A Proposal for Quantum Rational Secret Sharing

Arpita Maitra\(^1\), Sourya Joyee De\(^2\), Goutam Paul\(^2\) and Asim K. Pal\(^1\)

\(^1\)Management Information Systems Group, Indian Institute of Management Calcutta, India.
Email: {arpitam, asim}@iimcal.ac.in
\(^2\)Cryptology & Security Research Unit, R. C. Bose Centre for Cryptology & Security, Indian Statistical Institute, Kolkata.
Email: sjoyeede@gmail.com, goutam.paul@isical.ac.in

A rational secret sharing scheme is a game in which each party responsible for reconstructing a secret tries to maximize his utility by obtaining the secret alone. Quantum secret sharing schemes, either derived from quantum teleportation or from quantum error correcting code, do not succeed when we assume rational participants. This is because all existing quantum secret sharing schemes consider that the secret is reconstructed by a party chosen by the dealer. In this paper, for the first time, we propose a quantum secret sharing scheme which is resistant to rational parties. The proposed scheme is fair (everyone gets the secret), correct and achieves strict Nash equilibrium.

I. INTRODUCTION AND MOTIVATION

A \((t,n)\) or \(t\)-out-of-\(n\) threshold secret sharing scheme [3,22] comprises the distribution of shares of a secret \(s\) among \(n\) players \(P_1, \ldots, P_n\) such that at least \(t\) of these players must communicate their shares to each other. An example of such a secret sharing scheme is Shamir’s scheme [29] that uses the concept of polynomial interpolation for generation and distribution of shares of the secret by a dealer and subsequent reconstruction of the secret by the players. Players that are ‘good’ or ‘honest’ cooperate to reconstruct the secret, while players that are ‘bad’ or malicious do not cooperate [12]. So, for successful reconstruction of the secret, at most \((n-t)\) players may be ‘bad’.

In classical threshold secret sharing, Halpern and Teague [12] introduced the concept of rational players. Rational players are neither ‘good’ nor ‘bad’. They are selfish or utility maximizing. Each rational party wishes to learn the secret while allowing as few others as possible to learn the secret. Halpern and Teague [12] showed that in the presence of rational players, Shamir’s scheme fails. Specifically, no rational player has the incentive to send his share during secret reconstruction. From the viewpoint of each player \(P_i\), either \((t-1)\) other players send their shares or they do not. If they send, then \(P_i\), even without sending his own share, can reconstruct the secret for himself without allowing these \((t-1)\) players to reconstruct. If they do not send, then none of the players can reconstruct the secret. So from each player \(P_i\)’s point of view, not sending his share weakly dominates sending his share. Thus the Nash equilibrium achieved in Shamir’s secret sharing corresponds to the case where nobody sends anything to each other. To mitigate this problem, the authors of [12] introduced the concept of rational secret sharing (RSS). Its application in secure multiparty computation is known as rational multi-party computation or RMPC and has been an active area of research [1,2,3,4,17,19,20,22] in recent times.

The idea of quantum secret sharing (QSS) of a single qubit was first due to Hillery et al. [14] using three and four qubit GHZ states. Later, this process was investigated by Karlsson et al. [15] using three particle entanglement, Cleve et al. [4] using a process similar to error correction and Zheng [33] using W state. The QSS of an arbitrary two-qubit state was proposed by Deng et al. [7] using two GHZ states. QSS using cluster states was demonstrated by Nie [23], Panigrahi [22,26] and Han [13]. Recently, two qubit QSS was discussed using arbitrary pure or mixed resource states [32] and asymmetric multipartite state [31]. Note that in \(t\)-out-of-\(n\) QSS, the dealer chooses to reveal the secret to a specific subset of \(t\) parties and not to any arbitrary subset of \(t\) parties.

Thus in QSS, all the parties are ‘good’ or ‘honest’ as they have agreed to reconstruct the secret to the party (or parties) chosen by the dealer. However, if we impose rational behavior of the participants in QSS, it is quite natural for the last player, who generates the secret, to quit with the secret alone. Hence, the other players always prefer not to give their shares (either classical bits or quantum bits) and hence the traditional QSS scheme fails if the players behave rationally. In this paper, we propose for the first time a quantum secret sharing scheme that forces the participants to send the shares, though they are rational in nature. We call this scheme a quantum rational secret sharing (QRSS) scheme.

II. PRELIMINARIES

In this section, we briefly describe classical rational secret sharing and discuss the concepts of rationality, fairness, correctness and equilibrium used in this work. We also extend these concepts in the quantum domain.

The dealer in a classical rational secret sharing (RSS) protocol is honest and can be online or offline. An online dealer remains available throughout the secret reconstruction protocol, whereas an offline dealer becomes
unavailable after distributing the shares of the secret. Note that an online dealer is not very practical as he repeatedly interacts with the players and such a dealer can directly provide the secret to the players. In 2008, Kol and Naor [17] discussed rational secret sharing in the non-simultaneous channel model and in the presence of an offline dealer, in an information theoretic setting. Almost all the subsequent works [2, 6, 8, 20, 25] on rational secret sharing assumed the dealer to be offline.

Rational secret sharing proceeds in two phases: 1) share generation and distribution and 2) secret reconstruction.

Share generation and distribution: If the dealer is online, then at the beginning of each round, he distributes to each player $P_i$ the share of the actual secret with probability $\gamma$ or that of a fake secret with probability $(1-\gamma)$. The value of $\gamma$ is kept secret from the parties and is dependent on the utility values of the parties $\{2,12\}$. An offline dealer distributes to each party $P_i$ a list of shares, one of which is that of the actual secret $s$ and the remaining of fake secrets $\{8,17,24\}$. The position $r$ of this actual share in the lists is not revealed to the players and is chosen according to a geometric distribution $G(\gamma)$, where the parameter $\gamma$ in turn depends on the utility values of players. The dealer generates shares using Shamir’s secret sharing scheme.

Secret Reconstruction: In the $j$th round of communication, each player $P_i$ (either simultaneously or non-simultaneously) broadcasts or sends individually to each of the other players (in presence of synchronous, point-to-point channels) the share $s_{ij}$ corresponding to that round. The shares are signed by the dealer. Hence, no player can give out false shares undetected and the only possible action of a player in a round is to either 1) send the message or 2) remain silent. The round in which the shares of the actual secret are revealed and hence the secret is reconstructed is called revelation or definitive round. When the dealer is offline, players are made aware that they have crossed the revelation round by the reconstruction or exchange of an indicator (a bit in $[17]$, a signal in $[6]$). For simultaneous channel model, parties can identify a revelation round as soon as it occurs. However, for non-simultaneous channels, the indication is delayed till the subsequent round to avoid rushing strategy. In this case, the indicator cannot be reconstructed or interpreted by all the players. The player who communicates last during the reconstruction of the indicator is the first and only one to know that the last round was the revelation round. Once he comes to know this, he has no incentive to send his share of the indicator to the other players for reconstruction. Instead, he simply quits. The fact that this player quits signals to the other players that the secret has been reconstructed.

In classical RSS protocols, the dealer signs each share so that no player can give out wrong shares to others. However, in the quantum setting the scenario is different. Typically, quantum signature schemes consider signing either classical messages $[10]$ or quantum message string with independent qubits $[18]$. In these works, there is no concept of entanglement among the distributed shares, whereas in our proposed scheme, the shares are entangled. It is not known how to sign such qubits which contain the information of the secret, as any type of measurement on that qubits will destroy the entanglement and hence the information related to the secret. For this reason, we assume that a rational player in the quantum setting is fail-stop by nature, i.e., he may abort early in an attempt to obtain the secret alone but does not send false shares of the secret.

It is very natural for a player to measure his share as soon as he gets it. However, in this work, we encode the secret by CSS code which takes care of arbitrary error. Thus measuring his qubit in an arbitrary basis gives no advantage to the player. Even with unconditional power of computation the quantum adversary extracts no information about the secret. Moreover, if he measures the share he will lose the information stored in the qubit. Thus no player has any incentive to measure his qubit(s) and each player communicates each share as it is received from the dealer.

A $(t,n)$ rational secret reconstruction protocol is a pair $(\Gamma, \vec{\sigma})_{t,n}$, where $\Gamma$ is the game (i.e., specification of allowable actions) and $\vec{\sigma}=(\sigma_1,\ldots,\sigma_n)$ denotes the strategies followed by the players. We use the notations $\vec{\sigma}_{-i}=(\sigma_1,\ldots,\sigma_{i-1},\sigma_{i+1},\ldots,\sigma_n)$ and $(\sigma'_1,\vec{\sigma}_{-i})=(\sigma_1,\ldots,\sigma_{i-1},\sigma'_i,\sigma_{i+1},\ldots,\sigma_n)$. The outcome of the game is denoted by $\vec{\sigma}((\Gamma, \vec{\sigma})_{t,n})=(o_1,\ldots,o_n)$. The outcomes of a secret reconstruction game $\Gamma$ with respect to a party $P_i$ are as follows: 1) $P_i$ obtains the secret while others do not; 2) everybody obtains the secret; 3) nobody obtains the secret 4) others obtain the secret while $P_i$ does not and 5) others believe in a fake secret while $P_i$ does not. The output that no secret is obtained is denoted by $\bot$ and fake secret is denoted by any symbol $\notin \{s,\bot\}$.

### A. Utilities and Preferences

The utility function $u_i$ of each party $P_i$ is defined over the set of possible outcomes of the game. The outcomes and corresponding utilities for $t = n = 2$ are described in Table 1. For classical secret sharing, $u_i$ is assumed to be polynomial in the security parameter $k$ which is typically the size of the secret. Thus, $U_i^{NN} = u_i(1^k, \{o_i = s, o_j = \bot\}), U_i^{TT} = u_i(1^k, \{o_i = s, o_j = s\})$ (where $i \neq j$) and so on.

For quantum domain, the secret is a state $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$, or in other words, a pair of complex numbers $\{\alpha, \beta\}$. Thus, the size of the secret is effectively infinite. Hence, the assumption on the utilities as polynomial functions of the security parameter has no meaning. Rather, we treat the utilities as real numbers that depend on the output values.

Players have their preferences based on the different possible outcomes. In this work, a rational player $i$ is
TABLE I: Outcomes and Utilities for (2,2) rational secret reconstruction

| $P_i$’s outcome | $P_i$’s outcome | $P_i$’s Utility | $P_i$’s Utility |
|-----------------|-----------------|-----------------|-----------------|
| $(o_1)$         | $(o_2)$         | $U_{o_1,o_2}$   | $U_{o_1,o_2}$   |
| $o_1 = s$       | $o_2 = s$       | $U_{TT}$        | $U_{TT}$        |
| $o_1 = \bot$    | $o_2 = \bot$    | $U_{NN}$        | $U_{NN}$        |
| $o_1 = s$       | $o_2 = \bot$    | $U_{TN}$        | $U_{TN}$        |
| $o_1 = \bot$    | $o_2 = s$       | $U_{NT}$        | $U_{NT}$        |
| $o_1 = \bot$    | $o_2 \notin \{s,\bot\}$ | $U_{NF}$ | $U_{NF}$ |
| $o_1 \notin \{s,\bot\}$ | $o_2 = \bot$ | $U_{TN}$        | $U_{TN}$        |

assumed to have the following preference:

$$R_1 : U_{TT} > U_{NN} > U_{NT}.$$ 

Some players may have the additional preference

$$U_{iNF} \geq U_{iTT},$$

whereas the rest have

$$U_{iNF} < U_{iTT}.$$ 

For more than two players, the second superscript $Y$ in the notation $U_{iY}$ correspond to any of the other players (except $i$ itself).

### B. Fairness

A rational player, being selfish, desires an unfair outcome, i.e., obtaining the secret alone. Therefore, the basic aim of rational secret sharing schemes has been to achieve fairness. A formal definition of fairness in the context of a (2,2) RSS protocol was presented by Asharov and Lindell [2]. We modify this definition for the $(t, n)$ quantum setting as follows:

**Definition 1.** (Fairness, adapted from [2]) A rational secret reconstruction mechanism $(\Gamma, \overline{\sigma})_{i,n}$ is said to be completely fair if for every arbitrary alternative strategy $\sigma_i'$ followed by party $P_i$, $(i \in \{1, \ldots, n\})$ the following holds:

$$Pr[o_i(\Gamma, (\sigma'_i, \overline{\sigma} - i)) = s] < Pr[o_{-i}(\Gamma, (\sigma'_i, \overline{\sigma} - i)) = s].$$

In the above definition, the subscript $-i$ denotes all the players other than $i$.

Fairness can be achieved by a suitable randomized reconstruction of the protocol. The exact round in which the actual secret is to be revealed is not known to the parties. In Theorem 3 we show that the condition for fairness is

$$\gamma U_{iTN} + (1 - \gamma)U_{iNN} < U_{iTT}.$$ 

Or, $\gamma < \frac{U_{iTT} - U_{iNN}}{U_{iTN} - U_{iNN}}$ 

for each $i$. This is the same condition that is required in the classical scenario.

### C. Correctness

A formal definition of correctness in the context of a (2,2) RSS protocol was presented by Asharov and Lindell [2]. We modify this definition for the $(t, n)$ quantum setting as follows:

**Definition 2.** (Correctness) A rational secret reconstruction mechanism $(\Gamma, \overline{\sigma})$ is said to be correct if for every arbitrary alternative strategy $\sigma_i'$ followed by party $P_i$, $(i \in \{1, \ldots, n\})$ the following holds:

$$Pr[o_{-i}(\Gamma, (\sigma'_i, \overline{\sigma} - i)) \notin \{s, \bot\}] = 0.$$ 

In classical rational secret sharing, the condition of correctness becomes significant in the non-simultaneous channel model. The rational party with preference $R_1$ communicating last in any round may quit early in the protocol. Since other parties decide whether the revelation round has been reached depending on whether the last party has quit, they are easily misled into believing in a wrong value of the secret.

### D. Equilibrium

A rational secret reconstruction protocol should be such that no player has any incentive to deviate from this protocol. Consequently, Nash equilibrium and its several variants have been used as the equilibrium concept in the literature of rational secret sharing. A suggested strategy $\overline{\sigma}$ of a mechanism $(\Gamma, \overline{\sigma})$ is said to be in Nash equilibrium when there is no incentive for a player $P_i$ to deviate from the suggested strategy, given that everyone else is following this strategy.

The concept of strict Nash equilibrium becomes useful when the payoffs from playing a ‘good’ strategy and a ‘bad’ strategy are so close that any minor changes in the beliefs of players about the strategy others are going to adopt may lead each of them to play the ‘bad’ strategy [17]. It is defined as follows:

**Definition 3.** (Strict Nash Equilibrium) The suggested strategy $\overline{\sigma}$ in the mechanism $(\Gamma, \overline{\sigma})$ is a strict Nash equilibrium if for every $P_i$ and any strategy $\sigma_i'$, we have $u_i(\sigma'_i, \overline{\sigma} - i) < u_i(\overline{\sigma})$.

There may exist several strategies which are the same as the suggested strategy $\overline{\sigma}$, for party $P_i$ except for minor differences such as performing some irrelevant computation or sending different messages after the protocol is over. For the sake of proving that a proposed protocol is in strict Nash equilibrium, we assume that all such strategies are essentially the same and do not constitute any deviation.
III. OUR PROPOSAL ON QUANTUM RATIONAL SECRET SHARING

In this section we first present a $(3, 7)$ quantum rational secret sharing (QRSS) protocol and we generalize it to the $(t, n)$ setting in the next section.

We do not exploit the ideas related to teleportation in quantum secret sharing. The idea of teleportation does not naturally take the idea of the situation when parties are rational. Rather, we use quantum error correcting code.

There exist some works \cite{BB84, KS96, GH96, GNB96} for building quantum secret sharing schemes using (classical or quantum) error correcting codes. However, none of these schemes addresses the rationality issue.

An arbitrary pure single-qubit quantum state is given by $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$, where $\alpha, \beta \in \mathbb{C}$. Quantum error correction scheme known as CSS code \cite{CSS}, can be constructed from classical error correcting code. Let $C$ and $C_1$ be two classical linear codes such that $\{0\} \subset C_1 \subset C \subset \mathbb{F}_2^n$ with the generator matrices

\[ G = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1
\end{pmatrix}, \]

\[ G_1 = \begin{pmatrix}
0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 & 1
\end{pmatrix}. \]

From the above expression it is clear that $C_1$ is the dual code \cite{CSS} of $C$. A quantum CSS code can be constructed from these two linear codes with code words $|0\rangle_L$ and $|1\rangle_L$. A pure single quantum state can be encoded with this code by attaching an ancilla state $|0\rangle$ and applying the CNOT gate. After inserting the ancilla state we get $\alpha|00\rangle + \beta|10\rangle$ which is converted to $\alpha|00\rangle + \beta|11\rangle$ after the application of the CNOT gate. $|00\rangle$ can be encoded by the above CSS code as $|1\rangle_L$ and $|11\rangle$ can be encoded as $|0\rangle_L$. Thus the entire state is encoded as

\[ \frac{1}{\sqrt{8}}\left[ (\alpha|1111111\rangle + |1010010\rangle + |1100100\rangle + |1001001\rangle \\
+ |0000111\rangle + |0101010\rangle + |0011100\rangle + |0110001\rangle \\
+ \beta(|0000000\rangle + |0101101\rangle + |0011101\rangle + |0111010\rangle \\
+ |1111000\rangle + |1010100\rangle + |1100011\rangle + |1001110\rangle) \right]. \]

In light of the above discussion, let us now explain our exact proposal and its importance. Here, we assume the secret as a single qubit $\alpha|0\rangle + \beta|1\rangle$. We encode the secret with the above CSS code. Thus the secret is now split into seven qubits. The dealer distributes these seven qubits among seven parties. We now write the secret as

\[ \frac{1}{\sqrt{8}}\left[ (|1111\rangle [\alpha|11\rangle + \beta|00\rangle] + |1010\rangle [\alpha|01\rangle + \beta|10\rangle] \\
+ |1100\rangle [\alpha|10\rangle + \beta|01\rangle] + |1001\rangle [\alpha|00\rangle + \beta|11\rangle] \\
+ |0000\rangle [\alpha|11\rangle + \beta|00\rangle] + |0101\rangle [\alpha|01\rangle + \beta|10\rangle] \\
+ |0011\rangle [\alpha|10\rangle + \beta|01\rangle] + |0110\rangle [\alpha|00\rangle + \beta|11\rangle] \right]. \]

Applying CNOT gate on last three qubits, we obtain

\[ \frac{1}{\sqrt{8}}\left[ (|1111\rangle [\alpha|1\rangle + \beta|0\rangle] |00\rangle + |1010\rangle [\alpha|0\rangle + \beta|1\rangle] |10\rangle \\
+ |1100\rangle [\alpha|1\rangle + \beta|0\rangle] |11\rangle + |1001\rangle [\alpha|0\rangle + \beta|1\rangle] |01\rangle \\
+ |0000\rangle [\alpha|1\rangle + \beta|0\rangle] |00\rangle + |0101\rangle [\alpha|0\rangle + \beta|1\rangle] |10\rangle \\
+ |0011\rangle [\alpha|1\rangle + \beta|0\rangle] |11\rangle + |0110\rangle [\alpha|0\rangle + \beta|1\rangle] |01\rangle \right]. \]

Thus if last three parties collaborate, then one can reconstruct the secret by measuring the last two qubits in basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\$. If a party gets $|00\rangle$ or $|11\rangle$, he has to apply $X$ gate to obtain the secret. If a party gets $|01\rangle$ or $|10\rangle$, he has to apply $I$ gate to construct the secret. Close observation reveals that there are only seven combinations of three parties for which secret can be reconstructed. Denoting the position of the participants by integer values, we can write those combinations as $\mathcal{A} = \{(5, 6, 7), (1, 2, 5), (2, 4, 6), (1, 3, 6), (1, 4, 7), (2, 3, 7), (3, 4, 7)\}$. The set $\mathcal{A}$ is called the access structure of the secret sharing scheme.

A. (3,7) Quantum Rational Secret Sharing Protocol

In classical rational secret sharing, an indicator is distributed along the shares of each secret to each party. The parties reconstruct the indicator and comes to know about the revelation round. However, in quantum domain, including an indicator is costly. We solve this problem by assuming that the dealer is semi-offline. In other words, the dealer interacts with the participants twice, 1) at the time of the share distribution, and 2) at the time when the game is over. In Section II we discuss how to make the dealer offline. As in classical RSS protocols, our dealer is assumed to be honest.

In classical simultaneous broadcasting channel, each party is supposed to broadcast his share in each round. So, in each round, each party obtains $(t-1)$ shares from others and thus reconstructs the secret. In the point-to-point channel model, instead of broadcasting his share, each party in each round individually communicates his share to every other party. This means each party prepares copies of his share and distributes $(t-1)$ shares among $(t-1)$ parties retaining one share for himself. In quantum domain, due to the no cloning theorem \cite{NC}, a player cannot generate copies of his share. However, the dealer can prepare as many copies of the secret as required as he knows the secret. We exploit this idea to form our protocol. The communication in the quantum
setting is similar to the communication in the point-to-point channel model. Unlike classical RSS, each round is further sub-divided into sub-rounds. In the ith sub-round of a round j the participant \( P_i \) is given the current shares (qubits) by the remaining players. For example, in \((3,7)\) quantum rational secret sharing, in the first sub-round \( P_2 \) and \( P_3 \) give their current shares (qubits) to \( P_1 \). In the second sub-round \( P_1 \) and \( P_3 \) give their current shares to \( P_2 \). In the third sub-round \( P_1 \) and \( P_2 \) give their current shares to \( P_3 \).

We assume that the players are of fail-stop nature. This means that they do not send wrong shares. In each round, a player has just two strategies, either to send his share or to remain silent. Remaining silent is equivalent to quit the game. Throughout the paper whereas we use the word “quit”, we want to mean that the player remains silent from the very sub-round of a round. The dealer is assumed to be honest. We describe our protocol \( \pi^{3,7}_{QRSS} \) below. Without loss of generality, we assume that the dealer wishes to reveal the secret to the parties receiving qubits 5, 6 and 7 and we label them as players \( P_1, P_2 \) and \( P_3 \) respectively.

1. Protocol \( \pi^{3,7}_{QRSS} \)

1.1 The Dealer’s Protocol \( \pi^{3,7}_{ShareGen} \):

**Input.** The quantum secret to be shared using \((3,7)\) threshold secret sharing.

1.1.1 Share Generation: The dealer does the following:

- Chooses the \( r \) according to a geometric distribution \( G(\gamma) \) with parameter \( \gamma \).
- Generates three copies of each secret (fake as well as actual) for each round and encodes those in CSS code discussed above.
- Prepares a list \( \text{list}_i \) of shares for each party \( P_i \) such that:
  - Qubits \((5, 6, 7)\) of each secret are given to players \( P_1, P_2 \), and \( P_3 \) respectively so that each party gets three qubits, i.e. \( P_1 \) possesses three of 5, \( P_2 \) has three of 6 and \( P_3 \) possesses three of 7 for each round.
  - Each list contains \( 3(r + w) \) shares, where \( w \) is also chosen according to \( G(\gamma) \).

**Output.** The dealer distributes \( \text{list}_i \) to party \( P_i \).

1.1.2 Unmasking of Revelation Round \( \pi^{3,7}_{Unmask} \):

**Input.** Signal \( \text{sig}_i \) from each player \( P_i \), \( (i \in \{1, 2, 3\}) \).

**Computation and Communication.** The dealer does the following:

- If \( \text{sig}_1 = \text{sig}_2 = \text{sig}_3 = 1 \), announces the value of \( r \) to each \( P_i \).
- If for at least one value of \( i \), \( \text{sig}_i \neq 1 \), aborts after announcing abort to each party \( P_i \).

**Output.** The dealer outputs either \( r \) or abort depending on the values of \( \text{sig}_i \).

1.2 The Player’s Protocol

**Input.** The list of shares \( \text{list}_i \).

1.2.1 Secret Reconstruction \( \pi^{3,7}_{Recon} \):

**Computation and Communication.** Each player \( P_i \) does the following:

- In the ith sub-round of a round \( j \), \( P_i \) is given the current shares (qubits) by other two parties.
- Checks to see if the number of shares received is less than two. If yes, aborts and sends \( \text{sig}_i = 0 \) to dealer. Else, continues.
- At the end of round \( j \), does the following:
  - Applies CNOT gate considering his current share (qubit) as control.
  - Measures target bits in \([00, 01, 10, 11]\) basis.
  - Depending on the measured value operates either \( X \) gate or \( I \) gate.
- Stores the secret \( s_j \) obtained in the \( j \)th round.
- If \( j = \frac{1}{3} \lvert \text{list}_i \rvert \), sends \( \text{sig}_i = 1 \) to the dealer. If the dealer sends \( \text{abort} \), then aborts; else if the dealer sends the value of \( r \) stores only \( s_r \) and quits. If \( j < \frac{1}{3} \lvert \text{list}_i \rvert \), continues.

**Output.** The quantum secret \( s_r \).

IV. GENERALIZATION TO \((t, n)\) QUANTUM RATIONAL SECRET SHARING

Before going to the \((t, n)\) quantum rational secret sharing, first we show an existential result.

**Theorem 1.** Let \( C = [n, k, d] \) and \( C_1 = [n, k - 1, d'] \) be two linear codes such that \( C_1 \subset C \). Given \( C \cdot C_1^T = 0 \), there is always a secret sharing scheme provided \( k \) is a power of 2.

**Proof.** From the definition it is clear that we always construct a CSS code from given \( C \) and \( C_1 \) with codewords \( \lvert 0 \rvert_L \) and \( \lvert 1 \rvert_L \). Let the secret be \( \alpha \lvert 0 \rangle + \beta \lvert 1 \rangle \). Let us take the tensor product of the secret and \((m - 1)\) number of the ancilla states, where \( m \) is any integer value. The final state becomes \( \alpha \lvert 0_10_2 \ldots 0_m \rangle + \beta \lvert 1_10_2 \ldots 0_m \rangle \).

Applying CNOT gate we obtain \( \alpha \lvert 0_10_2 \ldots 0_m \rangle + \beta \lvert 1_10_2 \ldots 0_m \rangle \). This can be written in matrix form by a \( 2^m \) binary vector, \((100 \ldots 00)\). Similarly \( \lvert 1_10_2 \ldots 1_m \rangle \) can be represented by a \( 2^m \) binary vector, \((000 \ldots 01)\). In secret sharing scheme \( \lvert 0_10_2 \ldots 0_m \rangle \) and \( \lvert 1_10_2 \ldots 1_m \rangle \) are message states. Thus \( k = 2^m \) or \( m = \log_2 k \). As \( m \) is an integer, \( k \) should be power of 2. The encoded secret in CSS code becomes \( \alpha \lvert 1 \rangle_L + \beta \lvert 0 \rangle_L \).

The next result gives a bound on the number of parties that can reconstruct the secret.
Theorem 2. Let $C = [n, k, d]$ and $C_1 = [n, k - 1, d']$ be two linear codes such that $C_1 \subseteq C$. Given $C \cdot C_1^T = 0$, there are minimum $d$ number of parties who can reconstruct the secret.

Proof. According to the definition of the CSS code, $|0\rangle_L = \frac{1}{|C_1|} \sum_{x \in C_1} |x + C_1\rangle$ and $|1\rangle_L = \frac{1}{|C_1|} \sum_{x \notin C_1} |x + C_1\rangle$. Thus, the codewords which consist the codeword $|0\rangle_L$ belong to $C_1$. On the other hand, the codewords consisting the codeword $|1\rangle_L$ belong to $C/C_1$. So we always get two orthogonal codewords which come from two different cosets. One codeword is associated with $\alpha$ and other codeword is associated with $\beta$. Let they be $u$ and $v$. Since $\text{dist}(u - v) \geq d$, if we apply CNOT gate on these $d$ bits considering the first bit as control, we get $(d - 1)$ target bits which are equal in both the codewords. So measuring those $(d - 1)$ qubits in $\{0, 1\}^{d-1}$ basis we can reconstruct the secret depending on the measurement result. Thus, for secret reconstruction minimum $d$ parties have to collaborate.

Note that since $C_1 \subseteq C$, we must have $d' \geq d$. For $(t, n)$ QRSS, we set $t = d$.

A. $t$-out-of-$n$ Quantum Rational Secret Sharing Protocol

Let us now present our generalized scheme.

[2. Protocol $\pi_{\text{QRSS}}^{t,n}$]

2.1 The Dealer’s Protocol $\pi_{\text{ShareGen}}^{t,n}$

Input. The quantum secret to be shared using $(t, n)$ threshold secret sharing.

2.1.1 Share Generation: The dealer does the following:

- The dealer designates $t$ players among $n$, from the access structure.
- Chooses the $r$ according to a geometric distribution $G(\gamma)$ with parameter $\gamma$.
- Generates $t$ copies of each secret (fake as well as actual) for each round and encodes those in CSS code derived from $C$ and $C_1$ (see Theorem 2).
- Prepares a list $\text{list}_i$ of shares for each party $P_i$ such that:
  - Each player $P_i$ is given a qubit from a valid set of $t$ qubits from the access structure like $(3, 7)$ QRSS.
  - Each list contains $t(r + w)$ shares, where $w$ is also chosen according to $G(\gamma)$.

Output. The dealer distributes $\text{list}_i$ to party $P_i$.

2.1.2 Unmasking of Revelation Round $\pi_{\text{Unmask}}^{t,n}$

Input. Signal $sig_i$ from each player $P_i$, ($i \in [1, \ldots, t]$).

Computation and Communication. The dealer does the following:

- If $sig_i = 1$ for all $i \in [1, \ldots, t]$, announces the value of $r$ to each $P_i$.
- If for at least one value of $i$, $sig_i \neq 1$, aborts after announcing abort to each party $P_i$.

Output. The dealer outputs either $r$ or abort depending on the values of $sig_i$.

2.2 The Player’s Protocol

Input. The list of shares $\text{list}_i$.

2.2.1 Secret Reconstruction $\pi_{\text{Recon}}^{t,n}$

Each player $P_i$ does the following:

- In the $i$th sub-round of a round $j$, $P_i$ is given the current shares (qubits) by other $(t - 1)$ players.
- Checks to see if the number of shares received is less than $(t - 1)$. If yes, aborts and sends $sig_i = 0$ to dealer. Else, continues.

- At the end of round $j$, does the following:
  - Applies CNOT gate considering his current share (qubit) as control.
  - Measures target bits in $\{0, 1\}^{t-1}$ basis.
  - Depending on the measured value operates either $X$ gate or $I$ gate.

- Stores the secret $s_j$ obtained in the $j$th round.

If $j = \frac{1}{t}||\text{list}_i||$, sends $sig_i = 1$ to the dealer. If the dealer sends abort, then aborts; else if the dealer sends the value of $r$ stores only $s_r$ and quits. If $j < \frac{1}{t}||\text{list}_i||$, continues.

Output. The quantum secret $s_r$.

In the next result, we show that the fairness condition for classical domain remains valid in the quantum domain as well.

Theorem 3. If $\gamma > 0$ and $U_{TT}^{i} > \gamma U_{TN}^{i} + (1 - \gamma)U_{IN}^{i}$, the protocol $\pi_{\text{QRSS}}^{t,n}$ achieves fairness.

Proof. A player who wants to obtain the secret alone must be able to correctly guess which round is the revelation round. Suppose the $i$th player guesses that the $j$th round is the revelation round and quits in the $i$th sub-round of the $j$th round. On other words, the player remains silent in $(i - 1)$th sub-round of $j$th round. Our protocol is designed in such a way that if any player quits in any intermediate round, then it is reported to the dealer by a signal bit ($sig$). If for at least one value of $i$, $sig_i \neq 1$, the dealer aborts after announcing abort to each party $P_i$. Thus, if the guess of the $i$th player is correct i.e $j = r$, the probability of which is $\gamma_i$, his utility is $U_{TN}^{i}$, else his utility is $U_{IN}^{i}$. So the expected utility of the player who decides to deviate based on his guess is
given by $\gamma U_i^{TN} + (1 - \gamma)U_i^{NN}$. On the other hand, if he simply followed the protocol, his utility would have been $U_i^{TT}$. However, the dealer chooses the value $\gamma$ in such a way so that

$$\gamma U_i^{TN} + (1 - \gamma)U_i^{NN} < U_i^{TT}.$$ 

Thus the player should have no incentive to deviate. He always gives his share and hence the protocol achieves fairness.

The next result establishes the correctness of our general scheme.

**Theorem 4.** Even if some players may have $U_i^{NF} \geq U_i^{TT}$, the protocol $\pi^{t,n}_{QRSS}$ achieves correctness.

**Proof.** In our protocol, the dealer is semi-offline. The revelation round is unmasked by him after all the players report that the reconstruction game is over. Therefore, players do not depend on the action of the last player to know which round is the revelation round (see section IIIC). Thus, the protocol is $U_i^{NF}$ independent. No player has any incentive to quit in an intermediate round in the purpose to make the others believe in a fake secret as actual secret. Hence the protocol is correct. □

Note that in [2], it is mentioned that for non-simultaneous channel model, $U_i^{NF}$ independence is impossible. But there the underlying assumption is that the dealer is offline. Since in our QRSS, the dealer is semi-offline, we can easily get $U_i^{NF}$ independence even in non-simultaneous channel.

Now, we can state the following result on equilibrium.

**Theorem 5.** If $\gamma > 0$ and $U_i^{TT} \geq \gamma U_i^{TN} + (1 - \gamma)U_i^{NN}$, then protocol $\pi^{t,n}_{QRSS}$ achieves strict Nash equilibrium.

**Proof.** Let us assume that a party $P_i$ follows the deviating strategy $\sigma'_i$, when all other players follow the protocol. Suppose $P_i$ aborts at round $j$ and the revelation round is $r$. Then either $j$ is itself the revelation round, i.e., $r = j$ or it is a round before the revelation round, i.e. $r > j$. In our case, the secret reconstruction game is played until each party exhausts his list of shares. After that the dealer points out the revelation round. Hence, there is a possibility that $P_i$ deviates after the revelation round, i.e., $r < j$ although such deviation is not helpful in any way to the deviating party. We assume that the correct secret can be obtained by a player only when he quits in the revelation round. From the property of geometric distribution, we have

$$\gamma = \Pr[j = r | j \leq r] = \Pr[j = r] \text{ and } 1 - \gamma = \Pr[j < r | j \leq r] = \Pr[j < r].$$

Then, $u_i(\sigma'_i, \vec{\sigma}_{-i})$ is given by

$$U_i^{TN} \Pr[j = r] + U_i^{NN} \Pr[j < r] + U_i^{TT} \Pr[j > r] = \gamma U_i^{TN} \Pr[j \leq r] + (1 - \gamma)U_i^{NN} \Pr[j \leq r] + U_i^{TT} (1 - \Pr[j \leq r]) = (\gamma U_i^{TN} + (1 - \gamma)U_i^{NN} - U_i^{TT}) \Pr[j \leq r] + U_i^{TT} < U_i^{TT}.$$ 

The last inequality follows from our assumption that $\gamma U_i^{TN} + (1 - \gamma)U_i^{NN} < U_i^{TT}$, which makes the term added to $U_i^{TT}$ negative. In each sub-round, a player can send only a unique share (namely, the correct share) as we have $u_i(\sigma'_i, \vec{\sigma}_{-i}) < u_i(\vec{\sigma})$. So, our protocol follows strict Nash Equilibrium. □

In the classical rational secret sharing domain, Halpern and Teague [12] claimed that $(2, 2)$ rational secret sharing scheme cannot be constructed. Later, Gordon and Katz [3] showed a general $(t, n)$ rational secret sharing that works for $n = t = 2$, thus refuting the claim of [12]. Our $(t, n)$ quantum rational secret sharing scheme also works for $t = 2$. In that case, we require $[n, k, 2]$ linear code to construct the CSS code. In principle, $(2, n)$ QSS is the quantum analogue of $(2, 2)$ classical secret sharing, since in the quantum domain the dealer designates, from the access structures, a specific subset of 2 players (out of $n$) except whom no one else can obtain the secret.

## V. MAKING THE DEALER OFFLINE IN QRSS

In this section, we propose a $(t, n)$ quantum rational secret sharing scheme with the dealer offline, i.e., after distributing the shares, the dealer does not come into the picture.

Considering the dealer as semi-offline, we have shown that our protocol $\pi^{t,n}_{QRSS}$ becomes $U_i^{NF}$ independent and hence correct. In [2], it is shown that in case of offline dealer and non-simultaneous channel model, the protocol becomes $U_i^{NF}$ dependent. Hence achieving correctness is not guaranteed, when the preferences of the players are defined by $R_1$. Hence in case of offline dealer, to achieve correctness (which we show later), we suitably redefine the preferences of the players as follows:

$$R_2 : U_i^{TN} > U_i^{TT} > U_i^{NN} > U_i^{NF},$$

and

$$U_i^{NF} < U_i^{TT}$$

for all players $i$.

In our protocol $\pi^{t,n}_{QRSSDO}$ below, we use a Boolean indicator variable $b$ associated with each round. The secret bit $b$ is distributed among the designated $t$ parties through a $(t, t)$ Shamir secret sharing to denote whether the previous round was revelation round ($b = 1$) or not ($b = 0$). Later, we discuss how to move from classical indicator to quantum indicator.

### [3. Protocol $\pi^{t,n}_{QRSSDO}$]

#### 3.1 The Dealer’s Protocol $\pi^{t,n}_{ShareGen}$:

**Input.** The quantum secret to be shared using $(t, n)$ threshold secret sharing.

**3.1.1 Share Generation:** The dealer does the following:

- The dealer does the following:
Sets $t = d$ and designates $t$ players among $n$.

Chooses the $r$ according to a geometric distribution $\mathcal{G}(\gamma)$ with parameter $\gamma$.

Generates $t$ copies of each secret (fake as well as actual) for each round and encodes those in CSS code derived from $C$ and $C_1$ (see Theorem 2).

Prepares a list $\gamma_{\text{Recon}}$.

Depending on the measured value operates the CNOT gate.

Reconstructs the Boolean value associated with that round. In each sub-round $i$ of a round $j$, player $P_i$ reconstructs the qubit associated with that round. If it is $|0\rangle$, the player comes to know that the $(j-1)$th round was the revelation round. He reconstructs the secret for the $(j-1)$th round and discards other qubits obtained in the previous rounds.

Note that unlike the protocol for semi-offline dealer, the game will be over when the first player gets $1$ (in classical) or $|1\rangle$ (in quantum). He has no incentive to send his shares in subsequent sub-rounds. He then just quits the game. The rest of the players then conclude that the revelation round has been occurred just before that round. Thus they also get the secret by operating CNOT gate and measuring the target bits for the last complete round.

Unlike semi-offline dealer, in this case the players need not reconstruct the secret qubits for each round. Instead, they reconstruct the secret only for the revelation round. Moreover, the players are not forced to exhaust their lists of shares. The revelation round is the last round in this protocol as after the revelation round the players have no incentive to continue the game. The protocol is fair, correct and achieves strict Nash equilibrium.

Theorem 6. If $\gamma > 0$ and $U_i^{TT} > \gamma U_i^{TN} + (1 - \gamma)U_i^{NN}$, the protocol $\pi_{QRSSDO}^{t,n}$ achieves fairness.

The proof is the same as Theorem 3.

Theorem 7. Provided $U_i^{TT} > U_i^{NF}$, the protocol $\pi_{QRSSDO}^{t,n}$ achieves correctness.

Proof. As $U_i^{TT} > U_i^{NF}$, no player has any incentive to mislead others to believe in a wrong secret as an actual secret when he himself does not get the real secret. Thus the protocol is correct.

We show strict Nash equilibrium in the next result.

Theorem 8. If $\gamma > 0$ and $U_i^{TT} > \gamma U_i^{TN} + (1 - \gamma)U_i^{NN}$, then protocol $\pi_{QRSSDO}^{t,n}$ achieves strict Nash equilibrium.

Proof. Let us assume that a party $P_i$ follows the deviating strategy $\sigma'_i$, when all other parties follow the protocol. Suppose $P_i$ aborts at round $j$ and the revelation round is $r$. Then either $j$ is itself the revelation round, i.e., $r = j$ or it is a round before the revelation round, i.e., $r > j$. We assume that the correct secret can be obtained by a player only when he quits in the revelation round. From the property of geometric distribution, we have

\[
\gamma = \Pr[j = r | j \le r] = \frac{\Pr[j = r]}{\Pr[j \le r]}, \quad \text{and} \quad 1 - \gamma = \Pr[j < r | j \le r] = \frac{\Pr[j < r]}{\Pr[j \le r]}
\]

Then, $u_i(\sigma'_i, \sigma_{-i})$ is given by

\[
U_i^{TN} \Pr[j = r] + U_i^{NN} \Pr[j < r] = \gamma U_i^{TN} \Pr[j \le r] + (1 - \gamma) U_i^{NN} \Pr[j \le r] = (\gamma U_i^{TN} + (1 - \gamma) U_i^{NN}) \Pr[j \le r] < U_i^{TT}.
\]
The last inequality follows from our assumption that $\gamma U_{TT} + (1 - \gamma)U_{NN} < U_{TT}$. In each sub-round, a player can send only a unique share (namely, the correct share) as we have $u_i(\sigma'_i, \mathcal{F}_{-i}) < u_i(\mathcal{F})$. So, our protocol follows strict Nash Equilibrium.

Note that the proof in this case is a bit different from the proof in Theorem\cite{9} because the case $r < j$ does not occur here.

VI. CONCLUSION AND FUTURE WORK

Quantum secret sharing schemes either derived from QECC or teleportation do not succeed when we assume rational players. In this paper, for the first time we propose a new quantum rational secret sharing schemes that is fair, correct and achieves strict Nash equilibrium. Under this scheme, we propose two protocols, one with semi-offline dealer and the other with offline dealer. Semi-offline dealer appears twice 1) at the time of the share distribution, 2) at the end of the game. In the second protocol, we make the dealer offline by giving the players auxiliary information related to the revelation round.

The only disadvantage of the protocols is that they require quantum memory. Also, quantum no cloning theorem\cite{20} resists the players to copy their shares. So we let the dealer can prepare the copies of the secret as he knows the secret. Removing the requirement of the quantum memory is an interesting open problem.

In the classical rational secret sharing schemes, there are other notions of Nash equilibrium, such as computational Nash equilibrium under different adversarial models\cite{8,11,20,23}. Due to CSS code structure, no cloning and infinite range of the secret, the scenario is completely different in quantum setting and hence we consider only strict Nash equilibrium. Extended analysis of our protocol or its variants for alternative equilibrium models could be another potential future work.

[1] I. Abraham, D. Dolev, R. Gonen, J. Halpern. Proceedings of the 25th Annual ACM Symposium on Principles of distributed computing, New York, USA, 53–62, (2006).
[2] G. Asharov, Y. Lindell. Journal of Cryptology. 24, 157–202, (2010).
[3] G. R. Blakley. Managing Requirements Knowledge. International Workshop, Springer Berlin, Heidelberg, (2008).
[4] R. Cleve, D. Gottesman, H. K. Lo. Phys. Rev. Lett. 83, 648–651 (1999).
[5] C. Crepeau, D. Gottesman, A. Smith. EUROCRYPT 2005 LNCS 3494, 285–301 (2005).
[6] S. De, A. K. Pal. CANS 2013, LNCS 8257, 139–161 (2013).
[7] F. G. Deng, C. Li, Y. Li, P. Zhou, H. Zhou. Physics Rev. A 72, 043431 (2005).
[8] G. Fuchsbauer, J. Katz, D. Naccache. Proceedings of the 7th Conference on Theory of Cryptography, 419–436, Springer-Verlag, (2010).
[9] D. Gottesman and I. Chuang. arXiv [quant-ph] 0105032v2 (2001).
[10] J. Katz, D. Naccache. Advances in Cryptology - EUROCRYPT 2012, 81–98, Springer Berlin Heidelberg, (2012).
[11] J. Halpern, V. Teague. Proceedings of the 36th Annual ACM symposium on Theory of computing, 623–632, (2004).
[12] L. F. Han, H. F. Xu. Int. J. Theor. Phys. 51, 2540–2554, (2012).
[13] A. Groce, J. Katz. Advances in Cryptology - EUROCRYPT 2012, 81–98, Springer Berlin Heidelberg, (2012).
[14] J. Katz. Theory of Cryptography, 251–272, Springer Berlin Heidelberg, (2008).
[15] G. Kol, M. Naor. Proceedings of the 40th Annual ACM Symposium on Theory of Computing, 423–432, (2008).
[16] X. Li, D. -G. Feng. Computational and Information Science, LNCS 3314, 1054–1060 (2005).
[17] A. Lysyanskaya, N. Triandopoulos. Advances in Cryptology - CRYPTO’06, 180–197, (2006).
[18] A. Lysyanskaya, A. Segal. IACR Cryptology ePrint Archive : Report 2010/540, (2010).
[19] F. J. MacWilliams (Author), N. J. A. Sloane. The Theory of Error-Correcting Codes. North Holland Publishing Co., (1977).
[20] S. Muralidharan, S. Jain, P. K. Panigrahi. Opt. Commun. 284, 1082–1085 (2011).
[21] Y. Nie, M. Sang, Y. Li, J. Liu. Int. J. Theor. Phys. 50, 1367–1371 (2011).
[22] M. A. Nielsen and I. L. Chuang. Quantum Computation and Quantum Information, Cambridge University Press, 2004.
[23] S. J. Ong, D. V. Parkes, A. Rosen, S. Vadhan. Proceedings of the 6th Conference on Theory of Cryptography, 36–53, Springer-Verlag, (2009).
[24] N. Paul, J. V. Menon, S. Karamanchi, S. Muralidharan, P. K. Panigrahi. Quantum Inf. Process. 10, 619–632 (2011).
[25] K. Rietjens, B. Schoenmakers, P. Tuyls. IEEE ISIT 2005, Australia, 1598–1602 (2005).
[26] P. K. Sarvepalli, A. Klappenecker. arXiv [quant-ph] 0905.1661v1 (2009).
[27] A. Shamir. Communications of the ACM 22, 612–613, (1979).
[28] W. K. Wootters, W. H. Zurek. Nature 299, 802–803, (1982).
[29] Q. Y. Zhang, Y. B. Zhan. Int. J. Theor. Phys. 51, 3037–3044 (2012).
[30] M. Zhao, Z. Li, S. Fei, Z. Wang, X. Jost. J. Phys. A: Math. Theor. 44, 215302 (2011).
[31] S. B. Zheng. Phys. Rev. A 74, 054303 (2006).