Quantum Information Theoretical Analysis of Various Constructions for Quantum Secret Sharing

Karin Rietjens  
Dep. of Math. and Comp. Science  
Eindhoven University of Technology  
The Netherlands  
Email: k.p.t.rietjens@tue.nl

Berry Schoenmakers  
Dep. of Math. and Comp. Science  
Eindhoven University of Technology  
The Netherlands  
Email: berry@win.tue.nl

Pim Tuyls  
Information Security Systems  
Philips Research Eindhoven  
The Netherlands  
Email: pim.tuyls@philips.com

Abstract—Recently, an information theoretical model for Quantum Secret Sharing (QSS) schemes was introduced. By using this model, we prove that pure state Quantum Threshold Schemes (QTS) can be constructed from quantum MDS codes and vice versa. In particular, we consider stabilizer codes and the corresponding proof of their relation with QTS. Furthermore, we reformulate the Monotone Span Program (MSP) construction according to the information theoretical model and check the recoverability and secrecy requirement. Finally, we consider QSS schemes which are based on quantum teleportation.

I. INTRODUCTION

QSS schemes are used to share a quantum secret among a set of players such that only specific groups of players are able to reconstruct the secret (authorized sets), while all other groups have no information about the secret at all (unauthorized sets). The collection of unauthorized sets is called the adversary structure, which has the property that every subset of an unauthorized set is also unauthorized.

In [11], an information theoretical model for a QSS scheme was defined. This model is used throughout the rest of this paper and is repeated here. Suppose one wants to share a secret $S$ which is an element of a $q$-dimensional Hilbert space $\mathcal{H}_S$, where $q$ usually is a prime power. The elements $\{|0\rangle, |1\rangle, \ldots, |q-1\rangle\}$ form an orthonormal basis for $\mathcal{H}_S$ and we usually describe the state of the secret by its orthonormal decomposition $\rho_S = \sum_{i=0}^{q-1} \alpha_i |i\rangle \langle i|$. The reference system that purifies the state of $S$ is denoted by $R$ with corresponding Hilbert space $\mathcal{H}_R$. Finally, the secret is shared among a set of players $P = \{P_i, \ldots, P_n\}$ and the Hilbert space corresponding to a set $B \subseteq P$ is denoted by $\mathcal{H}_B$. The density matrix $\rho_B$ then describes the state of system $B$.

The model is defined as follows. We denote the mutual information between systems $R$ and $A$ by $I(R : A) = S(R) + S(A) - S(RA)$, where $S(A)$ is the Von Neumann entropy of the state $\rho_A$ of system $A$.

Definition 1: A QSS scheme realizing an adversary structure $A$ is described by a quantum operator which generates quantum shares from a quantum secret $S$ and distributes these among the players such that:

1) recoverability requirement: 
   for all $A \notin A$ we have that $I(R : A) = I(R : S)$;

2) secrecy requirement: 
   for all $B \in A$ we have that $I(R : B) = 0$.

A scheme that satisfies these conditions is called a perfect scheme. In a non-perfect scheme, some sets have some information about the secret, but not enough to recover it, i.e. $0 \neq I(R : B) < I(R : S)$ for some unauthorized set $B$.

In this paper, we investigate Quantum Threshold Schemes (QTS) and their relation with Quantum Error Correcting Codes (QECC). In [6], it was shown that a $(t, 2t - 1)$ QTS can be constructed from a $[[2t - 1, 1, t]]$ quantum code. Here, we give an information theoretical proof of this relation and also prove the reverse statement. In particular, we consider stabilizer codes and constructively show how these codes can be used for secret sharing. It is possible to compute the reduced density matrix of a subset of shares, by only making use of the properties of the stabilizer.

Furthermore, we reformulate the Monotone Span Program (MSP) construction [8] for a general adversary structure according to Definition 1. By directly computing the reduced density matrix of a set of shares, we verify that the recoverability and secrecy requirement are satisfied.

Finally, the construction of a non-perfect $(n, n)$ QTS using teleportation, as was proposed in [9], is reformulated in terms of the information theoretical model. We show that authorized sets satisfy the recoverability requirement, but unauthorized sets have some, but not enough, information about the secret.

II. PURE AND MIXED STATE QSS SCHEMES

In a pure state scheme, the encoding of a pure state of the secret is a pure state, while with a mixed state scheme the encoding of a pure state is sometimes a mixed state. In general, a QSS scheme is mixed, but it can be described as a pure scheme with one share discarded [7]. Therefore, it actually suffices to only consider pure state schemes, which have the following useful property. Part of it was previously considered in [11], but a full proof is given here.

Theorem 2: In a pure state QSS scheme, the recoverability requirement and the secrecy requirement are equivalent.

Proof: Suppose $P$ is the set of all players and let $A, B \subseteq P$ such that $B = P \setminus A$. Using the Araki-Lieb inequality and the fact that the systems $RS$ and $RAB$ are in a pure state, we have

$$I(R : S) - I(R : A) = I(R : B)$$  \hspace{1cm} (1)
and the theorem follows immediately.

Note that this also implies that in a pure state scheme, the authorized sets are precisely the complements of the unauthorized sets and vice versa. Moreover, this implies that a pure state \((t, n)\) QTS satisfies \(n = 2t - 1\).

III. QSS WITH QUANTUM MDS CODES

In the classical case, a linear \((t, n)\) threshold scheme over \(\mathbb{F}_q\) can be constructed from an \([n + 1, t, n + 2 - t]_q\) MDS code and vice versa [1]. We show that in the quantum case, a \([\lfloor 2t - 1, 1, t \rfloor]_q\) quantum MDS code can be used to construct a \(((t, 2t - 1))\) QTS and vice versa. As a special case, binary stabilizer codes are considered and the recoverability requirement is checked by directly computing the entropies of the reduced density matrices of a subset of shares.

A quantum code can correct for errors on a subsystem of the system of the codewords means that the operator that induces the errors is perfectly reversible. The quantum data processing inequality [3] gives a necessary and sufficient condition for a quantum operator to be perfectly reversible.

A different condition for quantum erasure correcting is given by Theorem 2. Cerf et al. [4] previously proved the necessity of this condition. First we need the following lemma, which is given without proof.

**Lemma 3:** Let \(A\) and \(B\) be two quantum systems. If \(A\) or \(B\) is in a pure state, then the composite system \(AB\) is in a product state.

**Theorem 4:** Let \(Q\) be a quantum system and let \(R\) be its reference system, such that \(RQ\) is in a pure state. Erasures can be corrected on some subsystem \(Q_e\) of \(Q\) if and only if \(I(\hat{R} : Q_e) = 0\).

**Proof:** Let \(Q = Q_uQ_e\) and suppose we can correct for erasures on \(Q_e\). This means that every quantum operator acting on \(Q_e\) and leaving \(Q_u\) invariant is perfectly reversible. Let \(E\) be a quantum operator that converts the system \(Q_e\) into an arbitrary pure state and let \(\rho_{R\ hat{Q}\ Q_e}\) be the system \(\rho_{RQ_e}\) after applying \(I \otimes I \otimes E\). Then \(\rho_{R\ hat{Q}\ Q_e}\) is in the product state \(\rho_{R\ hat{Q}\ Q_e} = S(RQ_u)Q_e = S(RQ_u) + S(Q_e)\). Analogously, we have \(S(Q_uQ_e) = S(Q_u) + S(Q_e)\). Furthermore, because of the quantum data processing inequality we have \(S(Q) = S(Q') - S(R'Q')\) and therefore

\[
0 = S(Q) - S(Q') + S(R'Q') = S(R) - S(Q_u) + S(RQ_u) + S(Q_e) = S(R) - S(RQ_e) + I(\hat{R} : Q_e),
\]

which completes the first part of the proof.

On the other hand, suppose \(I(\hat{R} : Q_e) = 0\) for some subsystem \(Q_e\) of \(Q\). Let \(E\) be a quantum operator acting on \(Q_e\). Then \(E\) has a representation as a unitary evolution on a larger system, say \(Q_eE\), where \(E\) is initially in a pure state. Let \(R'Q'E\) be the system \(RQE\) after this unitary evolution on \(Q_eE\) and leaving \(RQ_u\) invariant. Then because of the conservation rule for mutual information (see for example [10]) we have that

\[
I(R' : Q_e') = I(R : Q_e).
\]

Since \(E\) was initially in a pure state, we have (using Lemma 3)

\[
l(R : Q_e) = S(R) + S(Q_e) - S(RQ_e) = S(R) + S(Q) - S(RQ_e) - S(E) = I(R : Q_e).
\]

Furthermore, because of the strong subadditivity property for system \(R'Q'e'\) we have

\[
l(R' : Q'e') - l(R' : E') \geq 0,
\]

which implies that

\[
0 \leq l(R' : E') \leq l(R' : Q'e') = l(R : Q_e).
\]

Thus if \(I(R : Q_e) = 0\) then also \(I(R' : E') = 0\), which is equivalent to \(S(Q) = S(Q') - S(RQ')\) and therefore because of the quantum data processing inequality erasures can be corrected on \(Q_e\).

Now we have the tools to prove the general relation between quantum MDS codes and QTS.

**Theorem 5:** A \(((t, 2t - 1))\) QTS, where the secret is an element of a \(q\)-dimensional Hilbert space, can be translated into a \([\lfloor 2t - 1, 1, t \rfloor]_q\) quantum MDS code and vice versa.

**Proof:** Consider a \(((t, 2t - 1))\) QTS with system \(S\) of the secret, reference system \(R\) and system of the players \(P\). Then the secrecy requirement states that for every set of at most \(t\) players \(B\), we have \(I(R : B) = 0\). According to Theorem 2 we have that erasures can be corrected on the shares of any set of \(t - 1\) players. Hence, all possible sets of shares in \(P\) together form a \([\lfloor 2t - 1, 1, t \rfloor]_2\) QECC.

On the other hand, consider a \([\lfloor 2t - 1, 1, t \rfloor]_q\) quantum MDS code. We claim that each codeword can be the shares for a \(((t, 2t - 1))\) QTS. Indeed, if \(Q\) is the composite system of the codewords and \(R\) the reference system, then for every set \(Q_e\) of at most \(t - 1\) of the \(2t - 1\) subsystems of \(Q\) we have \(I(R : Q_e) = 0\) (Theorem 4). Hence, the secrecy requirement is satisfied. Moreover, because of Theorem 4 and the fact that a \(((t, 2t - 1))\) QTS is a pure state scheme, we also have that the recoverability requirement is satisfied.

**Stabilizer Codes**

We consider a \([\lfloor 2t - 1, 1, t \rfloor]_2\) quantum stabilizer code with stabilizer \(T\). We show that this code can be used to construct a \(((t, 2t - 1))\) QTS and verify the recoverability requirement, which is sufficient because the scheme is pure. First, we present the following technical lemma.

**Lemma 6:** Let \(W \in G_a\), where \(G_a\) denotes the Pauli group on \(n\) qubits, act on a composite quantum system \(Q = Q_1 \otimes Q_2\) and say \(W = W_1 \otimes W_2\), where \(W_1\) acts on system \(Q_i, i = 1, 2\). Suppose \(|\psi\rangle\) is a state of system \(Q\) that is stabilized by \(W\). If \(\rho_2 = tr_1(|\psi\rangle\langle\psi|)\), where \(tr_1\) is the trace over system \(Q_1\), then \(W_2\) and \(\rho_2\) commute with each other.
Proof: Let $A$ be an arbitrary quantum operator acting on the state space of system $Q_2$ and $tr_2$ the trace over system $Q_2$. Then we have
\[
tr_2(\rho_2 A) = tr_2 \left( tr_1(W|\psi\rangle\langle\psi|W^t)A \right) = tr_2 \left( W_2 \rho_2 W_2^t A \right),
\]
where we have used that the trace function is cyclic and the fact that $W_1^t W_1 = I$ if $W_1$ is a tensor product of Pauli matrices. Since this holds for any $A$ acting on the state space of system $Q_2$ we have that $\rho_2 = W_2 \rho_2 W_2^t$ which completes the proof.

Next let $T$ be generated by $\{G_1, \ldots, G_{2t-2}\}$ and let $\overline{X}$ and $\overline{Z}$ be the logical Pauli $X$ and $Z$ operators on the logical basis $\{|0_L\rangle, |1_L\rangle\}$ for the stabilizer code (see [10]). Then $\{G_1, \ldots, G_{2t-2}, \overline{X}, \overline{Z}\}$ forms a basis for the commutator $C(T)$ of $T$. Since an MDS code is pure [5], we have that $T$ has minimum distance $t + 1$ and $C(T)$ minimum distance $t$. This results in the following property, which we state here without proof.

**Lemma 7:** If we restrict the generators of $C(T)$ to at most $t - 1$ qubit positions, then the restricted generators of $C(T)$ remain independent.

We claim that the construction for the $((t, 2t-1))$ threshold scheme is given by the following isomorphism.

**Definition 8:** The mapping $V_{t,2t-1} : \mathbb{C}^2 \rightarrow (\mathbb{C}^2)^{\otimes 2t-1}$ is defined by
\[
V_{t,2t-1} (|\alpha_00\rangle + |\alpha_11\rangle) = |\alpha_00|_L + |\alpha_11|_L,
\]
where $\alpha_0, \alpha_1 \in \mathbb{C}$.

So if the secret is in state $\rho_S = |\alpha_00\rangle\langle0| + |\alpha_11\rangle\langle1|$, the state of the system of the shares $P$ is given by
\[
\rho_P = V_{t,2t-1} \rho_S V_{t,2t-1}^\dagger = |\alpha_00\rangle\langle0|_L + |\alpha_11\rangle\langle1|_L.
\]

The entropy of every possible subset of shares from $P$ is given by the following lemmas.

**Lemma 9:** Let $B \subseteq P$ with $|B| = t' \leq t - 1$. Then we have for the entropy of the state $\rho_B$ of system $B$\n\[
S(B) = t' \log 2.
\]

**Proof:** Suppose $B$ is a set of $t - 1$ qubits. Let $G_j'$ be the operator $G_j$ restricted to the qubit positions of $B$ for every $1 \leq j \leq 2t - 2$. Because of Lemma 6 these operators $G_j'$ are independent because of Lemma 7. Since $|0_L\rangle\langle0_L|$ and $|1_L\rangle\langle1_L|$ commute with $G_j'$ for every $j$ and also with $\overline{Z}$, we can write
\[
\rho_A^0 = tr_{A'}(|0_L\rangle\langle0_L|) = \frac{1}{2^t} I^{\otimes t} + \beta_0 R; \tag{12}
\]
\[
\rho_A^1 = tr_{A'}(|1_L\rangle\langle1_L|) = \frac{1}{2^t} I^{\otimes t} + \beta_1 R, \tag{13}
\]
where $R \in \{I, X, Y, Z\}^{\otimes t}$. This shows that $\rho_A$ is a set of independent operators, which would imply that $R = I^{\otimes t}$. Therefore, since $R$ and $\overline{X}$ are tensor products of Pauli matrices, $R$ anti-commutes with $\overline{X}$. Hence, because $\overline{X} tr_{A'}(|0_L\rangle\langle0_L|) \overline{X}^\dagger = tr_{A'}(|1_L\rangle\langle1_L|)$, we have that $\beta_0 = -\beta_1$.

Finally, by using the fact that $\alpha_0 + \alpha_1 = 1$, we are able to verify that the entropy of $\rho_A$ is given by Eq. (11), since $\rho_A$ has $2t-1$ eigenvalues equal to $1/2^t + \beta_0$ and $2t-1$ eigenvalues equal to $1/2^t - \beta_0$, because $R$ has $2t-1$ eigenvalues equal to $+1$ and $2t-1$ eigenvalues equal to $-1$. We also know that $\mathcal{S}(\rho_A^0) = \mathcal{S}(\rho_A^1) = (t - 1) \log 2$, since $|0_L\rangle\langle0_L|$ has zero entropy. Therefore, we have that $\beta_0 = \pm 1/2^t$. Analogously for $\beta_1$.

**Lemma 11:** Let $A \subseteq P$ with $|A| \geq t$. Then
\[
\mathcal{S}(A) = \mathcal{S}(S) + (2t - 1 - |A|) \log 2. \tag{14}
\]

**Proof:** Write $A = A_t \cup A'$, where $|A_t| = t$ and $|A'| = |A| - t' \leq t - 1$. Let $B = P \setminus A$. Then by using Lemmas 9 and 10 we have
\[
\mathcal{S}(A) \geq |\mathcal{S}(A_t) - \mathcal{S}(A')| = \mathcal{S}(S) + (2t - 1 - |A|) \log 2,
\]
\[
\mathcal{S}(S) = S(RB) \leq \mathcal{S}(S) + (2t - 1 - |A|) \log 2,
\]
which completes the proof.

Finally, we have the following.

**Theorem 12:** A $[[2t-1, 1, t]]$ binary stabilizer code can be used to share a secret according to a $((t, 2t-1))$ QTS.

**Proof:** Let $A, B = P$, such that $B = P \setminus A$ and $|A| \geq t$.
Then
\[
I(R : A) = \mathcal{S}(R) + \mathcal{S}(A) - \mathcal{S}(B) = 2\mathcal{S}(S) = I(R : S).
\]
Hence, the recoverability requirement is satisfied for any authorized set of shares of Eq. 9 and since the threshold scheme is pure, this completes the proof.

**IV. MONOTONE SPAN PROGRAM CONSTRUCTION**
In [8] it was shown how (classical) MSP can be used to construct a QSS scheme for a general access structure. We show that the recoverability and secrecy requirement are fulfilled for this construction.
We only consider the pure state case. The recoverability and secrecy requirement for the mixed scheme follow immediately from the entropies for the pure scheme.

Let $A$ be a self-dual adversary structure with corresponding MSP $(\mathbb{F}_q, M, q)$ (see [2]), where $q$ is a prime power, $M$ a $d \times e$ matrix over $\mathbb{F}_q$ with independent columns and $g$ a function that labels each row of $M$ with an element of $\{1, 2, \ldots, n\}$. Furthermore, by $\mathcal{H}$ we denote a $q$-dimensional Hilbert space and say the vectors that are labeled $\{a\}_{a \in \mathbb{F}_q}$ form an orthonormal basis for $\mathcal{H}^\otimes n$.

Consider the following isometry.

**Definition 13:** The mapping $V_M : \mathcal{H}^\otimes e \rightarrow \mathcal{H}^\otimes d$ is defined by

$$V_M \left( \sum_{i \in \mathbb{F}_q} \alpha_i |\psi_1^i \psi_2^i \ldots \psi_e^i \rangle \right) = \sum_{i \in \mathbb{F}_q} \alpha_i \left( \begin{pmatrix} \psi_1^i \\ \psi_2^i \\ \vdots \\ \psi_e^i \end{pmatrix} \right),$$

where $|\psi_1^i \psi_2^i \ldots \psi_e^i \rangle \in \mathcal{H}^\otimes e$ and $\alpha_i \in \mathbb{C}$ for every $i$, $1 \leq i \leq q$.

We show that this mapping can be used to share a secret according to a QSS with adversary structure $A$. Let the secret $S$ be an element of a $q$-dimensional Hilbert space $\mathcal{H}_S$ with orthonormal basis $\{|0\}, |1\}, \ldots, |q-1\}$. Again, $R$ denotes the reference system that purifies $S$ and $P$ denotes the system of the players. Let $I_R$ be the identity mapping on the system $R$. The encoding of the secret is then given by

$$|RP\rangle = (I_R \otimes V_M)(|RS\rangle \otimes |E\rangle),$$

where

$$|E\rangle = \frac{1}{\sqrt{q^{e-1}}} \sum_{a \in \mathbb{F}_q} |a\rangle$$

and $\{a\}_{a \in \mathbb{F}_q}$ is an orthonormal basis for $\mathcal{H}_E$, the Hilbert space corresponding to system $E$.

This means that if the state of $S$ is described by the density matrix $\rho_S$, which has orthonormal decomposition

$$\rho_S = \sum_{i \in \mathbb{F}_q} \alpha_i |i\rangle \langle i|,$$

then the state of the system of the shares $P$ together with the reference system $R$ is given by

$$|RP\rangle = \frac{1}{\sqrt{q^{e-1}}} \sum_{i \in \mathbb{F}_q} \sum_{a \in \mathbb{F}_q} \sqrt{\alpha_i} |i\rangle \otimes M \left( \begin{pmatrix} i \\ a \end{pmatrix} \right).$$

Finally, the dealer sends qudit $i$ to player $g(i)$ for $1 \leq i \leq d$.

Let $A$ be an authorized set and $B$ its unauthorized complement. To check the recoverability and secrecy requirement, we compute the entropy of system $A$ and $B$. By $M_A$ and $M_B$ we denote the rows of $M$ corresponding to $A$ and $B$ respectively, where $M_A$ has rank $l$ and $M_B$ rank $m$.

First, consider the following definition.

**Definition 14:** Let $B_i$ be the set of vectors $|i a_1 \ldots a_{e-1}\rangle$ such that

$$M_B(i, a_1, \ldots, a_{e-1})^\top = x,$$

where $i \in \mathbb{F}_q$, $a = (a_1, \ldots, a_{e-1})^\top \in \mathbb{F}_q^{e-1}$ and $x \in \text{im}(M_B)$. Then the vector $|\phi_x^i\rangle$ is defined by

$$|\phi_x^i\rangle = \frac{1}{\sqrt{q^{e-1} - 1}} \sum_{|a\rangle \in B_i} |M_A \left( \begin{pmatrix} i \\ a \end{pmatrix} \right)\rangle.$$ (21)

We claim that these vectors are the eigenvectors of the density matrix $\rho_A$ that describes the state of system $A$. To prove this, we need the next lemma.

**Lemma 15:** Consider two vectors $|\phi_x^i\rangle$ and $|\phi_x^{i'}\rangle$ for certain $i, i' \in \mathbb{F}_q$ and $x, x' \in \text{im}(M_B)$. Suppose there are vectors $|i a\rangle \in B_i^\otimes$ and $|i' a'\rangle \in B_i'^\otimes$ such that

$$|M_A \left( \begin{pmatrix} i \\ a \end{pmatrix} \right)\rangle = |M_A \left( \begin{pmatrix} i' \\ a' \end{pmatrix} \right)\rangle.$$

Then we have that $|\phi_x^i\rangle = |\phi_x^{i'}\rangle$. If there are no such vectors, then $\langle \phi_x^i | \phi_x^{i'} \rangle = 0$.

**Proof:** It is sufficient to show that with the assumptions above, we have that for every $i b\rangle \in B_i^\otimes$ there exist a vector $|i' b'\rangle \in B_i'^\otimes$ such that $|M_A(i b)\rangle = |M_A(i' b')\rangle$. This is fulfilled by setting $(i' b')(i, a') = (i, a) + (i, b)$.

The second part follows immediately from the fact that we labeled the vectors in such a way that they are orthonormal to each other.

**Lemma 16:** For every $i \in \mathbb{F}_q$ and $x \in \text{im}(M_B)$, $|\phi_x^i\rangle$ is an eigenvector of $\rho_A$, which has norm equal to 1.

**Proof:** The density matrix for subsystem $A$ is given by

$$\rho_A = \frac{\text{tr}_{RB} |RP\rangle \langle RP|}{\text{tr}_{RB} |RP\rangle \langle RP|} = \frac{1}{q^{e-1}} \sum_{i \in \mathbb{F}_q} \sum_{x \in \text{im}(M_B)} \sum_{|a\rangle \in B_i} |M_A \left( \begin{pmatrix} i \\ a \end{pmatrix} \right)\rangle \langle M_A \left( \begin{pmatrix} i \\ a \end{pmatrix} \right)| = \frac{1}{q^{e-1} - 1} \sum_{i \in \mathbb{F}_q} \sum_{x \in \text{im}(M_B)} |\phi_x^i\rangle \langle \phi_x^i|.$$ (22)

Since $M$ has independent columns and therefore its kernel only contains the all zero vector, the vectors $|\phi_x^i\rangle$ are correctly normalized. Because of Lemma 15, we have that the vectors $|\phi_x^i\rangle$ are all (not necessarily different) eigenvectors of $\rho_A$, which completes the proof.

In the next theorem, we compute the entropy of $\rho_A$ by calculating the eigenvalues of the eigenvectors of $\rho_A$.

**Lemma 17:** Let the matrix $M$ have $e$ independent columns and let the rank of matrices $M_A$ and $M_B$ be $l$ and $m$ respectively. Then we have

$$S(A) = S(S) + (m + l - e) \log q;$$

$$S(B) = (m + l - e) \log q.$$

**Proof:** Consider any vector $|\phi_x^i\rangle$ for $i \in \mathbb{F}_q$ and $x \in \text{im}(M_B)$. Because of Lemma 15 and the fact that the kernel of $M$ only contains the all-zero vector, this vector is repeated $q^{e-1}$ times in Eq. (22). Moreover, because of the properties of the MSP and the fact that $A$ is an authorized set, for all these $q^{e-1}$ vectors $|\phi_x^i\rangle$ we have that $i' = i$. Therefore, we have...
can write for $\rho_A$

$$
\rho_A = \frac{q^{m-l}}{q^m} \sum_i \alpha_i \sum_t |\phi_i^t\rangle\langle\phi_i^t|,
$$

(25)

where the vectors $|\phi_i^t\rangle$, with $1 \leq t \leq q^{m+l-c}$ and $1 \leq i \leq q$, are all different. Moreover, the vectors $|\phi_i^t\rangle$ are all eigenvectors of $\rho_A$, each with eigenvalue $\alpha_i/q^{m+l-c}$. Hence, it follows that the entropy of system $A$ is given by Eq. (23). The proof for the entropy of system $B$ is omitted here.

Finally, we have the following.

**Theorem 18:** For any adversary structure $A$, there exists a QSS realizing $A$.

**Proof:** We only prove the case that $A$ is self-dual, the scheme for the other adversary structures can be obtained from this one. In the case that $A$ is self-dual, consider the scheme given by Eq. (19). Let $A \subseteq P, A \notin \{A\}$ be an authorized set and $B = P \setminus A$. Then because of Lemma 17 we have

$$
I(R:S) = S(R) + S(S) - S(RS) = 2S(S);
$$

(26)

$$
I(R:A) = S(R) + S(A) - S(B) = 2S(S),
$$

where we have used the fact that systems $RS$ and $RAB$ are in a pure state. The secrecy requirement is equivalent to the recoverability requirement in this case, but can also be checked directly.

V. QSS USING TELEPORTATION

We verify the correctness of the $((n,n))$ QTS scheme using teleportation as was proposed in [9]. This is done by defining an equivalent scheme that does not use teleportation.

Let the state of the secret $S$ be given by the density matrix

$$
\rho_S = \alpha_0 |00\rangle\langle00| + \alpha_1 |11\rangle\langle11|,
$$

where $\alpha_0, \alpha_1 \in \mathbb{C}$. The state of $S$ together with its reference system $R$ is then given by

$$
|RS\rangle = \sqrt{\alpha_0} |00\rangle + \sqrt{\alpha_1} |11\rangle.
$$

(27)

Suppose the dealer $D$ and the $n$ players $P$ initially share the maximally entangled state

$$
|\psi\rangle_{DP} = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle).
$$

(28)

The first step in the teleportation scheme is that the dealer lets the secret interact with his part of the entangled state and then performs a Bell measurement on his two qubits. If he then communicates the (classical) outcome of this measurement to the players, they are able to obtain the state

$$
|RP\rangle = \sqrt{\alpha_0} |00\rangle + \sqrt{\alpha_1} |11\rangle.
$$

(29)

In [9] it was shown how the players can obtain the state of the secret if all of them cooperate. However, it was not analyzed what happens if a group of less than $n$ players cooperate. This is done here by formulating an equivalent protocol in terms of the information theoretical model. Let the isometry $V_{n,n}: \mathbb{C}^2 \rightarrow (\mathbb{C}^2)^{\otimes n}$ be defined by

$$
V_{n,n}(a|0\rangle + b|1\rangle) = a |0\rangle^{\otimes n} + b |1\rangle^{\otimes n},
$$

where $a, b \in \mathbb{C}$. The encoding of the secret by using teleportation is then equivalent to applying the mapping $I_R \otimes V_{n,n}$ to the system $RS$, where $I_R$ is the identity mapping on system $R$. However, the difference is, that with this mapping the dealer actually has to send quantum shares to the players, while otherwise he only has to perform a Bell measurement and sending two classical bits.

Next, we calculate the mutual informations in order to determine which sets of players are authorized. Let $P_i$ be the system of player $i = 1, 2, \ldots, n$. Then

$$
\rho_{P_i} = \alpha_0 |00\rangle\langle00| + \alpha_1 |11\rangle\langle11|,
$$

(30)

$$
\rho_{P_{i+1}} = \alpha_0 |00\rangle\langle00| + \alpha_1 |11\rangle\langle11|,
$$

(31)

$$
\rho_{P_{2i-2}} = \alpha_0 |00\rangle\langle00| + \alpha_1 |11\rangle\langle11|,
$$

(32)

hence the entropy of the system of an arbitrary set of players equals the entropy of the secret. For the mutual informations, we have

$$
I(R:P_1) = I(R:P_{12}) = \ldots = I(R:P_{12\ldots n-1}) = S(S);
$$

(33)

$$
I(R:P_{12\ldots n}) = S(S) < I(R:S);
$$

(34)

since $RP_{12\ldots n}$ is the only system with entropy not equal to $S(S)$, but equal to 0. Hence, a set of less than $n$ players has some information about the secret, but not enough to recover it, while all $n$ players together have enough information to recover the secret. Therefore, we have shown that this scheme is a non-perfect $((n,n))$ QTS.

REFERENCES

[1] R. J. McEliece and D. V. Sarwate, “On Sharing Secrets and Reed Solomon codes”, Comm. of the ACM 24(9), p. 583 – 584, 1981.

[2] M. Kautzher and A. Wigderson, “On Span Programs”, Proc. of Structure Complexity, p. 102-111, 1993.

[3] B. Schumacher and M. A. Nielsen, “Quantum Data Processing and Error Correction”, Phys. Rev. A 54(4), p. 2629, 1996; e-print quant-ph/0001087, 2000.

[4] E. M. Rains, “Nonbinary Quantum Codes”, e-print quant-ph/0001087, 2000.

[5] R. Cleve, D. Gottesman and H-K Lo, “How to share a Quantum Secret”, Phys. Rev. Lett. 83, p. 648, 1999; e-print quant-ph/9906025.

[6] D. Gottesman, “On the Theory of Quantum Secret Sharing”, e-print quant-ph/9911057, 1999.

[7] A. Smith, “Quantum Secret Sharing for General Access Structures”, e-print quant-ph/0001087, 2000.

[8] S. Bandopadhyay, “Teleportation and Secret Sharing with Pure Entangled States”, Phys. Rev. A 62, 012308, 2000; e-print quant-ph/0002023.

[9] M. A. Nielsen and I. L. Chuang, “Quantum Computation and Quantum Information”, Cambridge University Press, 2000.

[10] A. C. A. Nascimento, P. Tayls, A. Winter, H. Imai and J. Müller-Quade, “A Quantum Information Theoretical Model for Quantum Secret Sharing Schemes”, Quantum Information and Computation, Vol. 5, 1, 205, p. 68-79; e-print quant-ph/0311136, 2003.