Retrieving and Routing Quantum Information in a Quantum Network

S. Sazim,1 V. Chiranjeevi,2 L. Chakrabarty,2 and K. Srinathan2

1Institute of Physics, Sainik School Post, Bhubaneswar-751005, Orissa, India.
2International Institute of Information Technology, Gachibowli, Hyderabad 500 032, Andhra Pradesh, India.

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 Q1 and Q2 and she subsequently finds that Q2 is more reliable than Q1, the dealer may wish to transfer all her secrets from Q1 to Q2.

Known protocols are inadequate to address such a revocation. In this work we address this problem by designing a protocol that enables the source/dealer to bring back the information shared in the network, if desired. Unlike classical revocation, no-cloning-theorem automatically ensures that the secret is no longer shared in the network.

The implications of our results are multi-fold. 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. For example, we show that a source S can send quantum information to a destination R even though (a) S and R share no quantum resource, (b) R’s identity is unknown to S at the time of sending the message, but is subsequently decided, (c) S herself can be R at a later date and/or in a different location to bequeath her information (‘backed-up’ in the qnet) and (d) 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.

PACS numbers: 03.65.Yz, 03.65.Ud, 03.67.Mn

Quantum entanglement [1] not only gives us insight in understanding the deepest nature of reality but also acts as a very useful resource in carrying out various information processing protocols like quantum teleportation [2], quantum cryptography [3] and quantum secret sharing [4], to name a few.

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. Quantum secret sharing (QSS) [11] deals with the problem of sharing of both classical as well as quantum secrets. A typical protocol for quantum secret sharing, like many other tasks in quantum cryptography, uses entanglement as a cardinal resource, mostly pure entangled states. Karlsson et al. [6] studied quantum secret sharing protocols using bipartite pure entangled states. Many authors investigated the concept of quantum secret sharing using tripartite pure entangled states and multi partite states like graph states [7,13]. Q. Li et al. [14] proposed semi-quantum secret sharing protocols taking maximally entangled GHZ state as resource.

In a realistic situation, the secret sharing of classical or quantum information involves transmission of qubits through noisy channels that entails mixed states. Recently in [15], it is shown that Quantum secret sharing is possible with bipartite two qubit mixed states (formed due to noisy environment or otherwise). Subsequently in [16] authors propose a protocol for secret sharing of classical information with three qubit mixed state. Quantum secret sharing has also been realized in experiments [17–20].

In quantum secret sharing(QSS), it is typically assumed that the system consists of solely the dealer and the receivers. However, in practical settings the dealer/receivers are part of a quantum network. One important question of how information can be transferred through a quantum network is addressed in [21]. In this work we focus on two different situations in a given quantum network (qnet). In the first situation, we consider the problem of revoking the secret in QSS. For instance, if the dealer finds the receivers to be dishonest, she can stop them from accessing it. Moreover, she may choose to retrieve back the secret completely. 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 Byzantinely malicious receivers can easily destroy the secret, making revocation impossible.

In the second situation we have extended the above idea to design routing mechanism for multi-hop transmission
of secret qubits in the shared domain itself.

Although the above two situations appear to solve unrelated problems namely, revocable secret sharing and quantum routing, the following is an interesting symbiosis of the two to solve problems posed by resource constraints and asynchrony in the network. Consider a situation where quantum storage is constrained and therefore Alice needs to store her private data in some untrusted memory available in the network. This she can do using revocable quantum secret sharing. Further, if she wants to send this data to Bob, (for security reasons) she should be able to do it without reconstructing the quantum secret anywhere in the network. This she can achieve using the quantum routing in shared domain. Incidentally, our solution also takes care of scenarios where Bob too is in short supply of trusted quantum memory and uses network storage.

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 secretly share a qubit \(|S\rangle = \alpha|0\rangle + \beta|1\rangle\) (where \(|\alpha|^2 + |\beta|^2 = 1\); \(\alpha, \beta\) are amplitudes) with both the parties Bob and Charlie. In order to do so Alice has to do two-qubit measurements in Bell basis \(|\psi_\pm\rangle, |\phi_\pm\rangle\}\) jointly on her resource qubit and the message qubit she wants to share (see Appendix 1). In correspondence to various measurement outcomes obtained by Alice, Bob and Charlie’s qubits collapse into the states given in TABLE I.

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

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.

Revocation of Quantum Information:
If Bob and Charlie are semi-honest (i.e., they are faithful executors of the protocol but curious to learn Alice’s secret), we ask can Alice revoke her shared secret \(|S\rangle\)? The ability to revoke the shared secret is important for several reasons, some of which are (a) Alice decides to change her secret (for instance, \(|S\rangle\) might have been inadvertently shared) (b) Alice conjectures that the recipients are no longer trustworthy (c) there is an update of data/secrets in the higher-level application using secret sharing as a subroutine and (d) Alice has found a more economical alternative qnet to safeguard \(|S\rangle\).

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 two qubits (one from the shared resource and one from shared secret) and Charlie to do measurement on his qubit of shared secret in Hadamard basis (see Appendix 2, 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.

**TABLE I: Sharing of Quantum Information**

**FIG. 1:** 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).

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, possibly via successive entanglement swapping. However, this severely compromises the security of $|S\rangle$. 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. 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.

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 $\{R_1, R_2, R_3, ..., R_n\}$ 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.

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 ($R_i$). (In principle, receivers can share resource with any one of the agents Bob and Charlie. Without any loss of generality we assume the receivers share resources with Charlie only.) 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 $|S\rangle$, 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.

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 Appendix 3, see Fig.2). 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.

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 $|S\rangle$ and receivers $R_1, R_2, ..., R_n$ and we want to send the information to the receiver $R_i$ through a huge network with pair of agents $(A_1, B_1), (A_2, B_2), ......., (A_n, B_n)$ 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.

| Bob’s Outcomes | Charlie’s Outcomes | Alice’s Local Operations |
|----------------|--------------------|--------------------------|
| $|\phi^+\rangle$ | $|$        | $I$                       |
| $|\phi^-\rangle$ | $|$        | $\sigma_z$               |
| $|\phi^0\rangle$ | $+$       | $\sigma_z$               |
| $|\phi^-\rangle$ | $-$       | $I$                       |
| $|\psi^+\rangle$ | $+$       | $I$                       |
| $|\psi^-\rangle$ | $-$       | $\sigma_z$               |
| $|\psi^0\rangle$ | $+$       | $\sigma_z$               |
| $|\psi^-\rangle$ | $-$       | $I$                       |

TABLE II: Retrieving Quantum Information
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 $|S\rangle$ can be $q$-mailed across public QNETS, first by secret sharing $|S\rangle$ and then routing $|S\rangle$ (in the shared domain) to the desired receiver. We have assumed the resources to be pure entangled states, however working out with resources being mixed entangled states still remains an open question.

**Acknowledgment:** This work is done at Center for Security, Theory and Algorithmic Research (CSTAR), IIIT, Hyderabad. S Sazim gratefully acknowledge their hospitality. We acknowledge Prof. P. Agrawal for having useful discussions.

---

**TABLE III: Sending Quantum Information**

| Charlie’s Outcome | Bob’s Outcome | Unitary operations of $R_i$ |
|-------------------|--------------|-----------------------------|
| $|\phi^+\rangle$  | $|+\rangle$   | $I$                         |
| $|\phi^-\rangle$  | $|+\rangle$   | $\sigma_z$                 |
| $|\phi^+\rangle$  | $|-\rangle$   | $\sigma_z$                 |
| $|\phi^-\rangle$  | $|-\rangle$   | $I$                         |
| $|\psi^+\rangle$  | $|+\rangle$   | $\sigma_z$                 |
| $|\psi^-\rangle$  | $|+\rangle$   | $\sigma_z\sigma_z$         |
| $|\psi^+\rangle$  | $|-\rangle$   | $\sigma_z\sigma_z$         |
| $|\psi^-\rangle$  | $|-\rangle$   | $\sigma_z$                 |

FIG. 3: A typical quantum mail sending network where $S$ is the source and $(A_i, B_i)$ are the agents and $R_i$ are the receivers. The information is shared between the pair $(A_i, B_i)$ (the dotted line) and will be transferred to other pairs until the pair close to the desired receiver is reached.

Concluding remarks and Outlook:

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 quantum information (shared secret) reaches the pair $(A_i, B_i)$ close to the desired receiver. Thus, in a QNET we can share, retrieve, hold and as well as transfer the quantum information.

Concluding remarks and Outlook:

[1] A. Einstein, B. Podolsky and N. Rosen, Phys. Rev. 47, 777 (1935).
[2] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, W. K. Wootters, Phys. Rev. Lett. 70, 1895 (1993); D. Bouwmeester, J-W Pan, K. Mattle, M. Eibl, H. Weinfurter and A. Zeilinger, Nature 390, 575 (1997).
[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. 74, 145 (2002)
[4] M. Hillery, V. Buzek, and A. Berthiaume, Phys. Rev. A 59, 1829 (1999); R. Cleve, D. Gottesman, and H-K. Lo, Phys. Rev. Lett. 83, 648 (1999).
[5] R. Cleve et.al, Phys.Rev.Lett. 83 (1999) 648-651
[6] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A 59, 162 (1999).
[7] S. Bandyopadhyay, Phys. Rev. A 62, 012308 (2000);
[8] S. Bagherinezhad, and V. Karimipour, Phys. Rev. A 67, 044302 (2003).
[9] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, Phys. Rev. Lett. 92, 177903 (2004).
[10] G. Gordon, and G. Rigolin, Phys. Rev. A
[11] S. B. Zheng, Phys. Rev. A 74, 054303 (2006).
[12] A. Keet, B. Fortescue, D. Markham, B. C. Sanders, Phys. Rev. A 82, 062315 (2010)
[13] D. Markham, B.C. Sanders, Physical Review A 78, 042309 (2008).
[14] Q. Li, W. H. Chan, and D-Y Long, Phys. Rev. A 82, 022303 (2010).
[15] S. Adhikari, Quantum secret sharing with two qubit bipartite mixed states, arXiv:1011.2868
[16] S.Adhikari, I. Chakrabarty, P. Agrawal, Quantum Information and Computation, 12, 0253 (2012).
[17] W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A 63, 042301 (2001).
[18] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Zukowski, and H. Weinfurter, Phys. Rev. Lett. 95, 230505 (2005).
[19] C. Schmid, P. Trojek, S. Gaertner, M. Bourennane, C. Kurtsiefer, M. Zukowski, and H. Weinfurter, Fortschritte der Physik 54, 831 (2006).
[20] J. Bogdanski, N. Rafiei, and M. Bourennane, Phys. Rev. A 78, 062307 (2008).
Appendix 1:
Consider a 3-qubit GHZ state $\frac{1}{\sqrt{2}}\{|000\rangle + |111\rangle\}$ among Alice, Bob and Charlie and let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ be the message with Alice.

\[
|\psi\rangle \otimes \frac{1}{\sqrt{2}}\{|000\rangle + |111\rangle\} \\
= \{\alpha|0\rangle + \beta|1\rangle\} \otimes \frac{1}{\sqrt{2}}\{|000\rangle + |111\rangle\} \\
= \frac{1}{\sqrt{2}}\{\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle\} \\
= \frac{1}{\sqrt{2}}\{|00\rangle\alpha|00\rangle + |01\rangle\alpha|11\rangle + |10\rangle\beta|00\rangle + |11\rangle\beta|11\rangle\} \\
= \frac{1}{2}\{|[|\phi^+\rangle + |\phi^-\rangle]|\alpha|00\rangle + [|\psi^+\rangle + |\psi^-\rangle]|\alpha|11\rangle + |[|\psi^+\rangle - |\psi^-\rangle]|\beta|00\rangle + |[|\phi^+\rangle - |\phi^-\rangle]|\beta|11\rangle\} \\
= \frac{1}{2}\{|[|\phi^+\rangle]|\alpha|00\rangle + [|\phi^-\rangle]|\alpha|11\rangle| + |[|\psi^+\rangle]|\alpha|11\rangle + |[|\psi^-\rangle]|\beta|00\rangle + |[|\phi^+\rangle - |\phi^-\rangle]|\beta|11\rangle\} \\
(1)
\]

Appendix 2:
Suppose Alice and Bob share a bell state $\frac{1}{\sqrt{2}}\{|00\rangle + |11\rangle\}_{AB}$ and the secret is already being shared between Bob and Charlie is $\{\alpha|00\rangle + \beta|11\rangle\}_{BC}$.

\[
\frac{1}{\sqrt{2}}\{|00\rangle + |11\rangle\}_{AB} \otimes \{\alpha|00\rangle + \beta|11\rangle\}_{BC} \\
= \frac{1}{\sqrt{2}}\{\alpha|00\rangle\alpha|00\rangle + \alpha|00\rangle|01\rangle|1\rangle + \alpha|11\rangle|10\rangle|0\rangle + \beta|11\rangle|11\rangle|1\rangle\}_{ABBC} \\
= \frac{1}{2\sqrt{2}}\{|[|\phi^+\rangle + |\phi^-\rangle]|\alpha|00\rangle + |[|\psi^+\rangle + |\psi^-\rangle]|\alpha|11\rangle + |[|\psi^+\rangle - |\psi^-\rangle]|\beta|00\rangle + |[|\phi^+\rangle - |\phi^-\rangle]|\beta|11\rangle\} \\
= \frac{1}{2\sqrt{2}}\{|[|\phi^+\rangle]|\alpha|00\rangle + |[|\phi^-\rangle]|\alpha|11\rangle + |[|\phi^+\rangle]|\beta|00\rangle - |[|\phi^-\rangle]|\beta|11\rangle + |[|\psi^+\rangle]|\alpha|11\rangle - |[|\psi^-\rangle]|\beta|00\rangle \\
+ |[|\psi^+\rangle]|\beta|11\rangle - |[|\psi^-\rangle]|\alpha|00\rangle + |[|\psi^-\rangle]|\alpha|11\rangle - |[|\psi^+\rangle]|\beta|00\rangle - |[|\psi^-\rangle]|\beta|11\rangle|\} \\
(2)
\]

Appendix 3:
Suppose $R_i$ is the authorized receiver sending request to Charlie and sharing a bell state $\frac{1}{\sqrt{2}}\{|00\rangle + |11\rangle\}_{CR}$, with charlie. Suppose $\{\alpha|00\rangle + \beta|11\rangle\}_{BC}$ is shared among Bob and charlie.

\[
\{\alpha|00\rangle + \beta|11\rangle\}_{BC} \otimes \frac{1}{\sqrt{2}}\{|00\rangle + |11\rangle\}_{CR} \\
= \frac{1}{\sqrt{2}}\{\alpha|00\rangle|00\rangle + \alpha|00\rangle|01\rangle|1\rangle + \beta|11\rangle|10\rangle|0\rangle + \beta|11\rangle|11\rangle|1\rangle\}_{BCCR} \\
= \frac{1}{2\sqrt{2}}\{|[|\phi^+\rangle + |\phi^-\rangle]|\alpha|00\rangle + |[|\psi^+\rangle + |\psi^-\rangle]|\alpha|11\rangle + |[|\psi^+\rangle - |\psi^-\rangle]|\beta|00\rangle + |[|\phi^+\rangle - |\phi^-\rangle]|\beta|11\rangle\} \\
= \frac{1}{2\sqrt{2}}\{|[|\phi^+\rangle]|\alpha|00\rangle + |[|\phi^-\rangle]|\alpha|11\rangle + |[|\phi^+\rangle]|\beta|00\rangle - |[|\phi^-\rangle]|\beta|11\rangle \\
+ |[|\psi^+\rangle]|\alpha|11\rangle - |[|\psi^-\rangle]|\beta|00\rangle + |[|\psi^+\rangle]|\beta|11\rangle - |[|\psi^-\rangle]|\alpha|00\rangle|\} \\
(3)
\]