Presentation made for QIPA 2013

Harish Chandra Research Institute

Retrieving and Routing Quantum Information in a Quantum Network

Dr. Indranil Chakrabarty

International Institute of Information Technology, Hyderabad

December, 2013

Anyone who is not shocked by quantum theory has not understood it— Neils Bohr.

Authors and Affiliations

- **S Sazim** : Institute of Physics, Sainik School Post, Bhubaneswar-751005, Orissa, India.
- **V. Chiranjeevi, I Chakrabarty, K. Srinathan**: Centre for Security Theory Algorithimic Research, International Institute of Information Technology, Gachibowli, Hyderabad 500 032, Andhra Pradesh, India.

Outline of the Talk

- Background of Quantum Secret Sharing
- Motivation and Implications
- Description of the Work
- Concluding Remarks and Future Directions

Background of Quantum Secret Sharing

- In a secret sharing protocol the sender/dealer of the secret message, who is unaware of the individual honesty of the receivers, shares the secret in such a way that none of the receivers get any information about the secret. By Quantum Secret Sharing we refer to a situation where the dealer can share both quantum as well as classical secrets inform of qubits and cibits but only with a quantum resource [Hillary, Cleve].
- A typical protocol for quantum secret sharing, like many other tasks in quantum cryptography, uses entanglement as a cardinal resource, mostly pure entangled states. Many researchers studied quantum secret sharing protocols using bipartite pure entangled states as resources [Karlsson]. They have investigated the concept of quantum secret sharing using tripartite pure entangled states and multi partite states like graph states [Bandyopadhyay, Bagherinezhad, Lance, Gordon, Zheng, Markham, Markham]. It was proposed semi-quantum secret sharing protocols taking maximally entangled GHZ state as resource [Li].
- In a realistic situation, the secret sharing of classical or quantum information involves transmission of qubits through noisy channels that entails mixed states. Subsequently in [Adhikari, Chakrabarty, Agrawal] authors propose a protocol for secret sharing of classical information with three qubit mixed state. Quantum secret sharing has also been realized in experiments [Tittel, Schmid, Bogdanski].

Motivation and Implications

Motivation: Why we are interested in this problem?

- **Revocation of Secrets :**
  What is there ? In extant quantum secret sharing protocols, once the secret is shared in a quantum network (QNET) it can not be retrieved back, even if the dealer wishes that her secret no longer be available in the network. For instance, if the dealer is part of two QNETs, say $\mathcal{Q}_1$ and $\mathcal{Q}_2$ and she subsequently finds that $\mathcal{Q}_2$ is more reliable than $\mathcal{Q}_1$, the dealer may wish to transfer all her secrets from $\mathcal{Q}_1$ to $\mathcal{Q}_2$. Known protocols are inadequate to address such a revocation.

Motivation and Implications

Why Revocation is important?

- Alice decides to change the secret
- Alice conjectures that reciepents are no longer trustworthy.
- There is an update of secret in higher level application using secret sharing as a subroutine.
- Alice has found more economical alternative QNET to safeguard the secret.

Motivation and Implications

- **Routing of Secrets:**
  One interesting implication of our technique is the possibility of *routing* qubits in **asynchronous** QNETS.
  By asynchrony we mean that the requisite data/resources are intermittently available (but not necessarily simultaneously) in the QNET.
  Some Classical Examples (Asynchronous Network): 1) Postal Mail, 2) Email 3) A bulletin board system, or BBS, is a computer system running software that allows users to connect and log into the system using a terminal program. Once logged in, a user can perform functions such as uploading and downloading software and data, reading news and bulletins, and exchanging messages with other users, either through email, public message boards, and sometimes via direct chatting.
  Some Classical Examples (Synchronous Network): 1) Electricity flow

Motivation and Implications

Why it is important? source A can send quantum information to a destination R even though

- A and R share no direct quantum resource
- R's identity is *unknown* to A at the time of sending the message, but is subsequently decided
- A herself can be R at a later date and/or in a different location to bequeath her information ('backed-up' in the QNET)
- Importantly, the path chosen for routing the secret may hit a dead-end due to resource constraints, congestion etc. (therefore the information needs to be *back-tracked* and sent along an alternate path)
- Another implication of our technique is the possibility of using *insecure* resources. For instance, if the quantum memory within an organization is insufficient, it may safely store (using our protocol) its private information with a neighboring organization without (a) revealing critical data to the host and (b) losing control over retrieving the data.

Putting the two implications together, namely routing and secure storage, it is possible to envision applications like **QUANTUM MAIL (QMAIL)** as an outsourced service. An important consequence of both revoking and routing is that critical and private information can be q-mailed across **public QNETS** by secret sharing and then routing.
Public QNETS: Here we assume that the agents in the network are semi honest, i.e at least they run the protocol as instructed but will always be interested in getting hold of the secret. However if the agents are all malacious and have the freedom that they are allowed to do whatever they wish to do then perhaps no protocol will exists as one can simply shut down the machine and run away

Motivations and Implications

Important Consideration

In our model we consider the receivers to be semi-honest – that is the receivers, though dishonest to eavesdrop on their share and process it, diligently participate in the protocol. On the other hand, note that malicious receivers can easily destroy the secret, making revocation impossible.

Description of the Work

Sharing of a Message First of all, we consider a simple situation where we have three parties Alice, Bob and Charlie. They share a three qubit maximally entangled GHZ state, i.e., $|GHZ\rangle_{ABC} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$. Here the first qubit is with Alice, second is with Bob and the third one is with Charlie. Here Alice is the dealer and she wishes to secret-share a qubit $|S\rangle = \alpha|0\rangle + \beta|1\rangle$ (where $|\alpha|^2 + |\beta|^2 = 1$; α, β are amplitudes) with both the parties Bob and Charlie. In order to do so Alice has to do two-qubit measurements in Bell basis $\{|\phi_\pm\rangle, |\psi_\pm\rangle\}$ jointly on her resource qubit and the message qubit she wants to share . In correspondence to various measurement outcomes obtained by Alice, Bob and Charlie's qubits collapse into the states given in TABLE I.

Description of the Work

Table: **Sharing of Quantum Information**

Alice's Measurement Outcomes	Bob and Charlie's Combined State
$\|\phi^+\rangle$	$\alpha\|00\rangle + \beta\|11\rangle$
$\|\phi^-\rangle$	$\alpha\|\|00\rangle - \beta\|11\rangle$
$\|\psi^+\rangle$	$\alpha\|11\rangle + \beta\|00\rangle$
$\|\psi^-\rangle$	$\alpha\|11\rangle - \beta\|00\rangle$

Description of the Work

At this point if Alice finds both Bob and Charlie to be dishonest, she can stop them from accessing the message. She does this by not communicating about her measurement results to any one of them. So there is no transfer of classical bits at this stage. At this point there lies the question of security from Bob and Charlie sides. If we have malicious (parties who are not going to follow the protocol and do whatever they wish to do) Bob and Charlie can destroy the message by doing local operations in their respective qubits and by communicating classically between them. However, they will never be successful in obtaining the message without Alice's help.

Description of the Work

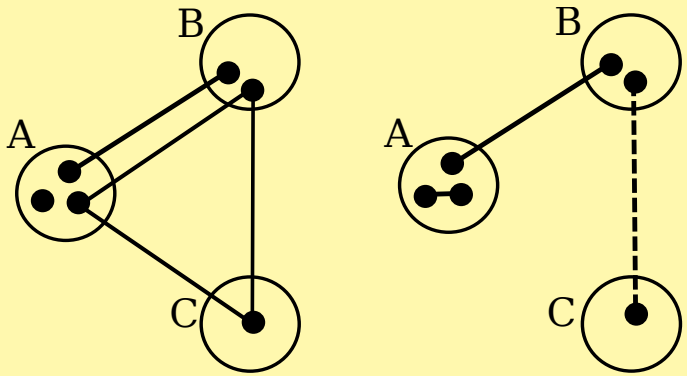

Figure: The figure on the left side indicates a three qubit GHZ state (depicted by a triangle) shared among Alice(A), Bob(B) and Charlie(C) and a two qubit Bell state shared between and Alice(A) and Bob(B). Alice is also having the secret (depicted by an isolated dot) with herself. The figure on the right describes the situation after Alice's measurement, where both Bob and Charlie are sharing the secret between them (the dotted line).

Description of the Work

Revocation of Quantum Information To make the revocation possible Alice needs an additional resource (a Bell state) shared with Bob. Consider a very simple case when Alice and Bob are sharing the Bell state $|Bell\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ in addition to the GHZ state shared by Alice, Bob and Charlie. Let us also assume the first case in the above TABLE I, when Bob and Charlie share the entangled state $\alpha|00\rangle + \beta|11\rangle$ as a result of Alice's measurement. Now Alice asks Bob to do Bell measurement on his qubit and Charlie to do measurement in Hadamard basis (see FIG. 1). In TABLE II we show how Alice can retrieve back her message by enlisting down the respective local operations corresponding to Bob's and Charlie's measurement outcomes.

Description of the Work

Table: **Retrieving Quantum Information**

Bob's Outcomes	Charlie's Outcomes	Alice's Local Operations
$\|\phi^+\rangle$	$\|+\rangle$	I
$\|\phi^+\rangle$	$\|-\rangle$	σ_z
$\|\phi^-\rangle$	$\|+\rangle$	σ_z
$\|\phi^-\rangle$	$\|-\rangle$	I
$\|\psi^+\rangle$	$\|+\rangle$	I
$\|\psi^+\rangle$	$\|-\rangle$	σ_z
$\|\psi^-\rangle$	$\|+\rangle$	σ_z
$\|\psi^-\rangle$	$\|-\rangle$	I

Description of the Work

Quantum Routing in shared domain If Alice has shared her secret qubit $|S\rangle$ in some part of a (huge) QNET, we ask *can she/anyone else retrieve* $|S\rangle$ *at some other part of the network* ? A naive way-out is to reconstruct $|S\rangle$ and teleport it. However, this compromises the security of $|S\rangle$ and may not be economical. A superior approach is to retain $|S\rangle$ in the shared domain while the shares are being routed across the QNET. However, since the shares are themselves entangled and distributed across multiple parties, it is non-trivial to teleport them over the QNET.

Description of the Work

We address the problem in two parts.

- First, we show its possible for Alice to dynamically choose the receiver (of her secret), *after* the sharing phase.
- Second, we show that quantum information can be transmitted in the shared domain; that is, the information secret shared among a set of nodes is transferred to another set of nodes. Putting the two together, Alice can now move her shared secret close to the desired receiver in the QNET and also remotely control the reconstruction of the secret at the receiver.

Description of the Work

Consider a situation where we have $(3 + n)$ parties. Here Alice is the sender, both Charlie and Bob act as agents, the remaining n parties are the potential receivers. Alice desires to send the message in form of a qubit to any one of them. Here the role of Bob and Charlie are changed as they are no longer receivers of information but they now act as agents for holding the information in the network. In broader sense they together act like a router and play a vital role in sending the information to the desired receiver.

Description of the Work

Once again we start with Alice, Bob and Charlie sharing a three qubit maximally entangled GHZ state, i.e., $|GHZ\rangle_{ABC} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ and Charlie shares Bell's states, i.e, $|Bell\rangle_{CR_i} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ with each of the receivers (R_i). Suppose Alice wishes to send a qubit $|S\rangle = \alpha|0\rangle + \beta|1\rangle$ to R_i through the parties Bob and Charlie. First Alice shares her secret with Bob and Charlie in the same way as it is shown in the (TABLE 1). At this point, Alice sends her measurement outcomes encoded in the form of two classical bits to R_i. Once the two bits of classical information are obtained, the receiver can easily get back the Alice's secret S, provided Bob and Charlie perform the actions as described next. We assume that the identity of the receiver is authentically known to Alice, Bob and Charlie, perhaps through a classically secure authentication/identification protocol.

Description of the Work

The agents Bob and Charlie do the following:

- Bob measures his qubit (part of the GHZ state) in the Hadamard basis.
- Charlie measures two qubits (one from GHZ state and one from Bell state shared with R_i) in the Bell basis.
- After performing these measurements both the agents will send their outcomes through classical channels to the receiver R_i. With these measurement outcomes the receiver can retrieve the message which Alice intended to send (see Fig(9)).

Let us consider the case, when Alice and Bob share the entangled state $\alpha|00\rangle + \beta|11\rangle$, obtained as a result of Alice's measurement. TABLE III gives an elaborate view of the unitary operations the receiver R_i has to do upon getting various measurement outcomes from Bob and Charlie.

Description of the Work

Table: **Sending Quantum Information**

Charlie's Outcome	Bob's Outcome	Unitary operations of R_i
$\|\phi^+\rangle$	$\|+\rangle$	I
$\|\phi^-\rangle$	$\|+\rangle$	σ_z
$\|\phi^+\rangle$	$\|-\rangle$	σ_z
$\|\phi^-\rangle$	$\|-\rangle$	I
$\|\psi^+\rangle$	$\|+\rangle$	σ_x
$\|\psi^-\rangle$	$\|+\rangle$	$\sigma_z\sigma_x$
$\|\psi^+\rangle$	$\|-\rangle$	$\sigma_z\sigma_x$
$\|\psi^-\rangle$	$\|-\rangle$	σ_x

Description of the Work

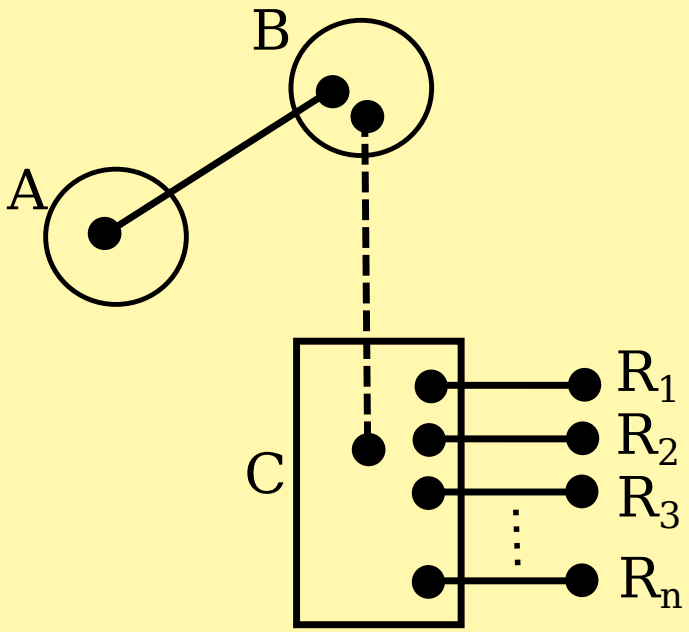

Figure: Any one of the n receivers $\{R_1, R_2, R_3, \ldots, R_n\}$ which individually share Bell states with Charlie can reconstruct the secret. On his request, an authentically identified R_i will get the encoded outcomes from Alice and Charlie, to be able to reconstruct the secret.

Description of the Work

Finally, we address the problem of transferring secret qubits in the shared domain till it comes close to the desired receiver. If we have a source (S) and receivers $R_1, R_2, \ldots, R_n$ and we want to send the information to the receiver R_i through a huge network with pair of agents $(A_1, B_1), (A_2, B_2), \ldots, (A_n, B_n)$ at each blocks. So every pair shares Bell state with consecutive pair say A_i with A_{i+1} and B_i with B_{i+1}. The above setting is depicted in FIG. 3. Once the source shares the information with i^{th} pair the information can be transferred to $(i+1)^{th}$ pair by the process of entanglement swapping in the following way. A_i performs the Bell measurement on two qubits one from the shared secret and other from the Bell state shared with A_{i+1}, similarly B_i performs the Bell measurement on two qubits one from the shared secret and other from the Bell state shared with B_{i+1}. This sequence of measurements goes on till the closest pair gets the Shared secret. The classical outcomes of each measurement are sent to Alice immediately after the measurement to keep track of the state of the shared secret. The receivers can stay in the network in between each pairs. The source is not going to send the classical information until the information reaches the pair close to the desired receiver is reached. Thus, in a QNET we can share, retrieve, hold and as well as transfer the quantum information.

Description of the Work

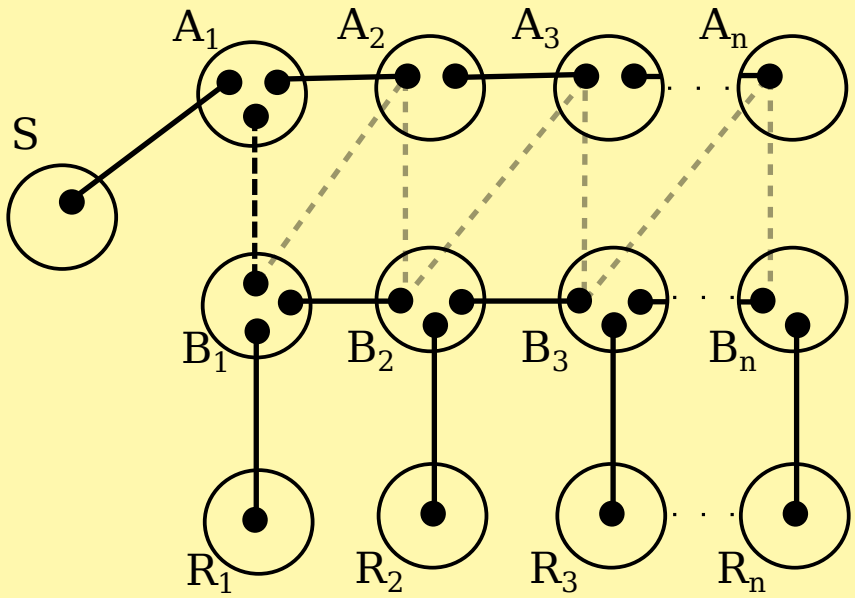

Figure: A typical quantum mail sending network where S is the source, (A_i, B_i) are the agents and R_i are the receivers. Initially, the information is shared between the pairs (A_1, B_1) (the dotted line) and will be transferred to other pairs until the pair close to the desired reciever is reached. The information is moved along $(A_1, B_1), (B_1, A_2), (A_2, B_2), (B_2, A_3)$ and so on till (A_n, B_n) as shown with grey dotted lines.

Description of the Work

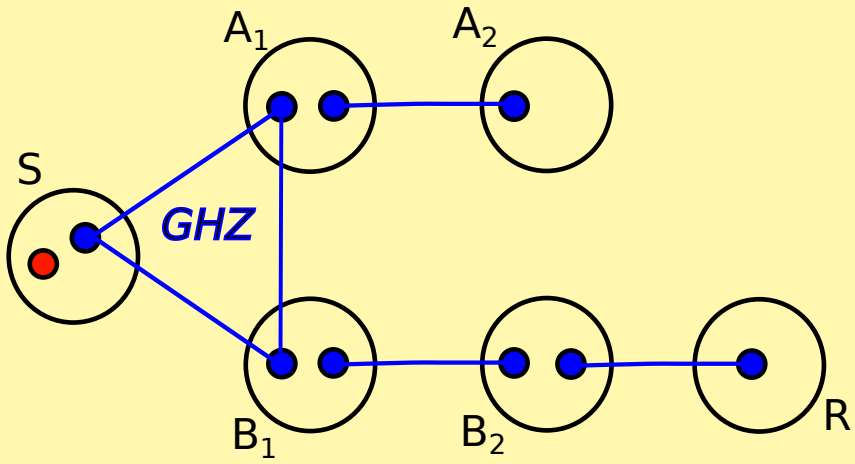

Figure: Suppose S is the source having the secret. A_1, B_1, A_2, B_2 are the agents and R is the receiver. (S, A_1, B_1) share a GHZ state. The pairs (A_1, B_1), (A_2, B_2) and (B_2, R) also share a Bell state each.

Description of the Work

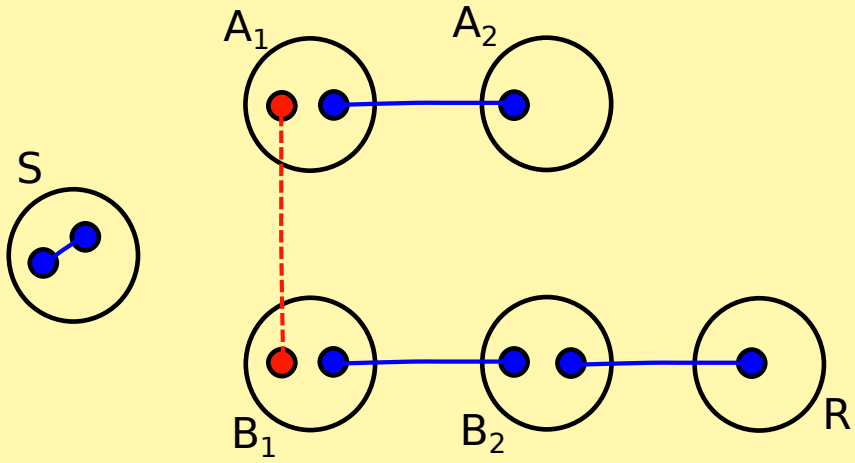

Figure: Secret is shared between A_1 and B_1 as a result of Bell measurement at S. Outcome of the measurement will be sent to S in classical channel.

$$|\psi\rangle \otimes \frac{1}{\sqrt{2}}\{|000\rangle + |111\rangle\}$$
$$= \frac{1}{2}\{|\phi^+\rangle[\alpha|00\rangle + \beta|11\rangle] + |\phi^-\rangle[\alpha|00\rangle - \beta|11\rangle] +$$
$$|\psi^+\rangle[\alpha|11\rangle + \beta|00\rangle] + |\psi^-\rangle[\alpha|11\rangle - \beta|00\rangle]\} \quad (1)$$

Description of the Work

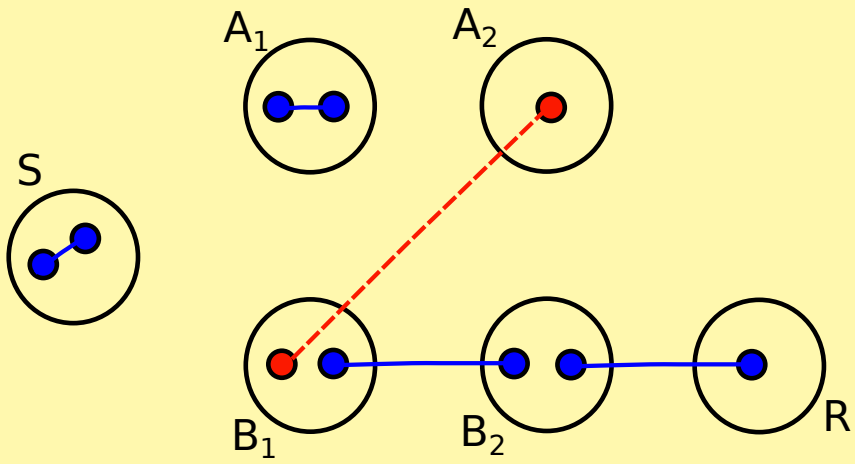

Figure: Secret is shared between B_1 and A_2 as a result of Bell measurement at A_1. Outcome of the measurement will be sent to S in classical channel.

$$\{\alpha|00\rangle + \beta|11\rangle\}_{A_{1s}B_{1s}} \otimes \frac{1}{\sqrt{2}}\{|00\rangle + |11\rangle\}_{A_{1r}A_{2r}}$$
$$= \frac{1}{2}\{|\phi^+\rangle[\alpha|00\rangle + \beta|11\rangle]$$
$$+|\phi^-\rangle[\alpha|00\rangle - \beta|11\rangle]$$
$$+|\psi^+\rangle[\alpha|01\rangle + \beta|10\rangle] + |\psi^-\rangle[\alpha|01\rangle - \beta|10\rangle]\}_{A_{1s}A_{1r}B_{1s}A_{2r}} \quad (2)$$

Description of the Work

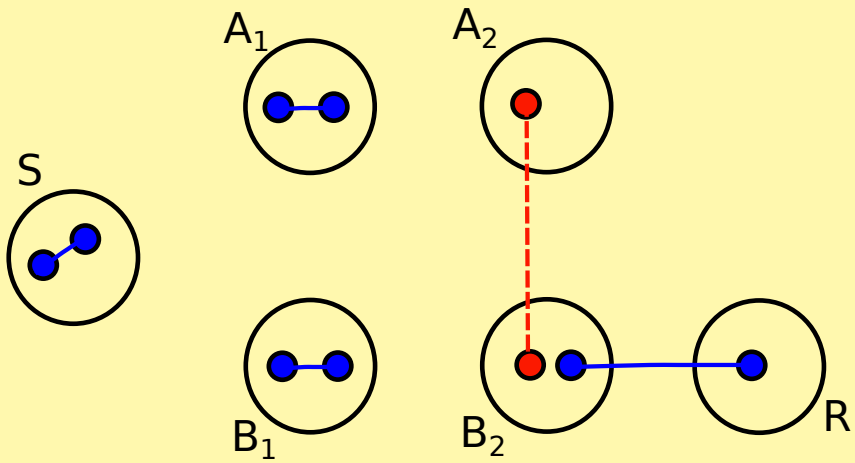

Figure: Secret is shared between A_2 and B_2 as a result of Bell measurement at B_1. Outcome of the measurement will be sent to S in classical channel.

Description of the Work

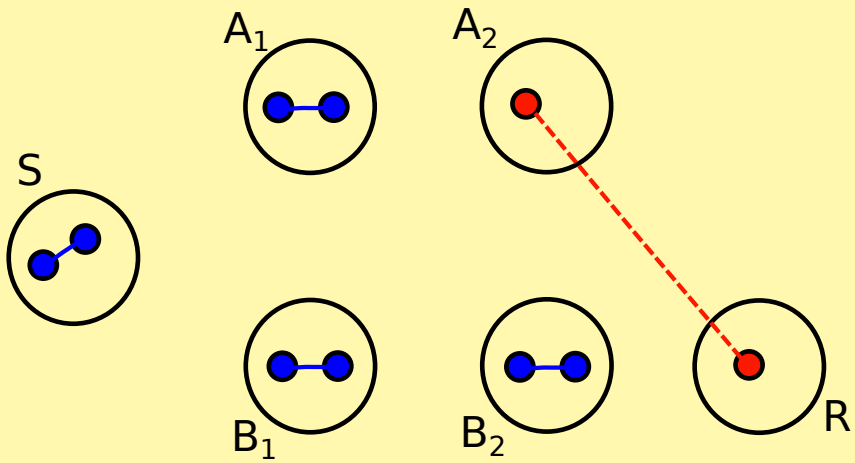

Figure: Secret is shared between A_2 and R as a result of Bell measurement at B_2. Outcome of the measurement will be sent to S in classical channel.

Description of the Work

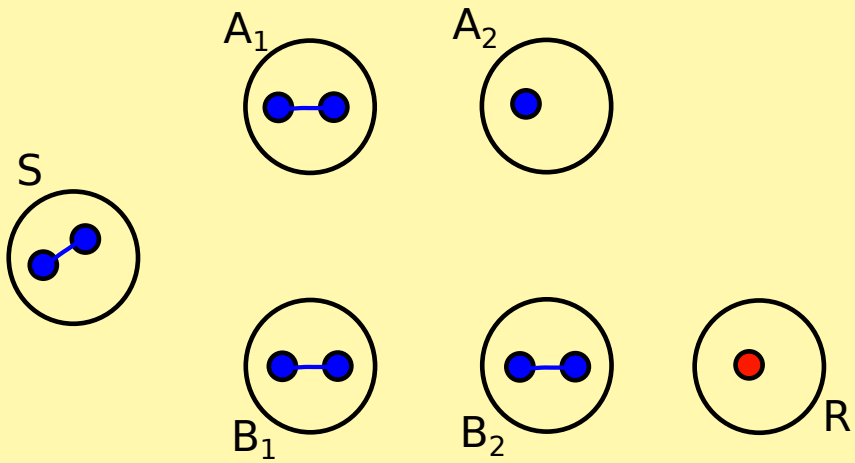

Figure: Finally secret is with R as part of the reconstruction. S will provide classical information to R so that R can actually apply corresponding operator to get the actual secret.

Concluding Remarks and Future Directions

This paper addresses the problem of *revocable* quantum secret sharing. The ability to revoke a quantum shared secret has implications on the possibility of quantum routing (backtracking etc.) in shared domain. An interesting consequence of the above is that critical/private information S can be *qmailed* across public QNETs, first by secret sharing S and then routing S (in the shared domain) to the desired receiver.

Concluding Remarks and Future Directions

Future Directions we are working on:

- We are trying to extend the protocol in most general situation where the consecutive nodes are sharing bi-partite mixed states instead of Bell states
- We are also trying to see how we can have quantum authentication protocol running in a QNET when we have mixed states as resource.

Acknowledgement

This work is done at Center for Security, Theory and Algorithmic Research (CSTAR), IIIT, Hyderabad. Sk Sazim gratefully acknowledge their hospitality. Sk. Sazim and I. Chakrabarty acknowledges Prof. P. Agrawal for having useful discussions.

Conclusion

THANK YOU