

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
 k.p.t.rietjens@tue.nl

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

Pim Tuyls
 Information Security Systems
 Philips Research Eindhoven
 The Netherlands
 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 give a constructive 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 $\{|0\rangle, |1\rangle, \dots, |q-1\rangle\}$ form an orthonormal basis for \mathcal{H}_S and we usually describe the state of the secret by its orthonormal decomposition $\rho_S = \sum_{i \in \mathbb{F}_q} \alpha_i |i\rangle\langle i|$. 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 $P = \{P_1, \dots, P_n\}$ and the Hilbert space corresponding to a set $B \subseteq P$ is denoted by \mathcal{H}_B . The density matrix ρ_B then describes the state of system B . Finally, let $\mathcal{S}(A)$ denote the Von Neumann entropy of the state ρ_A of system A , defined as $\mathcal{S}(A) = -\text{tr}(\rho_A \log \rho_A) = -\sum_i \lambda_i \log \lambda_i$, where λ_i are the eigenvalues of ρ_A , and recall that the mutual information between systems R and A is defined as $I(R : A) = \mathcal{S}(R) + \mathcal{S}(A) - \mathcal{S}(RA)$.

Definition 1: A QSS scheme realizing an adversary structure \mathcal{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 $A \notin \mathcal{A}$ we have that $I(R : A) = I(R : S)$;

- 2) *secrecy requirement:*

for all $B \in \mathcal{A}$ 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 $[[2t-1, 1, t]]_k$ 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 $I(R : S) - I(R : A) = I(R : B)$ and the theorem follows. ■

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 $[[2t - 1, 1, t]]_q$ 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 erasures on a subsystem of the system of the codewords means that the operator that induces the erasures is perfectly reversible. In [3] it was shown how the quantum data processing inequality gives rise to a necessary and sufficient condition for a quantum operator to be perfectly reversible.

A different condition for quantum erasure correcting is given by Theorem 4. 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 $I(R : Q_e) = 0$.

Proof: Let $Q = Q_u Q_e$ and suppose we can correct for erasures on Q_e . Furthermore, let \mathcal{E} be a quantum operator that converts the system Q_e into an arbitrary pure state and let $\rho_{R'Q'_uQ'_e}$ be the system $\rho_{RQ_uQ_e}$ after applying $I \otimes I \otimes \mathcal{E}$. Then $\rho_{R'Q'_uQ'_e}$ is in the product state $\rho_{R'Q'_u} \otimes \rho_{Q'_e}$ (Lemma 3) and $\mathcal{S}(R'Q'_uQ'_e) = \mathcal{S}(R'Q'_u) + \mathcal{S}(Q'_e) = \mathcal{S}(RQ_u) + \mathcal{S}(Q'_e)$. Analogously, we have that $\mathcal{S}(Q_uQ'_e) = \mathcal{S}(Q_u) + \mathcal{S}(Q'_e)$. Furthermore, because of the condition for perfect error correction [3], we have $\mathcal{S}(Q) = \mathcal{S}(Q') - \mathcal{S}(R'Q')$ and therefore

$$\begin{aligned} 0 &= \mathcal{S}(Q) - \mathcal{S}(Q') + \mathcal{S}(R'Q') \\ &= \mathcal{S}(R) - \mathcal{S}(Q_uQ'_e) + \mathcal{S}(RQ_uQ'_e) \\ &= \mathcal{S}(R) - \mathcal{S}(Q_u) - \mathcal{S}(Q'_e) + \mathcal{S}(RQ_u) + \mathcal{S}(Q'_e) \\ &= \mathcal{S}(R) - \mathcal{S}(RQ_e) + \mathcal{S}(Q_e) = I(R : Q_e), \end{aligned}$$

which completes the first part of the proof.

On the other hand, suppose $I(R : Q_e) = 0$ for some subsystem Q_e of Q . Let \mathcal{E} be a quantum operator acting on Q_e . Then \mathcal{E} has a representation as a unitary evolution on a larger system, say $Q_e E$, where E is initially in a pure state. Let $R'Q'E'$ be the system RQE after this unitary evolution on $Q_e E$ and leaving RQ_u invariant. Then because of the

conservation rule for mutual information (see for example [10]) we have that

$$I(R' : Q'_e E') = I(R : Q_e E).$$

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

$$\begin{aligned} I(R : Q_e E) &= \mathcal{S}(R) + \mathcal{S}(Q_e E) - \mathcal{S}(RQ_e E) \\ &= \mathcal{S}(R) + \mathcal{S}(Q_e) + \mathcal{S}(E) - \mathcal{S}(RQ_e) - \mathcal{S}(E) \\ &= I(R : Q_e). \end{aligned}$$

Furthermore, because of the strong subadditivity property for system $R'Q'_e E'$ we have

$$I(R' : Q'_e E') - I(R' : E') \geq 0,$$

which implies that

$$0 \leq I(R' : E') \leq I(R' : Q'_e E') = I(R : Q_e).$$

Thus if $I(R : Q_e) = 0$ then also $I(R' : E') = 0$, which is equivalent to $\mathcal{S}(Q) = \mathcal{S}(Q') - \mathcal{S}(R'Q')$ and therefore because of the condition for perfect error correction, 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 $[[2t - 1, 1, t]]_q$ 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 $t - 1$ players B , we have $I(R : B) = 0$. According to Theorem 4, 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 $[[2t - 1, 1, t]]_q$ QECC.

On the other hand, consider a $[[2t - 1, 1, t]]_q$ 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 2 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 $[[2t - 1, 1, t]]_2$ 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 $W \in \mathcal{G}_n$, where \mathcal{G}_n 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_i acts on system $Q_i, i = 1, 2$. Suppose $|\psi\rangle$ is a state of system Q that is stabilized by W . If $\rho_2 = \text{tr}_1(|\psi\rangle\langle\psi|)$, where tr_1 is the trace over system Q_1 , then W_2 and ρ_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

$$\begin{aligned}\text{tr}_2(\rho_2 A) &= \text{tr}_2\left(\text{tr}_1(W|\psi\rangle\langle\psi|W^\dagger)A\right) \\ &= \text{tr}_2\left(W_2\rho_2W_2^\dagger A\right),\end{aligned}$$

where we have used that the trace function is cyclic and the fact that $W_1^\dagger W_1 = I$ 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 $\rho_2 = W_2\rho_2W_2^\dagger$ which completes the proof. \blacksquare

Next let T be generated by $\{G_1, \dots, G_{2t-2}\}$ and let \bar{X} and \bar{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 $\{G_1, \dots, G_{2t-2}, \bar{X}, \bar{Z}\}$ 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 mention 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 isometry.

Definition 8: The mapping $V_{t,2t-1} : \mathbb{C}^2 \rightarrow (\mathbb{C}^2)^{\otimes 2t-1}$ is defined by

$$V_{t,2t-1}(\gamma_0|0\rangle + \gamma_1|1\rangle) = \gamma_0|0_L\rangle + \gamma_1|1_L\rangle,$$

where $\gamma_0, \gamma_1 \in \mathbb{C}$.

So if the secret is in state $\rho_S = \alpha_0|0\rangle\langle 0| + \alpha_1|1\rangle\langle 1|$, the state of the system of the shares P is given by

$$\rho_P = V_{t,2t-1}\rho_S V_{t,2t-1}^\dagger = \alpha_0|0_L\rangle\langle 0_L| + \alpha_1|1_L\rangle\langle 1_L|.$$

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

Lemma 9: Let $B \subset P$ with $|B| = t' \leq t-1$. Then we have for the entropy of the state ρ_B of system B

$$\mathcal{S}(B) = t' \log 2.$$

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 all commute with ρ_B . Moreover, because of Lemma 7, the operators G'_j are still independent. Since ρ_B is a $2^{t-1} \times 2^{t-1}$ density matrix that commutes with $2t-2$ independent elements in \mathcal{G}_{t-1} we have that $\rho_B = 1/2^{t-1}I$. In general, for any set B of at most $t-1$ shares, say t' , we have that $\rho_B = 1/2^{t'}I$. \blacksquare

Lemma 10: Let $A \subset P$ with $|A| = t$. Then we have for the entropy of the state ρ_A of system A

$$\mathcal{S}(A) = \mathcal{S}(S) + (t-1) \log 2.$$

Proof: Consider a set A of t shares. Let G'_j, \bar{X}' and \bar{Z}' be the operators G_j, \bar{X} and \bar{Z} restricted to the qubit positions in A respectively for every $1 \leq j \leq 2t-2$. Then these $2t$ operators

are independent because of Lemma 7. Since $|0_L\rangle\langle 0_L|$ and $|1_L\rangle\langle 1_L|$ commute with G'_j for every j and also with \bar{Z}' , we can write

$$\begin{aligned}\rho_A^0 &= \text{tr}_{A^c}(|0_L\rangle\langle 0_L|) = \frac{1}{2^t}I^{\otimes t} + \beta_0 R; \\ \rho_A^1 &= \text{tr}_{A^c}(|1_L\rangle\langle 1_L|) = \frac{1}{2^t}I^{\otimes t} + \beta_1 R,\end{aligned}$$

where $R \in \{I, X, Y, Z\}^{\otimes t}, R \neq I^{\otimes t}$ and $0 < |\beta_0|, |\beta_1| \leq 1/2^t$. The operator R cannot commute with \bar{X}' , since then it would commute with $2t$ independent operators, which would imply that $R = I^{\otimes t}$. Therefore, since R and \bar{X}' are tensor products of Pauli matrices, R anti-commutes with \bar{X}' . Hence, because $\bar{X}' \text{tr}_{A^c}(|0_L\rangle\langle 0_L|)\bar{X}'^\dagger = \text{tr}_{A^c}(|1_L\rangle\langle 1_L|)$, we have that $\beta_0 = -\beta_1$.

Furthermore, ρ_A^0 has 2^{t-1} eigenvalues equal to $1/2^t + \beta_0$ and 2^{t-1} equal to $1/2^t - \beta_0$, because R has 2^{t-1} eigenvalues equal to $+1$ and 2^{t-1} equal to -1 . We also know that $\mathcal{S}(\rho_A^0) = \mathcal{S}(\rho_{A^c}^0) = (t-1) \log 2$, since $|0_L\rangle\langle 0_L|$ has zero entropy. Therefore, we have that $\beta_0 = \pm 1/2^t$. Analogously for β_1 .

Finally, using that $\alpha_0 + \alpha_1 = 1$, it follows that indeed $\mathcal{S}(A) = \mathcal{S}(S) + (t-1) \log 2$, since ρ_A has 2^{t-1} eigenvalues equal to $1/2^t(1+\alpha_0-\alpha_1)$ and 2^{t-1} equal to $1/2^t(1-\alpha_0+\alpha_1)$. \blacksquare

Lemma 11: Let $A \subseteq P$ with $|A| \geq t$. Then

$$\mathcal{S}(A) = \mathcal{S}(S) + (2t-1-|A|) \log 2.$$

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

$$\begin{aligned}\mathcal{S}(A) &\geq |\mathcal{S}(A_t) - \mathcal{S}(A')| \\ &= \mathcal{S}(S) + (2t-1-|A|) \log 2, \\ \mathcal{S}(A) &= \mathcal{S}(RB) \\ &\leq \mathcal{S}(R) + \mathcal{S}(B) \\ &= \mathcal{S}(S) + (2t-1-|A|) \log 2,\end{aligned}$$

which completes the proof. \blacksquare

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

$$\begin{aligned}I(R : A) &= \mathcal{S}(R) + \mathcal{S}(A) - \mathcal{S}(B) \\ &= 2\mathcal{S}(S) = I(R : S).\end{aligned}$$

Hence, since the threshold scheme is pure, this completes the proof. \blacksquare

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 \mathcal{A} be a self-dual adversary structure with corresponding MSP (\mathbb{F}_q, M, g) (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 $\{1, 2, \dots, n\}$. Furthermore, by \mathcal{H} we denote a q -dimensional Hilbert space and say the vectors that are labeled $\{|\mathbf{a}\rangle\}_{\mathbf{a} \in \mathbb{F}_q^n}$ 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

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

where $|\psi_1^i \psi_2^i \dots \psi_e^i\rangle \in \mathcal{H}^{\otimes e}$ and $\gamma_i \in \mathbb{C}$ 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 \mathcal{A} . Let the secret S be an element of a q -dimensional Hilbert space \mathcal{H}_S with orthonormal basis $\{|0\rangle, |1\rangle, \dots, |q-1\rangle\}$. 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

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

and $\{|\mathbf{a}\rangle\}_{\mathbf{a} \in \mathbb{F}_q^{e-1}}$ 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 ρ_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

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

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 . Due to space limitations, however, we provide details for system A only, the analysis for system B is similar. 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: For every $i \in \mathbb{F}_q$ and $\mathbf{x} \in \text{im}(M_B)$ define the set B_x^i by

$$B_x^i = \{ |i \mathbf{a}\rangle : M_B(i, \mathbf{a})^\top = \mathbf{x}, \mathbf{a} \in \mathbb{F}_q^{e-1} \}.$$

Then the vector $|\phi_x^i\rangle$ is defined by

$$|\phi_x^i\rangle = \frac{1}{\sqrt{q^{e-m-1}}} \sum_{|\mathbf{a}\rangle \in B_x^i} \left| M_A \begin{pmatrix} i \\ \mathbf{a} \end{pmatrix} \right\rangle.$$

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

Lemma 15: Let $i, i' \in \mathbb{F}_q$ and $\mathbf{x}, \mathbf{x}' \in \text{im}(M_B)$. Then

$$|\phi_x^i\rangle = |\phi_{\mathbf{x}'}^{i'}\rangle \Leftrightarrow i = i' \wedge \exists z \in \ker(M_A) [M_B z = \mathbf{x} - \mathbf{x}'].$$

Proof: \Rightarrow There exist vectors $|i, \mathbf{a}\rangle \in B_x^i, |i', \mathbf{a}'\rangle \in B_{\mathbf{x}'}^{i'}$ such that $M_A(i, \mathbf{a})^\top = M_A(i', \mathbf{a}')^\top$. Since A is authorized this implies that $i = i'$. Furthermore, say $\mathbf{z} = (i, \mathbf{a}) - (i', \mathbf{a}')$. Then $\mathbf{z} \in \ker(M_A)$ and $M_B z = \mathbf{x} - \mathbf{x}'$.

\Leftarrow The first coordinate of \mathbf{z} is 0, because A is authorized and $\mathbf{z} \in \ker(M_A)$. Hence, if $|i\mathbf{a}\rangle \in B_x^i$, then $M_A(i, \mathbf{a})^\top = M_A(i, \mathbf{a})^\top + M_A z = M_A(i, \mathbf{a}')^\top$, where $M_B(i, \mathbf{a}')^\top = M_B(i, \mathbf{a})^\top + M_B z = \mathbf{x} + \mathbf{x}' - \mathbf{x} = \mathbf{x}'$. Thus $|i\mathbf{a}'\rangle \in B_{\mathbf{x}'}^i = B_{\mathbf{x}'}^{i'}$, since $i = i'$ and the theorem follows. \blacksquare

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

Proof: The density matrix for subsystem A is given by

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

Since $|B_x^i| = q^{e-m-1}$, the vectors $|\phi_x^i\rangle$ have norm 1. Furthermore, if $|\phi_x^i\rangle \neq |\phi_{\mathbf{x}'}^{i'}\rangle$, it follows that $\langle \phi_x^i | \phi_{\mathbf{x}'}^{i'} \rangle = 0$, since if there would be $|i\mathbf{a}\rangle \in B_x^i, |i'\mathbf{a}'\rangle \in B_{\mathbf{x}'}^{i'}$ with $M_A(i, \mathbf{a})^\top = M_A(i', \mathbf{a}')^\top$, then $i = i'$ and $\mathbf{z} = (i - i', \mathbf{a} - \mathbf{a}') \in \ker(M_A)$ and $M_B z = \mathbf{x} - \mathbf{x}'$, which is impossible on account of Lemma 15. \blacksquare

In the next theorem, we compute the entropy of ρ_A by calculating the eigenvalues of the eigenvectors of ρ_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

$$\begin{aligned} \mathbf{S}(A) &= \mathbf{S}(S) + (m + l - e) \log q; \\ \mathbf{S}(B) &= (m + l - e) \log q. \end{aligned}$$

Proof: From Lemma 15 it follows that for all $\mathbf{z} \in \ker(M_A)$ we have that $|\phi_x^i\rangle = |\phi_{\mathbf{x} + M_B z}^i\rangle$ and all these vectors $\mathbf{x} + M_B z$ are different since $\mathbf{z} \notin \ker(M_B)$. Therefore, since $|\ker(M_A)| = q^{e-l}$ we can write for ρ_A

$$\rho_A = \frac{q^{e-l}}{q^m} \sum_i \alpha_i \sum_t |\phi_t^i\rangle \langle \phi_t^i|,$$

where the vectors $|\phi_t^i\rangle$, with $1 \leq t \leq q^{m+l-e}$ and $1 \leq i \leq q$, are all different. Moreover, the vectors $|\phi_t^i\rangle$ are all eigenvectors of ρ_A , each with eigenvalue α_i/q^{m+l-e} . Hence, the result for the entropy of system A follows. The proof for the entropy of system B is omitted here. ■

Finally, we have the following.

Theorem 18: For any adversary structure \mathcal{A} , there exists a QSS realizing \mathcal{A} .

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

$$\begin{aligned} I(R : S) &= \mathcal{S}(R) + \mathcal{S}(S) - \mathcal{S}(RS) = 2\mathcal{S}(S); \\ I(R : A) &= \mathcal{S}(R) + \mathcal{S}(A) - \mathcal{S}(B) = 2\mathcal{S}(S), \end{aligned}$$

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 $\rho_S = \alpha_0|0\rangle\langle 0| + \alpha_1|1\rangle\langle 1|$, where $\alpha_0, \alpha_1 \in \mathbb{C}$. The state of S together with its reference system R is then given by

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

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

$$|\psi\rangle_{DP} = \frac{1}{\sqrt{2}}(|\underbrace{00\dots 0}_n\rangle + |\underbrace{11\dots 1}_n\rangle).$$

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

$$|RP\rangle = \sqrt{\alpha_0}|0\underbrace{0\dots 0}_n\rangle + \sqrt{\alpha_1}|1\underbrace{1\dots 1}_n\rangle.$$

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

$$V_{n,n}(a|0\rangle + b|1\rangle) = a|\underbrace{0\dots 0}_n\rangle + b|\underbrace{1\dots 1}_n\rangle,$$

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 $i = 1, 2, \dots, n$. Then

$$\begin{aligned} \rho_{P_1} &= \alpha_0|0\rangle\langle 0| + \alpha_1|1\rangle\langle 1| \\ \rho_{P_{12}} &= \alpha_0|00\rangle\langle 00| + \alpha_1|11\rangle\langle 11| \\ &\vdots \\ \rho_{P_{12\dots n}} &= \alpha_0|0\dots 0\rangle\langle 0\dots 0| + \alpha_1|1\dots 1\rangle\langle 1\dots 1|, \end{aligned}$$

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

$$\begin{aligned} I(R : P_1) &= I(R : P_{12}) = \dots = \\ I(R : P_{12\dots n-1}) &= \mathcal{S}(S) \\ &< I(R : S); \\ I(R : P_{12\dots n}) &= 2\mathcal{S}(S) \\ &= I(R : S), \end{aligned}$$

since $RP_{12\dots n}$ is the only system with entropy not equal to $\mathcal{S}(S)$, 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), pp. 583–584, 1981.
- [2] M. Karchmer and A. Wigderson, "On Span Programs", *Proc. of Structure Complexity*, pp. 102–111, 1993.
- [3] B. Schumacher and M. A. Nielsen, "Quantum Data Processing and Error Correction", *Phys. Rev. A* 54(4), p. 2629, 1996.
- [4] N. J. Cerf and R. Cleve, "Information-theoretic Interpretation of Quantum Error-correcting Codes", *Phys. Rev. A* 57, p. 1477, 1998.
- [5] E. M. Rains, "Nonbinary Quantum Codes", e-print quant-ph/9703048, 1997.
- [6] R. Cleve, D. Gottesman and H-K Lo, "How to share a Quantum Secret", *Phys. Rev. Lett.* 83, p. 648, 1999.
- [7] D. Gottesman, "On the Theory of Quantum Secret Sharing", e-print quant-ph/9910067, 1999.
- [8] A. Smith, "Quantum Secret Sharing for General Access Structures", e-print quant-ph/0001087, 2000.
- [9] S. Bandyopadhyay, "Teleportation and Secret Sharing with Pure Entangled States", *Phys. Rev. A* 62, 012308, 2000.
- [10] M. A. Nielsen and I. L. Chuang, "Quantum Computation and Quantum Information", Cambridge University Press, 2000.
- [11] H. Imai, J. Müller-Quade, A. C. A. Nascimento, P. Tuyls, and A. Winter, "A Quantum Information Theoretical Model for Quantum Secret Sharing Schemes", *Quantum Information and Computation*, Vol. 5, 1, 2005, pp. 69–80.