teleportation and optimization

Foundation: Fermi's 2 atom, Quantum Phase

Squeezing, antibunching, QPD

Here I will talk mostly on quantum communication excluding

How are different aspects of quantum cryptography connected?



Secure Quantum Communication

Quantum Dialogue

QKA

QSDC

DSQC

Semi-honest Alice & Bob

Don’t send meaningful information

QKD

HQSS=HQIS+QKD

QSS=QKA+QKD

Related problems: Socialist Millionaire Problem, Quantum Cryptographic Switch

Practical situations that require protocols beyond conventional QKD: Situation1

Alice: President of a country,

Diana: Defence minister of that country.

Bob: Defence secretary.

Charlie: The chief of the armed forces.

If the president wishes to permit the use of a nuclear weapon at a suitable time then she distributes an information (say, a key required to unlock the nuclear weapon) among the defence minister, the defence secretary and the chief of the armed forces in such a way that the minister can unlock the weapon if either the defence secretary or the chief of the armed forces agrees and cooperates with him. However, if the chief of the armed forces or the defence secretary wants to unlock the weapon they would require the cooperation of each other and that of the defence minister, too.

The defence minister is more powerful than the chief of the armed forces and the defence secretary, but even she is not powerful enough to unlock the weapon alone.

Observation: There exists a hierarchy

What do we need: Hierarchical Quantum Secret Sharing (HQSS)

Practical situations that require protocols beyond conventional QKD: Situation 2-3

Banking requires hierarchy: HQSS is required in banking sector, where a bank manager and/or cashier is usually more powerful than the other users (office assistants and secretaries). However, even the bank manager alone is not powerful enough to perform all the financial operations related to his bank. For example, the password required to unlock an ATM is always split into two or more pieces and the manager alone cannot unlock it.

Situation3: Hierarchical secret sharing is also essential for the smooth operation of the departmental stores.

quantum cryptographic switch

Practical situation 4

The director of an organization wishes to keep control over the time and amount of information to be disclosed to an employee of the company.

Consider that Charlie is VC/Rector of a university, Alice is register who keeps the records and Bob is an employ who needs a file, but Alice can send a file to Bob if and only if Charlie allows him to do so. Further, Charlie wants to control the amount of information Bob can read from the file sent by Alice.

Note: The custodian of the files (Alice) must not be worse than semi-honest, as she could otherwise create her own classical/quantum channel and communicate directly with Bob. But there is always a potential chance that Charlie can detect such communication.

Practical situation 5

The owner of a company (Charlie) has asked his semi-honest assistant (Alice) to send details of all his shares to a stock exchange broker Bob, to sell it in the stock market. But Charlie wishes to keep an eye on stock fluctuations and to permit Bob to sell his shares only at some suitable time.

Situation 6: Socialist Millionaire problem.

Security models: semi-honest models vs. malicious models

- Security models in the context of secure multiparty communication:
    1. Semi-honest model
    2. Malicious model.
- In a semi-honest model, a protocol is considered secure against a collusion of participants (Alice and Bob in our case) if by accumulating their data, these participants cannot gain more information than what they can from the input and output of the protocol alone. A semi-honest party strictly follows the protocol.
- In a malicious model, participants can deviate from the orignal protocol.
- The protocols described in this talk and the similar protocols are not secure under a malicious model.

Ideal cryptographic switch

(Quant. Infor. Process. **13** (2014) 59-70)

In the ideal situation, our protocol works as follows:

1. After receiving Alice’s request, Charlie prepares *n Bell states (not all the same)* and sends the first qubits of all the Bell states to Alice and the second qubits to Bob. Charlie does not disclose which Bell state, he has prepared.
2. After receiving the qubits from Charlie, Alice understands that she has been permitted to send the information to Bob.
3. Alice uses dense coding to encode two bits of classical information on each qubit and transmits her qubits to Bob.
4. When Charlie plans to allow Bob to know the secret information communicated to him, he discloses the Bell state he had prepared.
5. Since the initial Bell state is known, by measuring his qubits in the Bell basis, Bob obtains the information encoded by Alice.

Note: Bob can perform Step 5 (i.e., measurement in the Bell basis) before Step 4 but he will not obtain any meaningful information without the knowledge of the initial state. A

Motivated by: Adhikari, S., Chakrabarty, I.,Agrawal, P.: Probabilistic secret sharing through noisy quantum channels, arXiv:1012.5570v2

Restrictions imposed on the ideal quantum cryptographic switch

- **Channel is one way:** Bell-state measurement can reveal the state prepared by Charlie if both the qubits are in the possession of Alice or Bob. By the assumption that the channel between Alice and Bob is one-way, Bob cannot send his qubits to Alice for a Bell-state measurement.

- **Alice is semi honest:** Alice does not send her qubits to Bob as she is assumed to be a semi-honest party, who strictly follows the protocol. Her semi-honesty is motivated by the fact that, while she may wish to potentially cheat Charlie, she wants her communication to Bob to be secure both in the sense of being protected from the rest of the world (in the usual QKD sense) as well as being undetected by Charlie.

- Alice may protect her information from outside world by inserting decoy qubits.

Notion of quantum cryptographic switch

- Bob measures the two qubits in his possession to obtain the state that corresponds to Alice's encoding.
- Bob can decode the full information only if Charlie shares the full classical *key information c that would make the* initial entangled state pure.

Note: In absence of full information the pure state prepared by Charlie would appear as mixed state to Alice and Bob.

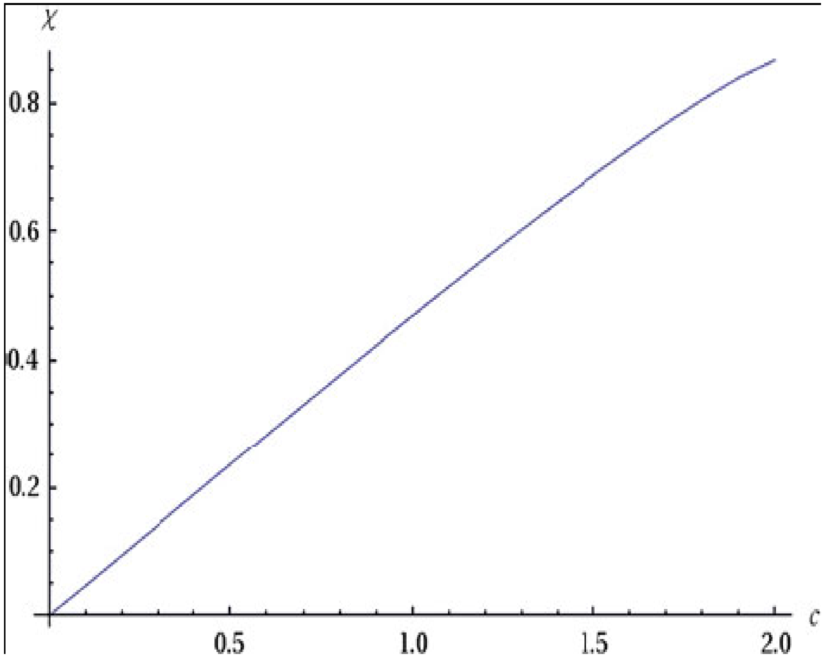
- Generally, Bob recovers Alice's transmitted bits depending on the key information obtained from Charlie. Thus Charlie acts as a *cryptographic switch who can determine the level of information Alice sends*

  to Bob *after the full transmission of her qubit.*

Note: We can consider a family of protocols in which the key information *c varies continuously* as $0 \leq c \leq c_{max}$ *= 2. Our protocol is characterized by* $c_{max} = 2$.

- ***Example****:* a continuous-valued key corresponds to an arbitrary probability distribution over the Bell states. For example, Charlie may choose to reveal that the parity-0 Bell states are twice more like than parity-1 states and that Bell states of equal parity are equally likely. This corresponds to a probability distribution, $\left(\frac{1}{3},\frac{1}{3},\frac{1}{6},\frac{1}{6}\right)$, i.e., an entropy of about 1.92 bits, implying that Charlie reveals *c = 0.08 bits.*

Information recovered by Bob, quantified by the Holevo quantity *χ, as a function of the key* information *c communicated by Charlie, in the noiseless case*



Can we remove the restrictions on the channel?

Yes, Charlie has to change her strategy and apply a random permutation on the qubits to be sent to Bob.

Since the sequence with Alice and Bob are different, even if they cooperate, *they will not be* able to find out the Bell states prepared by Charlie as they don’t know which particle of Bob is entangled with which particle of Alice.

PoP (Particle order permutation) is an excellent technique as it allows us to convert almost all conjugate coding-based quantum cryptographic protocols into corresponding orthogonal state based protocol.

Quantum Dialogue: Ba An protocol

1. Bob prepares large number of copies of a Bell state $|\phi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$. He keeps the first photon of each qubit with himself as home photon and encodes her secret message 00; 01; 10 and 11 by applying unitary operations U_0,U_1,U_2 and U_3 respectively on the second qubit. Without loss of generality we may assume that U_0 = I; U_1 = X; U_2 = iY and U_3 = Z.
2. Bob then sends the second qubit (travel qubit) to Alice and confirms that Alice has received a qubit.
3. Alice encodes her secret message by using the same set of encoding operations as was used by Bob and sends back the travel qubit to Bob. After receiving the encoded travel qubit Bob measures it in Bell Basis.
4. Alice announces whether it was a run in message mode (MM) or in control mode (CM). In a MM run, Bob decodes Alice's bits and announces his Bell basis measurement result. Alice uses that result to decode Bob's bits. In a CM run, Alice reveals her encoding value to Bob to check the security of their dialogue.

Information is spitted in a clever way.
The protocol is not secured under intercept-resend attack.
Unitary operators should form a group under multiplication

Sufficiency condition for quantum dialogue

- If we have a mutually orthogonal set of n-qubit states $\{|\phi_0\rangle, |\phi_1\rangle, \ldots, |\phi_{2^n-1}\rangle\}$ and a set of m-qubit $(m \le n)$ unitary operators

$$\{U_0, U_1, U_2, \ldots, U_{2^n-1}\} : U_i|\phi_0\rangle = |\phi_i\rangle \text{ and } \{U_0, U_1, U_2, \ldots, U_{2^n-1}\}$$

forms a group under multiplication then it would be sufficient to construct a quantum dialogue protocol of Ba An type using this set of quantum states and this group of unitary operators.

Rearrangement of order of the particles and insertion of decoy photons make the protocol ~~(unconditionaly)~~ secure.

Structure of the m-qubit unitary operators.

- We are restricting ourselves in discrete variable communications.
- Application of Hadamard, phase gate etc. will make the output non-orthogonal to input and consequently the states will not remain indistinguishable. Therefore,

$$U(m)=U_1(1)\otimes U_2(1)\otimes\cdots\otimes U_m(1):U_i(1)\in\{I,\sigma_x,i\sigma_y,\sigma_z\},$$

How to form groups of unitary operators?

Consider Pauli group with a different multiplication rule where global phase is ignored

$$G_1 = \{I, \sigma_X, i\sigma_y, \sigma_z\} \text{ forms a group of order } 4$$

$$\therefore G_n = \{I, \sigma_X, i\sigma_y, \sigma_z\}^{\otimes n} = G_1^{\otimes n} \text{ forms a group of order } 4^n$$

Example:

$$\begin{aligned} G_2 &= G_1 \otimes G_1 = \{\mathrm{I}, \sigma_x, \mathrm{i}\sigma_y, \sigma_z\} \otimes \{I, \sigma_x, i\sigma_y, \sigma_z\} \\ &= \{I \otimes I, I \otimes \sigma_x, I \otimes i\sigma_y, I \otimes \sigma_z, \sigma_x \otimes I, \sigma_x \otimes \sigma_x, \sigma_x \otimes i\sigma_y, \sigma_x \otimes \sigma_z, \\ &\quad i\sigma_y \otimes I, i\sigma_y \otimes \sigma_x, i\sigma_y \otimes i\sigma_y, i\sigma_y \otimes \sigma_z, \sigma_z \otimes I, \sigma_z \otimes \sigma_x, \sigma_z \otimes i\sigma_y, \sigma_z \otimes \sigma_z\} \end{aligned}$$

Subgroups of G$_2$

$$\begin{aligned}
G_2^1(8) &= \{I,\sigma_x,i\sigma_y,\sigma_z\}\otimes\{I,\sigma_x\} &&= \{I\otimes I, X\otimes I, iY\otimes I, Z\otimes I, I\otimes X, X\otimes X, iY\otimes X, Z\otimes X\}\\
G_2^2(8) &= \{I,\sigma_x,i\sigma_y,\sigma_z\}\otimes\{I,i\sigma_y\} &&= \{I\otimes I, X\otimes I, iY\otimes I, Z\otimes I, I\otimes iY, X\otimes iY, iY\otimes iY, Z\otimes iY\}\\
G_2^3(8) &= \{I,\sigma_x,i\sigma_y,\sigma_z\}\otimes\{I,\sigma_z\} &&= \{I\otimes I, X\otimes I, iY\otimes I, Z\otimes I, I\otimes Z, X\otimes Z, iY\otimes Z, Z\otimes Z\}\\
G_2^4(8) &= \{I,\sigma_x\}\otimes\{I,\sigma_x,i\sigma_y,\sigma_z\} &&= \{I\otimes I, I\otimes X, I\otimes iY, I\otimes Z, X\otimes I, X\otimes X, X\otimes iY, X\otimes Z\}\\
G_2^5(8) &= \{I,i\sigma_y\}\otimes\{I,\sigma_x,i\sigma_y,\sigma_z\} &&= \{I\otimes I, I\otimes X, I\otimes iY, I\otimes Z, iY\otimes I, iY\otimes X, iY\otimes iY, iY\otimes Z\}\\
G_2^6(8) &= \{I,\sigma_z\}\otimes\{I,\sigma_x,i\sigma_y,\sigma_z\} &&= \{I\otimes I, I\otimes X, I\otimes iY, I\otimes Z, Z\otimes I, Z\otimes X, Z\otimes iY, Z\otimes Z\}
\end{aligned}$$

$$\begin{aligned}
G_2^7(8) &= \{I\otimes I, I\otimes Z, Z\otimes I, Z\otimes Z, X\otimes X, iY\otimes X, X\otimes iY, iY\otimes iY\}\\
G_2^8(8) &= \{I\otimes I, Z\otimes Z, X\otimes iY, iY\otimes X, I\otimes X, Z\otimes iY, iY\otimes I, X\otimes Z\}\\
G_2^9(8) &= \{I\otimes I, Z\otimes Z, X\otimes iY, iY\otimes X, X\otimes I, iY\otimes Z, Z\otimes X, I\otimes iY\}\\
G_2^{10}(8) &= \{I\otimes I, X\otimes I, I\otimes X, X\otimes X, Z\otimes Z, iY\otimes Z, Z\otimes iY, iY\otimes iY\}\\
G_2^{11}(8) &= \{I\otimes I, iY\otimes I, I\otimes iY, iY\otimes iY, Z\otimes Z, Z\otimes X, X\otimes Z, X\otimes X\}
\end{aligned}$$

$G_n^j(m)$ is jth subgroup of order m < 4^n of G_n.

Subgroups of G_n

$$G_1^{\otimes i}\{1, X\}G_1^{\otimes(n-i-1)}, G_1^{\otimes i}\{1, iY\}G_1^{\otimes(n-i-1)}, G_1^{\otimes i}\{1, Z\}G_1^{\otimes(n-i-1)},$$

where i varies from 0 to n-1.

Example: Following are order 32 subgroups of G_3

$$\begin{gathered}
G_3^1(32) = G_2 \otimes \{I, X\}, G_3^2(32) = G_2 \otimes \{I, iY\}, G_3^3(32) = G_2 \otimes \{I, Z\}, \\
G_3^4(32) = \{I, X\} \otimes G_2, G_3^5(32) = \{I, iY\} \otimes G_2, G_3^6(32) = \{I, Z\} \otimes G_2, \\
G_3^7(32) = G_1 \otimes \{I, X\} \otimes G_1, G_3^8(32) = G_1 \otimes \{I, iY\} \otimes G_1, G_3^9(32) = G_1 \otimes \{I, Z\} \otimes G_1.
\end{gathered}$$

Are these groups useful for QD?

Quantum State	Dense coding for QD can be done using group of unitary operations
Bell states	G_1
4 qubit Cluster state, Ω state	G_2
GHZ state	$G_2^1(8), G_2^2(8), G_2^4(8), G_2^5(8)$
GHZ-like state	$G_2^2(8), G_2^3(8), G_2^5(8), G_2^6(8), G_2^8(8), G_2^9(8)$
W state	$G_2^8(8), G_2^9(8)$
Q_4 state	$G_2^6(8), G_2^7(8).$
Q_5 state	$G_2^3(8), G_2^4(8), G_2^5(8)$
5 qubit Brown state	$G_3^1(32), G_3^2(32), G_3^4(32), G_3^5(32), G_3^7(32), G_3^8(32).$
5 qubit cluster state	$G_3^4(32), G_3^5(32), G_3^7(32), G_3^8(32)$

Quantum dialogue protocols can be implemented in several ways

Socialist Millionaire problem: Application of dense coding achieved by groups of unitary operators

- Charlie is a semi-honest third party who creates entangled states of the last table, keeps home photons and sends the travel photons to Bob. Bob encodes his asset value and sends it to Alice. Alice encodes her asset value and sends it to Charlie. Charie measures the state in appropriate basis. If her outcome is same as the initial state then Alice and Bob has equal assets otherwise not. No one knows whose asset is more and what is the exact amount of asset.

We have obtained several solutions of this problem under a semi-honest model as Charlie needs to be semi-honest.

- Another form: Two countries wish to destroy equal number of bombs but no one wants to tell first how many they wish to destroy and say united nation works as semi-honest Charlie.

A PP-type 2-party orthogonal-state-based protocol of QKA

Step 1: Alice prepares $|\psi^{+}\rangle^{\otimes n}$ where $|\psi^{+}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. She uses first qubits of each Bell state to form an ordered sequences $p_A = \{p_A^1, p_A^2, p_A^3 \cdots p_A^n\}$. Similarly, she forms an ordered sequence $q_A = \{q_A^1, q_A^2, q_A^3 \cdots q_A^n\}$ with all the second qubits. Here p_A^i, q_A^i denote the first and second particles of ith copy of the Bell state $|\psi^{+}\rangle$, for 1 ≤ i ≤ n. She also prepares a random sequence $K_A = \{K_A^1, K_A^2, K_A^3, \cdots, K_A^n\}$, where K_A^i denotes the ith bit of sequence K_A and K_A^i is randomly chosen from {0, 1}. K_A may be considered as Alice's key.

Step 2: Alice prepares a sequence of n/2 Bell states $|\psi^{+}\rangle^{\otimes \frac{n}{2}}$ as decoy qubits and concatenates the sequence with q_A to form an extended sequence q'_A . She applies a permutation operator Π_{2n} on q'_A to create a new sequence $\Pi_{2n} q'_A = q''_A$ and sends that to Bob.

Step 3: After receiving the authentic acknowledgment of the receipt of the entire sequence q''_A from Bob, Alice announces the coordinates of the qubits (Π_{2n}) sent by her. Using the information Bob rearranges the qubits and performs Bell measurements on the decoy qubits and computes the error rate. Ideally in absence of Eve all the decoy Bell states are to be found in $|\psi^{+}\rangle$. If the error rate is found to be within the tolerable limit, they continue to the next step, otherwise they discard the protocol and go back to Step 1.

Step 4: Bob drops the decoy qubits to obtain q_A. Now he prepares a new random sequence $K_B = \{K_B^1, K_B^2, K_B^3 \cdots K_B^n\}$ where K_B^i denote the ith bit of sequence K_B, for 1 ≤ i ≤ n and K_B^i is randomly chosen from {0, 1}. K_B may be considered as Bob's key. He applies a unitary operation on each qubit of sequence q_A to encode K_B.
The encoding scheme is as follows: to encode $K_B^i=0$ *and* $K_B^i=1$ he applies I and X respectively on q_A^i. This forms a new sequence q_B. After encoding operation, Bob concatenates q_B with a sequence of n/2 Bell states($|\psi^+\rangle^{\otimes n/2}$) that is prepared as decoy qubits and subsequently applies the permutation operator Π_{2n} to obtain an extended and randomized sequence q'_B which he sends to Alice.
Step 5: After receiving the authenticated acknowledgment of the receipt of the entire sequence q'_B from Alice, Bob announces the position of the decoy qubits (note that he does not disclose the actual order of the message qubits) i.e., $\Pi_n \in \Pi_{2n}$. Alice checks the possibility of eavesdropping by following the same procedure as in Step 3. If the error rate is found to be within the tolerable limit, they continue to the next step, otherwise they discard the protocol and go back to Step 1.
Step 6: Alice publicly announces her key K_A and Bob uses that and his own key (sequence) K_B to form the shared key: $K = K_A \oplus K_B$.

Step 7: Bob announces the actual order of the message qubits $(\Pi_n \in \Pi_{2n})$. and Alice uses that information to obtain q_B. Now she combines p_A and q_B and performs Bell measurements on p_A^i, q_B^i This would reveal K_B as she knows the initial state and the encoding scheme used by Bob.

Step 8: Using K_A and K_B Alice prepares her copy of the shared key i.e.,
$K = K_A \oplus K_B$.

Security against dishonest Alice: Delay measurement technique

To communicate K_B if Alice and Bob use a standard protocol of DSQC or QSDC (say they use PP protocol), then it would be possible for Alice to know Bob's secret key before she announces K_A. In that case she will be able to completely control the shared key by manipulating K_A as per her wish. To circumvent this attack we have modified the protocol in such a way that Bob does not announce the coordinates of the message qubits sent by him till he receives K_A. This strategy introduces a delay in measurement of Alice and this delayed measurement strategy ensures that Alice cannot control the key by knowing K_B prior to her announcement of K_A.

Security against dishonest Bob

Alice announces her key only after receiving the message qubits (without their actual order) from Bob. This ensures that Bob cannot control the key by knowing Alice's key. Only thing that Bob can do after knowing K_A is to change/modify the coordinates of q'_B, but any modification in that would lead to entanglement swapping in our case and that would lead to probabilistic outcomes without any control of Bob.

Turning a protocol of QSDC/DSQC to a protocol of QKA

❑Eavesdropping can be avoided in all protocols of DSQC and QSDC and by randomizing the sequence of key encoded bits sent by Bob (i.e., by delaying the measurement to be performed by Alice) we can circumvent the attacks of dishonest Alice.

❑It is not sufficient to build a protocol of QKA. We also need to avoid the attacks of dishonest Bob.

=>We need to restrict the information available to Bob. Specifically, Bob must not have complete information of the basis that is used to prepare the qubits on which he has encoded his key. In the previous Protocol and in all orthogonal-state-based two-way DSQC/QSDC protocols this can be achieved if Alice keeps some of the qubits of each entangled state with her as that would restrict Bob from changing K_B after receiving K_A. The same can be achieved in a non-orthogonal-state-based protocol by using more than one MUBs. If Alice prepares the state randomly using one of the basis sets and don't disclose the basis set used by her till Bob discloses the sequence then Bob will not have complete access of the basis set used for preparation of the message qubits. As a consequence he will not be able to control the key.

Turning protocols of QD to protocols of QKA

Alice encodes nothing (i.e., she always choose $U_A = I_m$) and keeps $(n - m)$ qubits with herself and sends the remaining m-qubits to Bob who encodes his key by applying an m-qubit unitary operation U_B and sends that back to Alice, but only after changing the order so that Alice cannot measure the final state immediately. Alice announces her key after receiving the key encoded qubits from Bob as in Protocol 1 and subsequently Bob announces the sequence of the message qubits sent by him. In QKA Alice does not need to disclose her measurement outcome. This modified QD protocol is equivalent to our protocol of QKA.

This clearly shows that all protocols of QD with $n > m$ would lead to protocols of QKA.

A multi-party protocol of QKA

In analogy to the previous protocol Alice, Bob and Charlie produce their secret keys:

$$K_B = \{K_B^1, K_B^2, K_B^3 \cdots K_B^n\}$$
$$K_A = \{K_A^1, K_A^2, K_A^3 \cdots K_A^n\}$$
$$K_C = \{K_C^1, K_C^2, K_C^3 \cdots K_C^n\}$$

where K_A^i, K_B^i, K_C^i denote i^th bit of key of Alice, Bob and Charlie respectively and i = 1, 2,... , n. We describe a protocol of multi-party QKA in the following steps.

Step 1: Alice, Bob and Charlie separately prepare $|\psi^+\rangle_A^{\otimes n}, |\psi^+\rangle_B^{\otimes n}$ *and* $|\psi^+\rangle_C^{\otimes n}$ respectively. As in Step 1 of the previous protocol Alice prepares two ordered sequences p_A and q_A i.e., $q_A = \{q_A^1, q_A^2, q_A^3 \cdots q_A^n\}, p_A = \{p_A^1, p_A^2, p_A^3 \cdots p_A^n\}$ composed of all the first and the second qubits of the Bell states that she has prepared. Similarly, Bob and Charlie prepare $p_B = \{p_B^1, p_B^2, p_B^3 \cdots p_B^n\}$, $q_B = \{q_B^1, q_B^2, q_B^3 \cdots q_B^n\}$ *and*, $p_C = \{p_C^1, p_C^2, p_C^3 \cdots p_C^n\}, q_C = \{q_C^1, q_C^2, q_C^3 \cdots q_C^n\}$ from $|\psi^+\rangle_B^{\otimes n}$ *and* $|\psi^+\rangle_C^{\otimes n}$, respectively.

Step 2: Each of Alice, Bob and Charlie separately prepares sequence of n/2 Bell states $(|\psi^+\rangle^{\otimes \frac{n}{2}})_j$ with j ∈ {A, B, C} as decoy qubits and concatenates the sequence with q_j to form extended sequences q'_j. Subsequently user j applies permutation operator $(\Pi_{2n})_j$ on q'_j to create a new sequence $(\Pi_{2n})_j q_j^{/} = q_j^{//}$ and sends that to user j+1. Here we follow a notation in which j ∈ {A, B, C} and A, B,C follows a modulo 3 algebra that gives us the relations: A + 3 = B + 2 = C + 1 = A, A = C + 1, B = A + 1, C = B + 1 and so on.

Step 3: After receiving the authentic acknowledgment of receipt from the receiver (user j+1) corresponding sender (user j) announces the coordinates of the qubits $(\Pi_{2n})_j$ sent by him/her. Each receiver computes error rate as in Step 3 of the previous protocol. If the computed error rates are found to be within the tolerable limit, they continue to the next step, otherwise they discard the protocol and go back to Step 1.

Step 4: After discarding the decoy qubits each user j encodes his/her secret bits by applying the unitary operation on each qubit of the sequence received by him (i.e., on q_{j-1}) in accordance with his/her key K_j. The encoding scheme is as follows: If $K^i{}_j$ = 0 (1) then user j applies I (X) on $q^i{}_{j-1}$. As a result of encoding operations, user j obtains a new sequence r_j . After the encoding operation user j concatenates r_j with a sequence of n/2 Bell states $(|\psi^+\rangle^{\otimes \frac{n}{2}})_j$ that is prepared as decoy qubits and subsequently applies the permutation operator $(\Pi_{2n})_j$ to obtain an extended and randomized sequence r'_j which he/she sends to the user j+1.

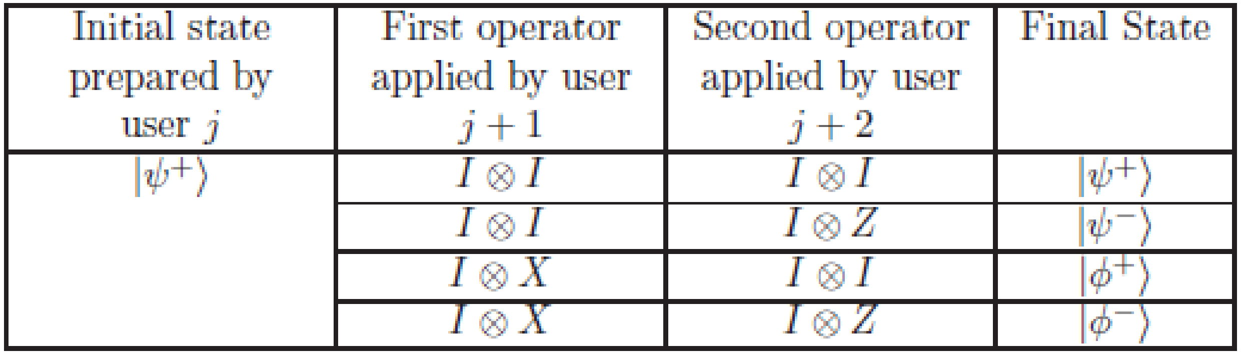
Step 5: After receiving the authentic acknowledgment of the receipt of the sequence r'_j from the receiver j+1, the sender j announces the coordinates of the decoy qubits i.e.,$(\Pi_n)_j \in (\Pi_{2n})_j$. User j+1 uses the information for computing the error rate as before and if it is below the threshold value then they go on to the next step, otherwise they discard the communication. In absence of eavesdropping user j announces the coordinates of the message qubits i.e., $(\Pi_n)_j \in (\Pi_{2n})_j$

Step 6: Same as Step 4 with only difference that if $K^i{}_j = 0$ and $K^i{}_j = 1$ then user j applies I and Z respectively on $r^i{}_{j-1}$. As a result of encoding operations user j obtains a new sequence s_j and after insertion of decoy qubits and applying permutation operator he/she obtains a randomized sequence s'_j which he/she sends to the user j+1.

Step 7: Same as Step 5.

Step 8: After discarding the decoy qubits each user rearranges the sequence received by him/her. Now each user j has two ordered sequences p_j and s_{j-1}. Each of the users j performs Bell measurements on $p^i_j s^i_{j-1}$. According to the output of the Bell measurement and Table 1 each user j can obtain the secret keys of the other two parties. Hence the shared secret key $K = K_A \oplus K_B \oplus K_C$ can be generated.

Table1: Transformation of $|\psi^+\rangle$ based on two operations. Here + refers to modulo 3 operations. j ∈ {A, B, C} where A, B, C stands for Alice, Bob and Charlie, respectively.



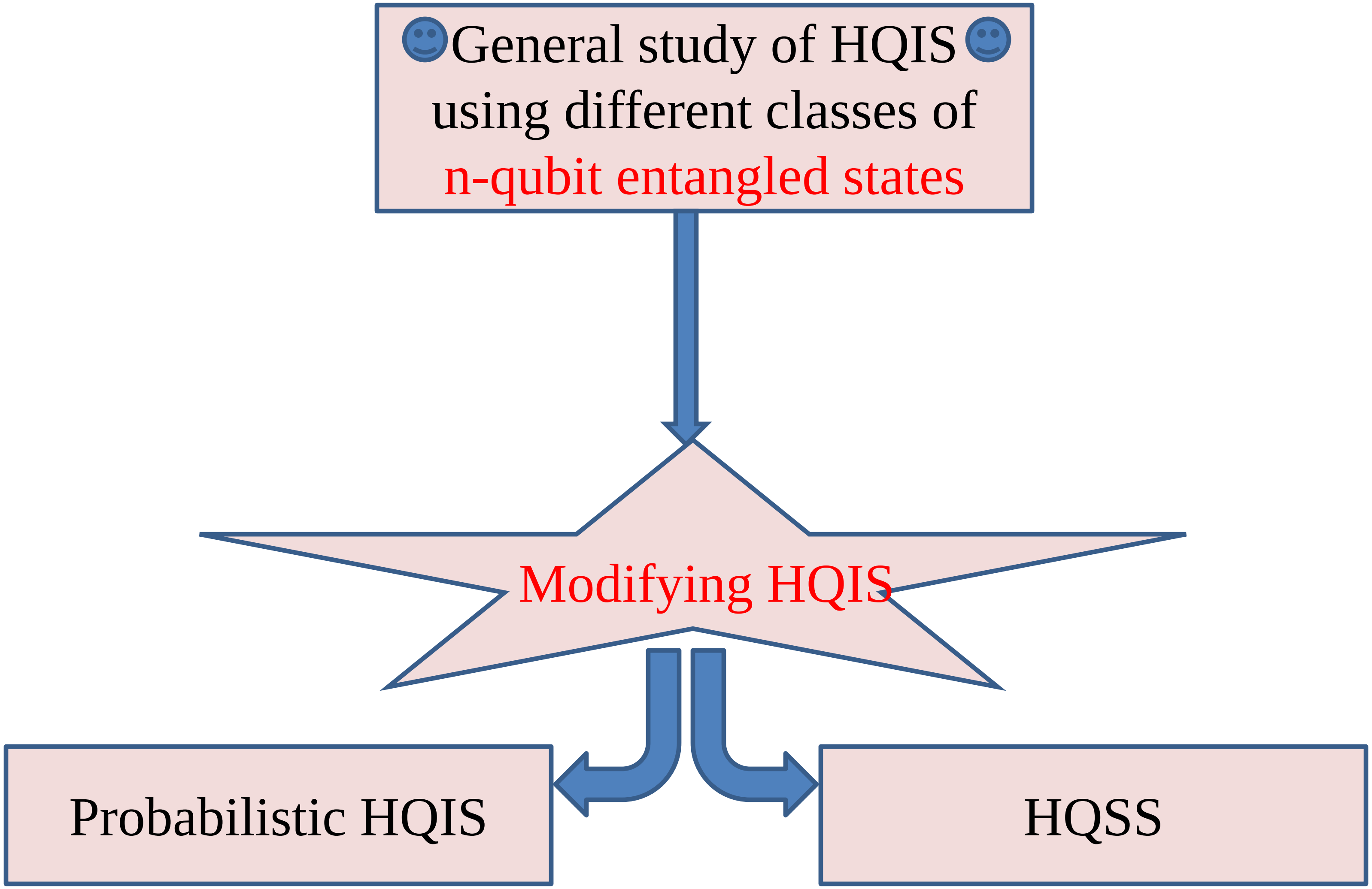
Initial state prepared by user j	First operator applied by user $j+1$	Second operator applied by user $j+2$	Final State
$\vert\psi^+\rangle$	$I \otimes I$	$I \otimes I$	$\vert\psi^+\rangle$
	$I \otimes I$	$I \otimes Z$	$\vert\psi^-\rangle$
	$I \otimes X$	$I \otimes I$	$\vert\phi^+\rangle$
	$I \otimes X$	$I \otimes Z$	$\vert\phi^-\rangle$

Thus A + 2 = C = A − 1 and so on. Further, to denote the Bell states, we have used the following conventions:

$$|\psi^{\pm}\rangle = \frac{(|00\rangle + |11\rangle)}{\sqrt{2}} \; and \; |\phi^{\pm}\rangle = \frac{(|01\rangle + |10\rangle)}{\sqrt{2}}$$

Disjoint Subgroups

Here we note that {I, X, iY, Z} is a modified Pauli group under multiplication and {I, X}, {I, Z} are its disjoint subgroups. Here disjoint subgroups refer to two subgroups g_i and g_j of a group G that satisfy $g_i \cap g_j = \{I\}$, where I is the identity element. Thus except identity element g_i and g_j do not contain any other common element. Now we assume that G is a group of order M under multiplication and elements of G are x-qubit unitary operators. Further, we assume that there exist n mutually disjoint subgroups g_i with i = 1,...,n of the group G such that g_i's are of equal size (say each of the g_i's has 2^y elements) and $\prod_i^{\otimes m} g_i = g_1 \otimes g_2 \otimes g_3 \otimes \ldots\ldots \otimes g_m = U_1, U_2, \ldots\ldots U_{(2y)}{}^m$ where $(2^y)^m \leq M$; $U_i \in G$ and $U_i \neq U_l$ $\forall$ i, l $\in \{1, 2, \cdot \cdot \cdot, (2^y)^m\}$. Now if we have $I^{\otimes(N-x)} U_i | \phi_0 \rangle = | \phi_i \rangle$ and $\langle \phi_i | \phi_l \rangle = \delta_{i,l}$ where $| \phi_i \rangle$ is an N-qubit quantum state with N > x, then we can have an (m + 1)-party version of protocol of QKA.



☺General study of HQIS☺
using different classes of
n-qubit entangled states

Modifying HQIS

Probabilistic HQIS

HQSS

Generalization of HQIS

General (n+1) qubit state of our interest: $|\psi_c\rangle = \frac{1}{\sqrt{2}}[|0\rangle|\psi_0\rangle + |1\rangle|\psi_1\rangle]\cdots(1)$

where $|\psi_0\rangle$ and $|\psi_1\rangle$ are arbitrary n qubit state and are orthogonal to each other. The first qubit of $|\psi_c\rangle$ is with Alice and rest are with n agents.

Alice wishes to teleport (share) among her agents a general one qubit state,

$$|\psi_s\rangle = \frac{1}{\sqrt{1+|\lambda|^2}}(|0\rangle + \lambda|1\rangle), \ \ldots\ (2)$$

which represents an arbitrary qubit. So the combined state is

$$|\psi_s\rangle \otimes |\psi_c\rangle = \frac{1}{\sqrt{1+|\lambda|^2}}(|0\rangle + \lambda|1\rangle) \otimes \frac{1}{\sqrt{2}}[|0\rangle|\psi_0\rangle + |1\rangle|\psi_1\rangle]$$

$$= \frac{1}{\sqrt{2(1+|\lambda|^2)}}[|00\rangle|\psi_0\rangle + |01\rangle|\psi_1\rangle] + \frac{\lambda}{\sqrt{2(1+|\lambda|^2)}}[|10\rangle|\psi_0\rangle + |11\rangle|\psi_1\rangle]$$

$$= \frac{1}{2\sqrt{1+|\lambda|^2}}[|\psi^+\rangle(|\psi_0\rangle + \lambda|\psi_1\rangle) + |\psi^-\rangle(|\psi_0\rangle - \lambda|\psi_1\rangle)$$

$$+|\phi^+\rangle(|\psi_1\rangle + \lambda|\psi_0\rangle) + |\phi^-\rangle(|\psi_1\rangle - \lambda|\psi_0\rangle)]\cdots\cdots\cdots\cdots\cdots(3)$$

If Alice does Bell measurement on the first 2 qubits the states of all the n agents reduces to

$$|\Psi^\pm\rangle = \frac{|\psi_0\rangle \pm \lambda|\psi_1\rangle}{\sqrt{1+|\lambda|^2}} \text{ and} |\Phi^\pm\rangle = \frac{|\psi_1\rangle \pm \lambda|\psi_0\rangle}{\sqrt{1+|\lambda|^2}}$$

4-qubits are required for HQIS and we restrict ourselves to n = 3

Outcome of Alice's measurement	**Combined state of all agents after measurement of Alice**
$\left\|\psi^{+}\right\rangle$	$\left\|\Psi^{+}\right\rangle=\dfrac{\left\|\psi_{0}\right\rangle+\lambda\left\|\psi_{1}\right\rangle}{\sqrt{1+\|\lambda\|^{2}}}$
$\left\|\psi^{-}\right\rangle$	$\left\|\Psi^{-}\right\rangle=\dfrac{\left\|\psi_{0}\right\rangle-\lambda\left\|\psi_{1}\right\rangle}{\sqrt{1+\|\lambda\|^{2}}}$
$\left\|\phi^{+}\right\rangle$	$\left\|\Phi^{+}\right\rangle=\dfrac{\left\|\psi_{1}\right\rangle+\lambda\left\|\psi_{0}\right\rangle}{\sqrt{1+\|\lambda\|^{2}}}$
$\left\|\phi^{-}\right\rangle$	$\left\|\Phi^{-}\right\rangle=\dfrac{\left\|\psi_{1}\right\rangle-\lambda\left\|\psi_{0}\right\rangle}{\sqrt{1+\|\lambda\|^{2}}}$

Table 2

Relation between outcomes of Bell measurement performed by Alice and the combined state of the agents, which is true in general. **This provides us the framework to investigate the possibilities of HQIS in different quantum states**.

Examples of 4-qubit states

Case I: $|\psi_c\rangle$ is 4-qubit Omega state ($|\Omega\rangle$) :

Alice has chosen 4-qubit $|\Omega\rangle$ state as channel and kept the first qubit with her and has sent the second, third and fourth qubits to Bob, Charlie and Diana respectively.

In that case

$$|\psi_c\rangle = |\Omega\rangle_{ABCD} = \frac{1}{2}[|0000\rangle + |0110\rangle + |1001\rangle - |1111\rangle]_{ABCD}$$

$$= \frac{1}{\sqrt{2}}[|0\rangle_A |\psi_0\rangle_{BCD} + |1\rangle_A |\psi_1\rangle_{BCD}] \cdots\cdots\cdots\cdots\cdots\cdots (channel)$$

where $|\psi_0\rangle_{BCD} = \frac{1}{\sqrt{2}}[|000\rangle + |110\rangle]$ and $|\psi_1\rangle_{BCD} = \frac{1}{\sqrt{2}}[|001\rangle - |111\rangle]$.

Now after Alice's Bell measurement on the first two qubits, the combined state of Bob, Charlie and Diana collapses according to Table 1. If Alice's measurement outcome is $|\psi^{\pm}\rangle$ then the state of the agents is

$$|\Psi^{\pm}\rangle_{BCD} = \frac{1}{\sqrt{1+|\lambda|^2}}[|\psi_0\rangle_{BCD} \pm \lambda |\psi_1\rangle_{BCD}]$$

$$= \frac{1}{\sqrt{2(1+|\lambda|^2)}}[|000\rangle + |110\rangle \pm \lambda(|001\rangle - |111\rangle)]_{BCD} \cdots\cdots\cdots\cdots\cdots\cdots (4)$$

Similarly, if Alice obtains $|\phi^{\pm}\rangle$ then the state of the agents is

$$|\Phi^{\pm}\rangle_{BCD} = \frac{1}{\sqrt{1+|\lambda|^2}}[|\psi_1\rangle_{BCD} \pm \lambda |\psi_0\rangle_{BCD}]$$

$$= \frac{1}{\sqrt{2(1+|\lambda|^2)}}[|001\rangle - |111\rangle \pm \lambda(|000\rangle + |110\rangle)]_{BCD} \cdots\cdots\cdots\cdots\cdots\cdots (5)$$

Now **if the agents decide that Diana will reconstruct** the secrets, then we can decompose (4) and (5) as

$$|\Psi^{\pm}\rangle_{BCD} = \frac{1}{\sqrt{2(1+|\lambda|^{2})}}[|00\rangle_{BC}(|0_{D}\rangle \pm \lambda|1_{D}\rangle) + |11\rangle_{BC}(|0_{D}\rangle \mp \lambda|1_{D}\rangle)] \cdots (6)$$

$$|\Phi^{\pm}\rangle_{BCD} = \frac{1}{\sqrt{2(1+|\lambda|^{2})}}[|00\rangle_{BC}(|1_{D}\rangle \pm \lambda|0_{D}\rangle) - |11\rangle_{BC}(|1_{D}\rangle \mp \lambda|0_{D}\rangle)] \cdots (7)$$

Now from (6) and (7) it is clear that if Bob and Charlie measure their qubits in computational basis and only one of them sends the result to Diana then Diana will be able to reconstruct the state sent by Alice using appropriate unitary operators as shown in Table 3.

The more information is known, less collaboration is needed.

Alice measurement outcome	Joint measurement outcome of Bob and Charlie	Diana's operation
$\|\psi^{+}\rangle$	$\|00\rangle_{BC}$	I
$\|\psi^{+}\rangle$	$\|11\rangle_{BC}$	Z
$\|\psi^{-}\rangle$	$\|00\rangle_{BC}$	Z
$\|\psi^{-}\rangle$	$\|11\rangle_{BC}$	I
$\|\phi^{+}\rangle$	$\|00\rangle_{BC}$	X
$\|\phi^{+}\rangle$	$\|11\rangle_{BC}$	XZ
$\|\phi^{-}\rangle$	$\|00\rangle_{BC}$	XZ
$\|\phi^{-}\rangle$	$\|11\rangle_{BC}$	X

Table 3
Relation among the measurement outcomes of Alice, Bob and Charlie and the unitary operations to be applied by Diana when the initial state is an omega state and Diana reconstructs the unknown state. **Here the measurement outcomes of Bob and Charlie are always same.** So the communication from one of them and Alice would be sufficient for Diana to reconstruct the unknown state sent by Alice.

If Bob reconstructs the state sent by Alice.

We can decompose (4) and (5) as:

$$|\Psi^{\pm}\rangle_{BCD} = \frac{1}{2\sqrt{1+|\lambda|^2}}[(|0_B\rangle \mp \lambda|1_B\rangle)|\psi^+\rangle_{CD} + (|0_B\rangle \pm \lambda|1_B\rangle)|\psi^-\rangle_{CD} + (|1_B\rangle \pm \lambda|0_B\rangle)|\phi^+\rangle_{CD} - (|1_B\rangle \mp \lambda|0_B\rangle)|\phi^-\rangle_{CD}]\cdots(8)$$

$$|\Phi^{\pm}\rangle_{BCD} = \frac{1}{2\sqrt{1+|\lambda|^2}}[(|0_B\rangle \pm \lambda|1_B\rangle)|\phi^+\rangle_{CD} + (|0_B\rangle \mp \lambda|1_B\rangle)|\phi^-\rangle_{CD} - (|1_B\rangle \mp \lambda|0_B\rangle)|\psi^+\rangle_{CD} + (|1_B\rangle \pm \lambda|0_B\rangle)|\psi^-\rangle_{CD}]\cdots(9)$$

The state with Bob in (8) can be considered as quantum encrypted with classical data of 2 bits in the joint possession of Charlie and Diana, which is seen manifestly as follows:

$$|\Psi^{+}\rangle_{BCD} = \frac{1}{2}[(Z|\psi_S\rangle)_B|\psi^+\rangle_{CD} + (I|\psi_S\rangle)_B|\psi^-\rangle_{CD} + (X|\psi_S\rangle)_B|\phi^+\rangle_{CD} - (iY|\psi_S\rangle)_B|\phi^-\rangle_{CD}]\cdots(10)$$

Without access to knowledge of the state with Charlie and Diana, Bob's state is given by the reduced density operator:

$$\rho_B = \frac{1}{4}(I|\psi_S\rangle\langle\psi_S|I + Z|\psi_S\rangle\langle\psi_S|Z + X|\psi_S\rangle\langle\psi_S|X + iY|\psi_S\rangle\langle\psi_S|iY) = \frac{I}{2}\cdots(11)$$

implying that Bob gains no information without the cooperation of Charlie and Diana. Analogous observations hold for the state $|\Psi^-\rangle$ in (8) and states $|\Phi^{\pm}\rangle$ in (9).

If Alice inserts some decoy qubits and applies PoP before sending a sequence of qubits to a user, they will be able to circumvent eavesdropping and the protocol of HQIS will become a protocol of HQSS.

Alice measurement outcome	Joint measurement outcome of Charlie and Diana	Bob’s operation
$\vert\psi^{+}\rangle$	$\vert\psi^{+}\rangle_{CD}$ $\vert\psi^{-}\rangle_{CD}$	Z (I)
$\vert\psi^{+}\rangle$	$\vert\phi^{+}\rangle_{CD}$ $\vert\phi^{-}\rangle_{CD}$	X (XZ)
$\vert\psi^{-}\rangle$	$\vert\psi^{+}\rangle_{CD}$ $\vert\psi^{-}\rangle_{CD}$	I (Z)
$\vert\psi^{-}\rangle$	$\vert\phi^{+}\rangle_{CD}$ $\vert\phi^{-}\rangle_{CD}$	XZ (X)
$\vert\phi^{+}\rangle$	$\vert\phi^{+}\rangle_{CD}$ $\vert\phi^{-}\rangle_{CD}$	I (Z)
$\vert\phi^{+}\rangle$	$\vert\psi^{+}\rangle_{CD}$ $\vert\psi^{-}\rangle_{CD}$	XZ (X)
$\vert\phi^{-}\rangle$	$\vert\phi^{+}\rangle_{CD}$ $\vert\phi^{-}\rangle_{CD}$	Z (I)
$\vert\phi^{-}\rangle$	$\vert\psi^{+}\rangle_{CD}$ $\vert\psi^{-}\rangle_{CD}$	X (XZ)

Table 4
Relation among the measurement outcomes of Alice, Charlie and Diana and the unitary operations to be applied by Bob when the initial state is an omega state and Bob reconstructs the unknown state. Here Charlie and Diana need to do a joint measurement and consequently Bob requires assistance of both of them and Alice to reconstruct the unknown state sent by Alice.

Bob can recover the arbitrary state $|\psi_S\rangle$ if Charlie and Diana make a joint measurement (a nonlocal operation) by applying the appropriate unitary operators shown in Table 4, this requires assistance of Charlie, Diana and Alice.

Thus, Bob requires more information than required by Diana (more powerful than Bob) to reconstruct. Hence Bob (Charlie) and Diana have different powers to recover the arbitrary state. This makes the scheme hierarchical.

Case II: $|\psi_c\rangle$ is 4-qubit cluster state $(|C_4\rangle)$:

If Alice has chosen 4-qubit cluster state $(|C_4\rangle)$ as channel

$$|\psi_c\rangle = |C_4\rangle_{ABCD} = \frac{1}{2}[|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle]_{ABCD}$$

$$= \frac{1}{\sqrt{2}}[|0\rangle_A|\psi_0\rangle_{BCD} + |1\rangle_A|\psi_1\rangle_{BCD}]......(channel)$$

$$where\ |\psi_0\rangle_{BCD} = \frac{1}{\sqrt{2}}[|000\rangle + |011\rangle]$$

$$and\ |\psi_1\rangle_{BCD} = \frac{1}{\sqrt{2}}[|100\rangle - |111\rangle].$$

Now after Alice's Bell measurement the combined state of the agents collapse according to (12) and (13);

$$|\Psi^{\pm}\rangle_{BCD} = \frac{1}{\sqrt{1+|\lambda|^2}}[|\psi_0\rangle_{BCD} \pm \lambda|\psi_1\rangle_{BCD}]$$

$$= \frac{1}{\sqrt{2(1+|\lambda|^2)}}[|000\rangle + |011\rangle \pm \lambda(|100\rangle - |111\rangle)]_{BCD} \cdots\cdots\cdots\cdots\cdots\cdots(12)$$

$$|\Phi^{\pm}\rangle_{BCD} = \frac{1}{\sqrt{1+|\lambda|^2}}[|\psi_1\rangle_{BCD} \pm \lambda|\psi_0\rangle_{BCD}]$$

$$= \frac{1}{\sqrt{2(1+|\lambda|^2)}}[|100\rangle - |111\rangle \pm \lambda(|000\rangle + |011\rangle)]_{BCD} \cdots\cdots\cdots\cdots\cdots\cdots(13)$$

Cleary from (4), (5), (12) and (13) we can easily observe the following symmetry:

$$|\Psi^{\pm}\rangle_{BCD}\big|_{|\psi_c\rangle=|\Omega\rangle} \equiv |\Psi^{\pm}\rangle_{DCB}\big|_{|\psi_c\rangle=|C_4\rangle}, \qquad |\Phi^{\pm}\rangle_{BCD}\big|_{|\psi_c\rangle=|\Omega\rangle} \equiv |\Phi^{\pm}\rangle_{DCB}\big|_{|\psi_c\rangle=|C_4\rangle}.$$

Thus after the measurement of Alice the combined states of the agents in this case [i.e., when $|\psi_c\rangle = |C_4\rangle$] is equivalent to that in the previous case [i.e., when $|\psi_c\rangle = |\Omega\rangle$]. The only difference is that the role of Diana and Bob are now reversed. Consequently, we obtain a HQIS scheme with $|\psi_c\rangle = |C_4\rangle_{ABCD}$. However, here Bob is more powerful than Charlie and Diana.

HQSS=HQIS+QKD

Hierarchical quantum state sharing (HQSS):

Suppose, Alice is boss of a company and Bob, Charlie and Diana are her agents. Alice trusts Diana more than the other two agents as he is the oldest employ. Thus there is a hierarchy among the agents. In this situation, **Alice may use HQIS scheme with 4-qubit** $(|\Omega\rangle)$ **as described in case-I and send the information in three pieces** so that none of Bob, Charlie and Diana can read the message of Alice without the help of the other. However, Diana would require lesser help than Bob.

Possibilities of eavesdropping. **For example**, consider that Bob is dishonest and he captures the qubit sent to Charlie and Diana, too. If Bob does a Bell measurement on Charlie's and Diana's qubit then using the unitary operations described in Table 3, he will be able to get the entire information without any help of Charlie and Diana. So **Alice needs to add some error checking schemes** for security purpose to the above proposed HQIS scheme.

Security

If Alice adopts **the insertion of decoy qubits and rearrangement of the order of particles technique** then HQIS will become HQSS.

There may be many kind of attacks. An external Eve may attack the protocol or a dishonest party (say Bob, Charlie or Diana) may capture the qubits of the others and obtain the entire information without the help of others. Such attacks are prevented by **above strategy** adopted by Alice. If the eavesdropping is finally checked by the BB84 subroutine, security of the protocol would be equivalent to that of BB84 protocol.

Our recent papers related to the present talk

1. Shukla C., and **Pathak. A**, “On the group-theoretic structure of a class of quantum dialogue protocols”. *Physics Letters A*, 377, pp. 518-527, 2013.
2. Banerjee, A., and **Pathak, A.,** “Maximally efficient protocols for direct secure quantum communication”. *Physics Letters A*, Vol. 376, pp. 2944–2950, 2012.
3. Srinatha, N., Omkar, S., Srikanth, R., Banerjee, S., and **Pathak, A**. “The quantum cryptographic switch”. *Quantum Information Processing*, **13,** pp 59-70, 2014.
4. Shukla, C., Banerjee, A., and **Pathak, A**. ”Improved protocols of secure quantum communication using W states”. *International Journal of Theoretical Physics*, **52** , pp. 1914-1924, 2013.
5. Shukla, C., **Pathak, A.,** and Srikanth, R., “Beyond the Goldenberg-Vaidman protocol: Secure and efficient quantum communication using arbitrary, orthogonal, multi-particle quantum states”. *International Journal of Quantum Information,* **10** (2012) 1241009..
6. Yadav, P. , Srikanth, R., and **Pathak, A**. “Generalization of the Goldenberg-Vaidman QKD Protocol”, arXiv:1209:4304.
7. Banerjee, A., and **Pathak, A., “**Bidirectional controlled teleportation by using 5-Qubit states: A generalized view”, C. Shukla,, Int. J. Theor. Phys, **52** (2013) 3790-3796.
8. Shukla, C., and **Pathak, A. “**Hierarchical quantum communication”, Phys. Lett. A **377** (2013) 1337-1344.
9. Shukla, C., Nasir A., and **Pathak., A**., "Orthogonal-state-based protocols of quantum key agreement." *arXiv:1310.1435*.

Book: Anirban Pathak, Elements of Quantum Computation and Quantum Communication, CRC Press, May, 2013. All the cartoons are from the book.

TO CLOSE AC.
TO OPEN AC.
TO CLOSE AC.
TO OPEN AC.
CLASSICAL BANK
50 YEARS OF SAFE ONLINE BANKING
QUANTUM BANK
SECURE YOUR MONEY WITH QUANTUM KEYS
WHAT HAPPENED?
YESTERDAY, A SCALABLE QUANTUM COMPUTER IS LAUNCHED SO RSA IS NO MORE SAFE!!

Thank you