A NOVEL APPROACH FOR SECURE MULTI-PARTY SECRET SHARING SCHEME VIA QUANTUM CRYPTOGRAPHY

Noor Ul Ain
Dept. of Computing, SEECS
National University of Sciences and Technology
H-12 Islamabad, Pakistan
13msccsnaain@seecs.edu.pk

Abstract*—Classical secret sharing proposed by Shamir used classical computational power in classical cryptography to achieve secret key sharing, but with the advent of quantum systems, computational power can be overruled. To ensure a secure secret sharing scheme independent of computational power, a scheme independent of computational complexity is needed to achieve security. This paper will provide a protocol dependent on inherent secure nature of quantum cryptography (quantum no cloning theorem and quantum measurement rule). A secure multiparty quantum secret sharing scheme has been proposed to ensure that no one can eavesdrop or extract any share of the secret message via inherent security provided by quantum entanglement swapping and quantum teleportation. Entanglement swapping is a process that allows two non-interacting quantum systems to be entangled. Whereas, Quantum teleportation allows a party to send a qubit to another entangled party without sending the qubit over the channel. Moreover, in order to ensure security against possible active attacks, sender himself will generate and distribute EPR pairs to be used in the scheme. Result will be a secure multiparty QSS scheme which will be secure against internal and external eavesdropping, masquerading and brute-force attacks.

Keywords*— Quantum cryptography; Entanglement Swapping; QSS (Quantum Secret Sharing); EPR pair (Einstein-Podolsky-Rosen); Teleportation; OTP (One Time Pad); BSM (Bell State Measurement); Cnot (Controlled Not Gate)

I. INTRODUCTION

Secret sharing [1], a building block of multiparty cryptography, ensures secure communication of any secret among a set of parties in a way that secret can only be revealed when all of the intended recipients come together and communicate with each other. Where classical cryptography assures computational security only, quantum cryptography promises information-theoretic security through the rules of quantum mechanics including quantum no-cloning theorem, and quantum entanglement.

Quantum cryptography proves to be secure as compared to classical cryptography as the protocols in classical systems depend on computational power which can be overruled through quantum systems. Thus a protocol is required against computational attacks. This can be ensured if we use quantum system. Quantum measurement rule states that if someone gets access to a qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ *(where* $|\alpha|^2$ *is the probability of qubit having value 0 and* $|\beta|^2$ *is the probability of qubit having value 1),* and tries to measure it, the measuring qubit will be transformed into classical bit 0 or 1 and cannot be retransformed into original unknown qubit. After the measurement, the system remains in the state corresponding to the result of the measurement.

This protocol will make use of bell states [2], entanglement swapping and quantum teleportation. Bell states $\left(|\Phi^{\pm}\rangle, |\Psi^{\pm}\rangle\right)$ to be used in this protocol are:

$$|\Phi^{\pm}\rangle = \frac{|00\rangle \pm |11\rangle}{\sqrt{2}} \quad (1)$$

$$|\Psi^{\pm}\rangle = \frac{|01\rangle \pm |10\rangle}{\sqrt{2}} \quad (2)$$

Entanglement swapping [2] refers to correlate two parties that have never interacted before. This

can be done by the parties themselves or a trusted third party.

Quantum teleportation [3] is a process where quantum information is sent from one location to another with the help of classical information without sending the qubit over the channel. This is done with the help of pre-shared EPR pairs between the communicating parties.

Quantum no cloning theorem [4] states that no one can create a clone of an unidentified quantum state. This helps in such a way that if someone eavesdrop a quantum bit (qubit), it will be useless for him as he cannot recreate it back to perform an active attack.

Based on quantum entanglement swapping [4] and non-local correlations generated by quantum teleportation and entanglement swapping, an unconditionally secure (4,4) quantum secret sharing scheme for classical secret will be discussed. Both secrecy and authenticity is assured by the sender through quantum non-local correlations. The proposed security protocol will be secure against internal and external eavesdropping along with the attacks during sharing and reconstruction of secrets for (4,4) threshold scheme.

II. PROPOSED ALGORITHM

The proposed (4,4) quantum secret sharing protocol is divided into 4 main phases: 1) EPR pair distribution, 2) Secret distribution, 3) Receiver verification and 4) Secret Recovery. The four phases are discussed below:

A. EPR Pair Distribution Phase

Sender will initially generate 8 EPR pairs that will be known publically. $\left|\Phi^{\pm}\right\rangle = \frac{\left|00\right\rangle \pm \left|11\right\rangle}{\sqrt{2}}$ **or** $\left|\Psi^{\pm}\right\rangle = \frac{\left|01\right\rangle \pm \left|10\right\rangle}{\sqrt{2}}$ with 4 receivers (R_1, R_2, R_3 and R_4).Sender will send second half of 1st two EPR pairs to R_1, 2nd half of next two EPR pairs will be sent to R_2. Similarly, to R_3 and R_4as shown in fig.1. R_1, R_2, R_3 and R_4 will perform BSM on the qubits in their possession to obtain 2 bit classical results: R_1R_1', R_2R_2', R_3R_3' and R_4R_4' respectively. The procedure is shown below in fig 1:*(Dotted lines show that qubit is being sent from one party to another.)*

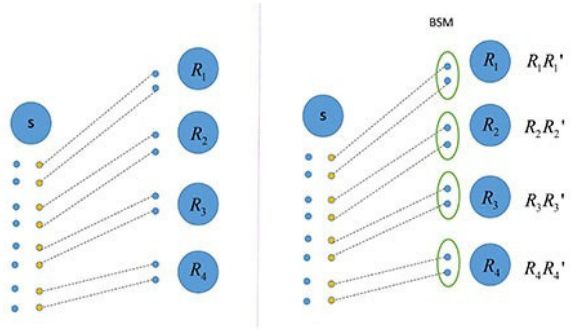

Fig. 1. EPR pairs shared between sender and R_1, R_2, R_3, R_4 and corresponding BSM results

B. Secret Distribution Phase

Based on the results obtained from EPR Pair Distribution phase, 4 EPR pairs will be generated by the sender by performing following operations

EPR pair1 (a)(b) will be generated as:
(a)(b) =(OTP $\oplus$ R_1) (OTP $\oplus$ R_1') (3)

EPR pair2 (c)(d) will be generated as:
(c)(d) =(OTP $\oplus$ R_2) (OTP $\oplus$ R_2') (4)

EPR pair3 (e)(f) will be generated as:
(e)(f) =(OTP $\oplus$ R_3) (OTP $\oplus$ R_3') (5)

EPR pair4 (g)(h) will be generated as:
(g)(h) =(OTP $\oplus$ R_4) (OTP $\oplus$ R_4') (6)

Sender will send second half of 1st 2 EPR pairs (3) and (4) to R_1 and second half of next two EPR pairs (5) and (6) will be sent to R_2. R_1 and R_2 will perform BSM on qubits in their possession to get 2-bit classical result R_aR_a' and R_bR_b' respectively. As a result, the qubits in possession of sender will be transformed to ss' and s_1s_1' as shown in fig 2. *(Dotted*

lines show that qubit is being sent from one party to another.)

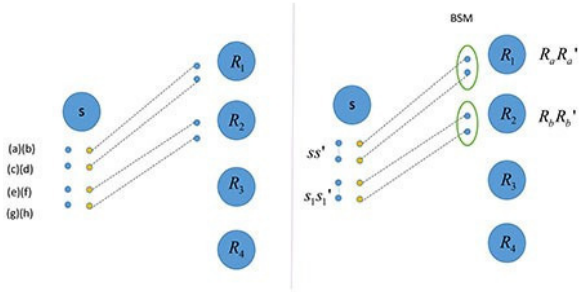

Fig. 2. EPR pairs shared between R_1, R_2 and corresponding BSM results for secret sharing

Now, sender will send 2-bit classical message s_2s_2' to R_3 after performing following operation:

$$s_2s_2' = (OTP \oplus s)\ (OTP \oplus s') \qquad (7)$$

Finally, sender will generate an EPR pair on basis of s_1s_1' and will send one half of that EPR pair to R_4. After that sender will perform quantum teleportation on the EPR pair share $|\varphi\rangle$ in his possession to send the secret qubit share to R_4 via entanglement swapping. Thus the qubit in possession of R_4 will be transformed into $|\varphi\rangle' = \sigma_T |\varphi\rangle$ (where σ_T is the secret operator applied by sender and $|\varphi\rangle'$ is the transformed qubit at R_4 side). Sender will get 2-bit classical result s_3s_3' because of BSM performed on the qubits in his possession as shown in fig 3.

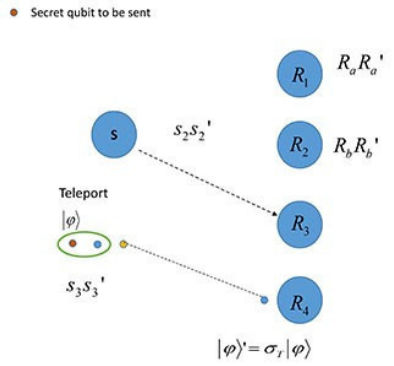

Fig. 3. Teleportation of secret qubit $|\varphi\rangle$ from sender to R_4

As all parties have some share of the secret message so no one can individually extract the secret message. In order to extract the secret message, sender has to provide OTP (One Time Pad) and s_3s_3'. R_1 has to provide R_1R_1' and R_aR_a'. R_2 has to provide R_2R_2' and R_bR_b'. R_3 has to provide R_3R_3' and R_4 has to provide R_4R_4' and $|\varphi'\rangle$. Thus secret has been distributed and all parties will collaborate to decrypt the secret message.

To avoid any possible active or passive attack, sender will first authenticate all the receivers and once they get authenticated, sender will provide the secret share in his possession to help them in decrypting the secret message.

C. *Receiver(s) Validation Phase*

In order to verify R_1, R_2, R_3 and R_4, these parties will send following information to sender for verification:

- R_1 will send $(R_1 CnotR_a)(R_1'CnotR_a')$
- R_2 will send $(R_2 CnotR_b)(R_2'CnotR_b')$
- R_3 will send $(R_3 CnotR_3')$
- R_4 will send $(R_4 CnotR_4') \oplus |\varphi'\rangle$

Sender will verify the results by applying reverse operators on the information to verify the receivers. If results sent by receiver(s) match with the results at sender side, only then sender will reveal the necessary secret information.

D. *Secret Recovery Phase*

To extract secret, R_1 will give R_aR_a', R_2 will give R_bR_b', R_3 will give s_2s_2', R_4 will give $|\varphi'\rangle$ and sender will give s_3s_3' and OTP to decrypt the secret message. Hence secret has been distributed successfully. As sender will give the final secret share only after verifying the receivers, system cannot be cheated. Now, to reconstruct the secret, contribution of all parties is necessary. Thus the proposed secret sharing scheme is secure against active and passive eavesdropping as nothing was ever shared on the channel publically.

In the next section, we will discuss the possible results related to receiver verification and secret share distribution.

III. RESULT AND DISCUSSION

After completing the protocol, sender will verify R_1, R_2, R_3 and R_4. Once all receivers are successfully verified, only then sender will share the necessary part to decrypt the secret qubit.

A. Notation

$RpRp'$ is the value of $R_1R_1'$and R_qR_q' is the value of R_2R_2' known to sender.
R_wR_w' is the value of R_1R_1' and $R_xR_x'$is the value of R_2R_2' in possession of R_1 and R_2 respectively.
R_yR_y' is the value of R_aR_a' andR_zR_z' is the value of R_bR_b' in possession of R_1 and R_2 respectively.

B. Calculations to be Performed

In order to verify R_1 and R_2, following operations will be performed by sender:

To verify R_w sender will do ($Rp \oplus R_w$), if ($Rp \oplus R_x$=0) R_w will be verified.
To verify R_w' sender will do ($Rp' \oplus R_w'$), if ($Rp' \oplus R_w'$=0) R_w' will be verified.
To verify R_yR_y', sender will perform following operation:

If R_w=0, (R_y=R_y)
else (R_y= $\overline{R_y'}$)

Similarly,

If R_w'=0, (R_y'=R_y')
Else R_y' = $\overline{R_y'}$

Same procedure can be done to verify R_2.

Table I. Verification of values of R_1R_1' sent by receiver R_1

R_pR_p'	Data sent by R_1 (R_wR_w')				Verification of R_1 by sender for R_1R_1'			
00	00	01	10	11	00	01	10	11
01	00	01	10	11	01	00	11	10
10	00	01	10	11	10	11	00	01
11	00	01	10	11	11	10	01	00

Highlighted values show the points where values sent by receiver R_1 are verified by the sender. Same table can be drawn to verify R_2 as well.
In order to verify R_3, following operations will be performed:

To verify R_3 sender will perform ($R_{s3} \oplus R_3$), if ($R_{s3} \oplus R_3$=0) R_3 will be verified.
To verify R_3' sender will perform following operation:

If R_3=0, R_3'=R_3'
else R_3= $\overline{R_3'}$

where $R_{s3}R_{s3}'$ are the values of R_3R_3' at sender side.

Table II: Results of R_3 verification by the sender via the mutual classical information between them.

Verification of R_3R_3' by Sender				
R_3R_3' at sender side	**00**	**01**	**10**	**11**
R_3CNOTR_3' / R_3R_3'	**00**	**01**	**11**	**10**
00	00	01	10	11
01	00	01	10	11
10	10	11	00	01
11	10	11	00	01

To verify R_4, sender will perform $(R_4CnotR_4)_{sender}$ on the classical result in his possession and then, sender will perform XOR of his measurement results with the result sent by R_4 to verify φ' .

$$(R_4CnotR_4)_{sender} \oplus (R_4CnotR_4) \oplus \varphi' \qquad (8)$$

From (8), it can be seen that if R_4R_4' are same at sender and R_4 side, then

$(R_4CnotR_4)_{sender} \oplus (R_4CnotR_4)$ will be 0 and sender will get φ'. Else R_4 will not be verified.

Now, if sender and R_4 share bell state $\left|\Phi^+\right\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$ and the secret state sent by sender to R_4 is $\alpha|0\rangle + \beta|1\rangle$, then if R_4 wants to extract the qubit, he needs s_3s_3' from sender to know

which operator must be applied to reconstruct the original qubit.

Table III: Results of quantum teleportation between sender and R_4 when $\left|\Phi^+\right\rangle$ is shared between S and R_4

Classical Result at sender side s_3s_3'	**Transformed qubit at Receiver side $\left\|\varphi'\right\rangle$**	**Operator to be applied (σ_T)**
00	$\alpha\|0\rangle+\beta\|1\rangle$	$I\|\varphi'\rangle$
01	$\alpha\|1\rangle+\beta\|0\rangle$	$X\|\varphi'\rangle$
10	$\alpha\|0\rangle-\beta\|1\rangle$	$Z\|\varphi'\rangle$
11	$\alpha\|1\rangle-\beta\|0\rangle$	$ZX\|\varphi'\rangle$

If sender and R_4 share bell state $\left|\Psi^+\right\rangle=\frac{|01\rangle+|10\rangle}{\sqrt{2}}$ and the secret state sent by sender to R_4 is $\alpha|0\rangle+\beta|1\rangle$, then if R_4 wants to extract the qubit, he needs s_3s_3' from sender to know which operator must be applied to reconstruct the original qubit.

Table IV: Results of quantum teleportation between sender and R_4 when $\left|\Psi^+\right\rangle$ is shared between S and R_4

Classical Result at sender side s_3s_3'	**Transformed qubit at Receiver side $\left\|\varphi'\right\rangle$**	**Operator to be applied (σ_T)**
00	$\alpha\|1\rangle+\beta\|0\rangle$	$X\|\varphi'\rangle$
01	$\alpha\|0\rangle+\beta\|1\rangle$	$I\|\varphi'\rangle$
10	$\alpha\|1\rangle-\beta\|0\rangle$	$ZX\|\varphi'\rangle$
11	$\alpha\|0\rangle-\beta\|1\rangle$	$Z\|\varphi'\rangle$

The results can be verified for other two bell states as well. When R_1, R_2, R_3 and R_4 will be verified, only then sender will share s_3s_3' and OTP. Then R_1, R_2, R_3 and R_4 will play their part to determine the secret qubit sent by the sender.

The scheme proposed is thus secure against any internal and external eavesdropping attacks, as if someone eavesdrop on any classical information it is of no use, because the secret has not been sent directly over the channel. Secondly, if someone gets access on the qubit in any way, and tries to measure it, qubit will be transformed into classical result. Thus attacker will not be able to extract any secret without the help of all other parties. Hence, no active attack can be performed as well. This proves that the proposed scheme is secure and verified as per the results provided.

IV. CONCLUSIONS AND FUTURE WORK

Quantum cryptography is a relatively new field and there is a lot of room for improvement. A lot of work is still needed to be done and there are many questions that are still unanswered. The protocol defined here is complete in itself. However, there are some other ways that can be utilized to achieve quantum secret sharing provided the predefined security requirements met. One can make use of super dense coding where the classical information to be sent will also be encoded over the qubits formed in a shared EPR pair. Second important thing that is needed to be explored in field of quantum cryptography is "*Quantum Digital Signature*". Another important issue is user masquerading, i.e. if a user with infinite quantum computational power succeeds to capture a qubit before the legitimate party and then starts participating in the authentication, the user will never be able to capture them. Hence these issues are needed to be addressed and can be treated as future work in field of quantum cryptography.

REFERENCES

[1] Nadeem, M. (2015). "Quantum cryptography – an information theoretic security". *arXiv:1507.07918.*

[2] M Nadeem, Noor Ul Ain, (2015) "Secure and authenticated quantum secret sharing**",** *arXiv preprint arXiv:1506.08558, 2015 - arxiv.org.*

[3] MuneerAlshowkan, Khaled Elleithy (2014) "Authenticated Multiparty Secret Key Sharing Using Quantum Entanglement Swapping". *Conference of the American Society for Engineering Education*

[4] David McMAHON, (2008) "Quantum Computing Explained*," IEEE Computer Society, Wiley & Sons Canada*

[5] Xiaoqing Tan, Zhihong Feng, Lianxia Jiang, Afen Fang, (2013) "Verifiable Quantum Secret Sharing Protocol". *Fourth International Conference on Emerging Intelligent Data and Web Technologies*