

QUANTUM INFORMATION THEORETICAL ANALYSIS OF VARIOUS CONSTRUCTIONS FOR QUANTUM SECRET SHARING

Karin Rietjens * Berry Schoenmakers * Pim Tuyls †

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, the recoverability and secrecy requirement are checked for the Monotone Span Program (MSP) construction.

INTRODUCTION

QSS schemes are used to share a quantum secret among a set of players such that only *authorized* subgroups of players are able to reconstruct the secret, while all other subgroups (*unauthorized sets*) have no information about the secret at all. The collection of unauthorized sets is called the *adversary structure*.

We use the following notations. The unknown quantum secret S 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 $\varrho_S = \sum_{i \in \mathbb{F}_q} \alpha_i |i\rangle \langle i|$. 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 subset $B \subseteq P$ is denoted by \mathcal{H}_B . The density matrix ϱ_B then describes the state of system B .

The information theoretic model of [9] is defined as follows. Let $S(A)$ denote the Von Neumann entropy of state ϱ_A of system A , defined as $S(A) = -\text{tr}(\varrho_A \log \varrho_A) = -\sum_i \lambda_i \log \lambda_i$ where λ_i are the eigenvalues of ϱ_A , and recall that the mutual information between systems R and A is defined as $I(R : A) = S(R) + S(A) - S(RA)$.

* Technical University Eindhoven, Dept. of Mathematics and Computer Science, P.O. Box 513, 5600 MB Eindhoven, The Netherlands. k.p.t.rietjens@tue.nl, berry@win.tue.nl

† Philips Research Labs, Prof. Holstlaan 4, 5656 AA Eindhoven, The Netherlands. pim.tuyls@philips.com

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

$$\begin{aligned}\forall_{A \notin \mathcal{A}} I(R : A) &= I(R : S) \quad (\text{recoverability requirement}); \\ \forall_{B \in \mathcal{A}} I(R : B) &= 0 \quad (\text{secrecy requirement}).\end{aligned}$$

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 [6]. Therefore, it actually suffices to only consider pure state schemes, which have the following useful property.

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 systems RS and RAB are in a pure state, we have $I(R : S) - I(R : A) = I(R : B)$ and the theorem follows. ■

QSS WITH QUANTUM MDS CODES

Here, we show that a $[[2t-1, 1, t]]_q$ quantum MDS code can be used to construct a $((t, 2t-1))$ QTS and vice versa.

A quantum code can correct for erasures if the operator that induces the erasures is perfectly reversible. The quantum data processing inequality [2] gives a necessary and sufficient condition for perfect reversibility. A different condition for erasure correcting is given by Theorem 4. We use the following lemma.

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: We only give the proof for the second part, as the first part was already proven in [3]. Suppose $I(R : Q_e) = 0$ for some subsystem Q_e of $Q = Q_e Q_u$. 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 [8]) 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)

$$I(R : Q_e E) = S(R) + S(Q_e E) - S(RQ_e E) = I(R : Q_e).$$

Furthermore, the strong subadditivity property for system $R'Q'_e E'$ proves that

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

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 $S(Q) = S(Q') - S(R'Q')$ and therefore because of the quantum data processing inequality erasures can be corrected on Q_e . ■

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. 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 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 and show that this code leads to a $((t, 2t - 1))$ QTS.

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 $\rho_2 = \text{tr}_1(|\psi\rangle\langle\psi|)$, then W_2 and ρ_2 commute with each other.*

Proof: The proof follows from a symmetry argument. ■

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 [8]). 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 [4], we have that T has minimum distance $t + 1$ and $C(T)$ minimum distance t . This results in the following property.

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 QTS 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*

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

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

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

Lemma 9 *Let $B \subset P$ with $|B| = t' \leq t - 1$. Then*

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

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, the operators G'_j are still independent (Lemma 7). 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 $\rho_B = 1/2^{t'}I$. ■

Lemma 10 *Let $A \subset P$ with $|A| = t$. Then*

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

Proof: Consider a set A of t shares. Let G'_j , \overline{X}' and \overline{Z}' be the operators G_j , \overline{X} and \overline{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 \overline{Z} , we can write

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

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 \overline{X}' , since then it would commute with $2t$ 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 $\overline{X}' \text{tr}_{A^c}(|0_L\rangle\langle 0_L|) \overline{X}'^\dagger = \text{tr}_{A^c}(|1_L\rangle\langle 1_L|)$, 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 $\mathcal{S}(\varrho_A^0) = \mathcal{S}(\varrho_{A^c}^0) = (t - 1) \log 2$, since $|0_L\rangle\langle 0_L|$ has zero entropy. Therefore, we have that $\beta_0 = \pm 1/2^t$. Similarly, 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 $1/2^t(1 - \alpha_0 + \alpha_1)$. ■

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

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

Proof: Let $B = P \setminus A$ and $A = A_t \cup A'$, with $|A_t| = t$, $|A'| = |A| - t \leq t - 1$. Then, $\mathcal{S}(A) \geq |\mathcal{S}(A_t) - \mathcal{S}(A')| = \mathcal{S}(S) + (2t - 1 - |A|) \log 2 = \mathcal{S}(R) + \mathcal{S}(B) \geq \mathcal{S}(RB) = \mathcal{S}(A)$, using Lemmas 9, 10 and the Araki-Lieb and subadditivity inequalities. ■

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 $A, B \subset P$, with $B = P \setminus A$ and $|A| \geq t$. Then $I(R : A) = \mathcal{S}(S) + \mathcal{S}(A) - \mathcal{S}(B) = I(R : S)$. Since the scheme is pure, this completes the proof. ■

MONOTONE SPAN PROGRAM CONSTRUCTION

We reformulate the MSP scheme of [7] and verify the recoverability and secrecy requirement.

Let \mathcal{A} be a self-dual adversary structure with corresponding MSP (\mathbb{F}_q, M, g) (see [1]), 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 $\mathcal{H}^{\otimes n}$.

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

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

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 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 has orthonormal decomposition $\varrho_S = \sum_{i \in \mathbb{F}_q} \alpha_i |i\rangle\langle i|$, then we have

$$|RP\rangle = \frac{1}{\sqrt{q^{e-1}}} \sum_{i \in \mathbb{F}_q} \sum_{\mathbf{a} \in \mathbb{F}_q^{e-1}} \sqrt{\alpha_i} |i\rangle \otimes |M(i, \mathbf{a})^\top\rangle.$$

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. 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 .

Definition 14 *Let B_x^i be the set of vectors $|i a_1 \dots a_{e-1}\rangle$ such that*

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

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

$$|\varphi_x^i\rangle = \frac{1}{\sqrt{q^{e-m-1}}} \sum_{|i\mathbf{a}\rangle \in B_x^i} |M(i, \mathbf{a})^\top\rangle.$$

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 *Consider two vectors $|\varphi_x^i\rangle$ and $|\varphi_{x'}^{i'}\rangle$ for certain $i, i' \in \mathbb{F}_q$ and $\mathbf{x}, \mathbf{x}' \in \text{im}(M_B)$. Suppose there are vectors $|i \mathbf{a}\rangle \in B_x^i$ and $|i' \mathbf{a}'\rangle \in B_{x'}^{i'}$ such that*

$$|M(i, \mathbf{a})^\top\rangle = |M(i', \mathbf{a}')^\top\rangle.$$

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

Proof: It is sufficient to show that with the assumptions above, we have that for every $|i \mathbf{b}\rangle \in B_x^i$, there exist a vector $|i' \mathbf{b}'\rangle \in B_{x'}^{i'}$ such that $|M_A(i, \mathbf{b})^\top\rangle = |M_A(i', \mathbf{b}')^\top\rangle$. This is fulfilled by setting $(i', \mathbf{b}') = (i', \mathbf{a}') - (i, \mathbf{a}) + (i, \mathbf{b})$.

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 $\mathbf{x} \in \text{im}(M_B)$, $|\varphi_x^i\rangle$ is an eigenvector of ϱ_A , which has norm equal to 1.*

Proof: The density matrix for subsystem A is given by

$$\begin{aligned} \varrho_A &= \text{tr}_{RB} |RP\rangle\langle RP| \\ &= \frac{1}{q^m} \sum_{i \in \mathbb{F}_q} \alpha_i \sum_{\mathbf{x} \in \text{im}(M_B)} |\varphi_x^i\rangle\langle \varphi_x^i|. \end{aligned}$$

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

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*

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

Proof: Consider any vector $|\varphi_x^i\rangle$ for $i \in \mathbb{F}_q$ and $\mathbf{x} \in \text{im}(M_B)$. Because of Lemma 15 and the fact that the kernel of M only contains the all-zero vector, there are q^{e-1} vectors $|\varphi_{\mathbf{x}'}^{i'}\rangle$ equal to $|\varphi_x^i\rangle$, where $i' \in \mathbb{F}_q$, $\mathbf{x}' \in \text{im}(M_B)$. Moreover, because of the properties of the MSP and the fact that A is an authorized set, we have that $i' = i$ for all these q^{e-1} vectors. Therefore, we can write for ϱ_A

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

where the vectors $|\varphi_t^i\rangle$, with $1 \leq t \leq q^{m+l-e}$ and $1 \leq i \leq q$, are all different. Moreover, the vectors $|\varphi_t^i\rangle$ 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. ■

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

Proof: The recoverability and secrecy requirement can directly be verified using Lemma 17. ■

REFERENCES

- [1] M. Karchmer and A. Wigderson, "On Span Programs", Proc. of Structure Complexity, p. 102–111, 1993.
- [2] B. Schumacher and M. A. Nielsen, "Quantum Data Processing and Error Correction", Phys. Rev. A 54(4), p. 2629, 1996.
- [3] N. J. Cerf and R. Cleve, "Information-theoretic Interpretation of Quantum Error-correcting Codes", Phys. Rev. A 57, p. 1477, 1998.
- [4] E. M. Rains, "Nonbinary Quantum Codes", e-print quant-ph/9703048, 1997.
- [5] R. Cleve, D. Gottesman and H-K Lo, "How to share a Quantum Secret", Phys. Rev. Lett. 83, p. 648, 1999.
- [6] D. Gottesman, "On the Theory of Quantum Secret Sharing", e-print quant-ph/9910067, 1999.
- [7] A. Smith, "Quantum Secret Sharing for General Access Structures", e-print quant-ph/0001087, 2000.
- [8] M. A. Nielsen and I. L. Chuang, "Quantum Computation and Quantum Information", Cambridge University Press, 2000.
- [9] 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.