A Quantum Information Theoretical Model for Quantum Secret Sharing Schemes

Anderson Nascimento, Hideki Imai
Institute of Industrial Science, The University of Tokyo

In this contribution we introduce a quantum information theoretical model for quantum secret sharing schemes. We show that quantum information theory provides an unifying framework for the study of these schemes. We show a shorter proof that the size of the shares in a quantum secret sharing scheme must be at least as large as the secret itself, this result was first stated in [1].

I. A MODEL FOR QUANTUM SECRET SHARING SCHEMES

The quantum entropy of a quantum state X with a density matrix ρ is defined as$S(X) = Tr(-\rho\log\rho) = \sum_{1\leq j\leq m}\lambda_j\log\lambda_j$, here $\lambda_1,\ldots,\lambda_m$ are the eingenvalues of ρ. The quantum entropy can be interpreted as the average number of qubits necessary to describe a realization of the system X.

The quantum conditional operator and quantum conditional entropies are basic tools that will be used in our analysis [2] [3] [4] [5]. Let be a bipartite quantum system XY represented by a density matrix ρ_{XY} in the Hilbert space $\mathcal{H}_{XY} = \mathcal{H}_X \otimes \mathcal{H}_Y$. The subsystems X and Y will be represented by the partial traces $\rho_X = Tr_Y\rho_{XY}$ and $\rho_Y = Tr_X\rho_{XY}$. The conditional amplitude operator is defined as $\rho_{X|Y} = \lim_{n\to\infty}[\rho_{XY}^{1/n}(\mathbf{1}_X\otimes\rho_Y)^{-1/n}]^n$. With the conditional amplitude operator is straightforward to generalize the concept of conditional entropy to the quantum scenario. The quantum entropy of a quantum system X conditional on another quantum system Y is $S(X|Y) = Tr(-\rho_{XY}\log\rho_{X|Y})$. One can understand the quantum conditional entropy as the ignorance about the quantum system X when having full knowledge of Y. A nice point about this definition is that several well known properties of classical conditional entropies are valid in the new scenario.

In a quantum secret sharing protocol, a dealer D wants to share a quantum state $|X\rangle$ with a set of players $\mathcal{P}$ according to a given access structure Γ. The access structure Γ is a family that lists all the subsets of players that can recover the quantum secret $|X\rangle$. A secret sharing scheme is called perfect if the subsets not listed in Γ cannot have any information about $|X\rangle$. When $|\mathcal{P}| = w$ and $\Gamma = \{B \subseteq \mathcal{P} : |B| \geq t\}$ we say we have a $(t,w)-$threshold scheme.

In our model, the quantum secret $|X\rangle$ is chosen from a set of possible quantum secrets $\mathcal{X} = \{|X_1\rangle, |X_2\rangle, \ldots, |X_n\rangle\}$. Each quantum secret is assumed to lie in a n-dimensional Hilbert space $\mathcal{H}_n$. The *a priori* probability that the secret $|X_i\rangle$ is chosen is p_i. The quantum secret can thus be represented by the quantum mixture:$S = p_1|X_1\rangle + p_2|X_2\rangle + \ldots + p_n|X_n\rangle$.

The set of possible quantum shares given to a player P and any quantum state that he may posses is represented by another quantum mixture which, for simplicity of notation, is also denoted by P. For a given subset of players $A = \{P_1,\ldots,P_j\} \subseteq \mathcal{P}$, we define:$A = P_1\otimes P_2\otimes\ldots\otimes P_j$, where $\otimes$ stands for the tensor product and $P_1, P_2, \ldots, P_j$ are the quantum mixtures that represent the quantum shares given to the respective players.

A perfect quantum secret sharing scheme realizing an access structure Γ is the sharing of a quantum secret $S = p_1|X_1\rangle + p_2|X_2\rangle + \ldots + p_n|X_n\rangle$ among a set of players $\mathcal{P}$ such that:(1)For all $A \in \Gamma$ we have that $I(S:A) = S(S)$; For all $A \notin \Gamma$ we have that $I(S:A) = 0$. The item 1 means that when the players of an authorized subset put their shares together they can recover the quantum secret with certainty. The item 2 means that unauthorized groups have no information on the quantum secret S.

Lemma 1. *Let be an access structure Γ of any secret sharing scheme sharing a quantum secret S and two set of users A and B such that $A \notin \Gamma$, but $A \cap B \in \Gamma$. The inequality $S(B|A) \geq S(S)$ holds.*

Theorem 2. *In any secret sharing scheme realizing an access structure Γ for any subsets of players A and B such that $A \notin \Gamma$, but $A \cap B \in \Gamma$ it holds that $S(A) \geq S(S)$ where S is the secret being shared.*

Corollary 1. *If all the quantum secrets $X = \{|X_1\rangle, |X_2\rangle, \ldots, |X_n\rangle\}$ are equally probable $S(B) \geq \log n$, where n is the dimension of the quantum secrets $|X_i\rangle$.*

---

[1] D. Gottesman, On the Theory of Quantum Secret Sharing, LANL e-print, quant-ph/9910067

[2] N. J. Cerf, C. Adami, Negative entropy and information in quantum mechanics, Phys.Rev.Lett. 79 (1997) 5194

[3] N. J. Cerf, C. Adami, Quantum Information Theory of Entanglement and Measurement, Physica D120 (1998) 62-81

[4] N. J. Cerf, C. Adami, Entropic Bell Inequalities, Phys.Rev. A55 (1997) 3371

[5] N. J. Cerf, C. Adami, R. M. Gingrich, Quantum conditional operator and a criterion for separability, Phys.Rev. A60 (1999) 893-898