Quantum Secret Sharing with Maximally Mixed States

Mostafa Mansour | Dahbi Zakaria

m.mansour@usm.ac.ma | etriziko@gmail.com

Department of Physics

Polydisciplinary Faculty of Beni Mellal

University Sultan Moulay Slimane

1st Mediterranean Conference on Higgs Physics

23-27 September 2019 - Tanger (Morocco)

Abstract

In this work we build threshold quantum secret sharing schemes by using particular states that are maximally mixed across any arbitrary bipartition of the multi-qudit system. We introduce first multi-qudit disconnected states as states of a multi-qudit Hilbert space associated to a multi-qubit system of n non-interacting qudits. The interaction between qudits generates maximally entangled states. The multi-qudit entangled states are chosen to be maximally mixed with respect to any possible bipartition $(A \cup B)$ with $|A| < |B|$ of the whole system. The maximally mixed property of multi-qudit states will be used to share secret between the two sets A and B.

B. Maximally mixed multi-qubit states

We consider a multi-qudit physical lattice where all the qudits occupying the sites are disconnected and prepared in the ground state ($|+\rangle = \frac{1}{\sqrt{d}}\sum_{j=1}^{d-1}|j\rangle$. Then, the initial state of the physical lattice denoted $|\phi_{\vec{0}}\rangle$ can be considered as a cluster state without any connection between qudits and it is obtained as

$$|\phi_{\vec{0}}\rangle = |+,+,...,+\rangle = \frac{1}{\sqrt{d^n}} \sum_{k_1,k_2,...,k_n=0}^{d-1} |k_1, k_2, ..., k_n\rangle . \tag{6}$$

The corresponding separable density matrices $\sigma_{\vec{0}}$ write $\sigma_{\vec{0}} = |\phi_{\vec{0}}\rangle\langle\phi_{\vec{0}}| = \left[\frac{1}{d}\sum_{k_i,k_i'}^{d-1}|k_i\rangle\langle k_i'|\right]^{\otimes n}$. Now we consider a special dynamical evolution of the separable density matrices $\sigma_{\vec{0}}$. This dynamical evolution writes [5]

$$e^{+itH}\sigma_0 e^{-itH} = \sigma_0(t) \quad \text{with } H = \sum_{r<h}^{n} g_{rh}M_{rh} \text{ and } t = \pi(2l-q) \text{ with } q \in \mathbb{Z}/d\mathbb{Z} \text{ and } l \in \mathbb{N}. \tag{7}$$

The actions of the unitary operators M_{rh} on the computational basis are defined by $M_{rh}|k_1, \cdots, k_n\rangle = k_r k_h |k_1, \cdots, k_n\rangle$. The coupling constant g_{rh} entering in the expression of the Hamiltonian describing the multi-qubit system corresponds to the simplest qudit exchange between two sites. The resulting entangled density matrices denoted now $\rho_0 = \sigma_0(t)$ writes as

$$\rho_{\vec{0}} = |\Phi, n\rangle\langle\Phi, n| = \frac{1}{d^n} \sum_{k_1,...,k_n k_1',...,k_n'} \omega^{\sum_{r<h} p_{rh}(k_r k_h - k_r' k_h')} |k_1, ..., k_n\rangle\langle k_1', ..., k_n'| ; \text{ with } p_{rh} = q g_{rh}. \tag{8}$$

where the vector state $|\Phi, n\rangle$ is obtained as $|\Phi, n\rangle = \frac{1}{d^n}\sum_{k_1,...,k_n}\omega^{\sum_{r<h} p_{rh}k_r k_h}|k_1, ..., k_n\rangle$. In the following, we consider the splitting of the entire system into two subsystems; one subsystem $A_2 = \{k_{n-m+1}, ..., k_n\}$ containing any $m(1 \leq m \leq n-1)$ qudits and the other $A_1 = \{k_1, ..., k_{n-m}\}$ containing the remaining $(n-m) = s$ qudits. The density matrix associated to the subsystem A_2 is obtained by tracing out the qudits of the subsystem A_1

$$\rho_{A_2} = Tr_{A_1}(|\Phi, n\rangle\langle\Phi, n|) = \sum_{k_1,...,k_n} \langle k, ..., k_s|\Phi, n\rangle\langle\Phi, n|k_1, ..., k_s\rangle ; s = n - m. \tag{9}$$

Operating the partial trace, we get

$$\rho_{A_2} = \frac{1}{d^k} \sum_{k_1,...,k_s,k_{s+1}...k_n,k_{s+1}'...k_n'} \omega^{\sum_{j=s+1}^{n} k_1[p_{1j}(k_j-k_j')]}\omega^{\sum_{j=s+1}^{n} k_2[p_{2j}(k_j-k_j')]}... \tag{10}$$
$$... \omega^{\sum_{j=s+1}^{n} k_s[p_{sj}(k_j-k_j')]}\omega^{\sum_{i<j;i,j\neq\{1,...,s\}} p_{ij}(k_j-k_j')} |k_{s+1}, ..., k_n\rangle\langle k_{s+1}', ..., k_n'| .$$

Then, the entangled state $|\Phi, n\rangle$ is m-maximally mixed [6, 7] or equivalently, the reduced density matrix ρ_{A_2} for the subset A_2 is totally mixed, $\rho_{A_2} = \frac{1}{d^m}\mathbb{I}_{d^m}$ if and only if the $(n-m)$ vectors $(p_{i(s+1)}, p_{i(s+2)}, ..., p_{in})$ with $(0 \leq i \leq n-m)$ are linearly independent. We note at the end, that if $|\phi\rangle$ is a m-uniform maximally mixed and $|\psi\rangle = U|\phi\rangle$, where The operation U is a local unitary operation which preserves the amount of the entanglement in the states $|\phi\rangle$, then the basic entanglement properties of the entangled states $|\psi\rangle$ are encoded in the m-uniform maximally states of type $|\phi\rangle$.

Bibliography

[1] D. Gottesman, Phys. Rev. A 61, 042311 (2000)

[2] Adrian Keet, Ben Fortescue, Damian Markham, Barry C. Sanders, Phys. Rev. A 82, 062315 (2010)

[3] Helwig, W., Cui, W., Latorre, J. I., Riera, A., & Lo, H. K. (2012). Physical Review A, 86(5), 052335.

[4] Helwig, W., & Cui, W. (2013) arXiv preprint arXiv:1306.2536.

[5] M.Mansour, M.Daoud, IJMPB Vol. 31, No. 20, 1750132 (2017)

[6] A. J. Scott, Phys. Rev. A 69, 052330 (2004); M.Mansour, M.Daoud, , MPLA Mai 2019.

[7] M. Mansour, submitted IJQI.

A. Quantum secret sharing

Quantum teleportation is one of the strangest uses of entanglement. It allows distant parts to share a secret (quantum secret) [1, 2] from one part to the other. In a pure state $(k, 2k-1)$ threshold quantum secret sharing scheme [3, 4], the secret is encoded into a pure state that is distributed among an odd number of players $P = \{1, ..., 2k-1\}$ such that a subset $B \subset P$ of players is authorized if and only if the set contains more than half the players, $|B| \geq k$. Furthermore, a subset $B \subset P$ of players with less than k-players is always a forbidden set. More precisely, the dealer shares an unknown quantum state with a set of players such that authorized subgroups of players can recover the quantum state, where the role of the dealer D is assigned to one of the $2k-1$ parties of a maximally entangled state. The corresponding protocol is described as follows: the secret that the dealer will share with the other players is encoded in an arbitrary qudit given by

$$|S\rangle_D = \sum_{i=0}^{d-1} \alpha_i |i\rangle , \tag{14}$$

by combining the secret with a maximally entangled state, the dealer prepares a general state of the form

$$|S\rangle_D |\Phi, n\rangle . \tag{15}$$

Where $|\Phi, n\rangle$ is a maximally entangled state shared between the dealer and the $(n-1)$ players. The dealer gives a share to every player and measures after that his two qudits in the generalized Bell basis

$$|\psi_{mn}\rangle = \sum_j \omega^{jn} |j\rangle |j+m\rangle . \tag{16}$$

If the dealer informs the players of their measurement result (m, n), then only a set of players (the authorized set) can apply a correction operator to recover the secret.

C. QSS with maximally mixed states

In the following we consider a n-qudit entangled state

$$|\Phi, n\rangle = \frac{1}{\sqrt{d^n}} \sum_{k_1,...,k_n} \omega^{\sum_{r<h} p_{rh}k_r k_h} |k_1, ..., k_n\rangle , \tag{23}$$

which is maximally mixed with respect to bipartition $A_1|A_2$, where the sets A_1 and A_2 termed respectively unauthorized and authorized sets are given by $A_2 = \{k_1, ..., k_{m-1}\}$ and $A_1 = \{k_m, ..., k_n\}$. Following [3, 4], the (m-1)-maximally mixed state $|\Phi, n\rangle$ takes the form

$$|\Phi, n\rangle = \frac{1}{\sqrt{d^{m-1}}} \sum_{k_1,...,k_{m-1}} |k_1\rangle ... |k_{m-1}\rangle \otimes |\psi(k)\rangle_{A_1} ; \text{ where } |\psi(k)\rangle_{A_1} = \frac{1}{\sqrt{d^{n-m+1}}} \sum_{k_m,...,k_n} \omega^{\sum_{r<h} p_{rh}k_r k_h} |k_1, ..., k_n\rangle . \tag{24}$$

Satisfies $\langle|\psi(k)\rangle||\psi(k')\rangle\rangle = \delta_{kk'}$. To construct a threshold quantum secret sharing scheme, we note first the role of the dealer D will be assigned to the first qudit k_1 of A_2. The dealer posses a quantum secret described by an arbitrary qudit state (14) which will share with the other $(n-1)$ players $\{k_2, ..., k_n\}$ of the whole system. To do that he prepares the general state

$$|\Psi\rangle = |S\rangle_D |\Phi, n\rangle = \frac{1}{\sqrt{d^n}} \sum_{k_1,...,k_n} \alpha_i \omega^{\sum_{r<h} p_{rh}k_r k_h} |i\rangle_D |k_1, ..., k_n\rangle = \frac{1}{\sqrt{d^{m-1}}} \sum_{i,k_1,...,k_n} \alpha_i |i\rangle_D |k_1, ..., k_n\rangle |\psi(\tilde{k}, i)\rangle . \tag{25}$$

where $\langle|\psi(\tilde{k}, i)\rangle||\psi(\tilde{k'}, i')\rangle\rangle = \delta_{kk'}\delta_{ii'}$ and he distributes the player's qudits to them by a public channel. After that the dealer $\{k_1\} \equiv \{D\}$ measures her two qudits in the generalized *Bell* basis $|B_{lq}\rangle = \frac{1}{d}\sum_j \omega^{jl}|j\rangle|j+q\rangle$. The projection of the operator $|B_{lq}\rangle\langle B_{lq}|$ on the state $|\Psi\rangle$ gives

$$|B_{lq}\rangle\langle B_{lq}|\Psi\rangle = |B_{jq}\rangle \left(\sum_j \alpha_j \omega^{-jl} |\phi_j\rangle\right) ; \text{ where } |\phi_j\rangle = \frac{1}{\sqrt{d^n}} \sum_{k_2,...,k_n} \omega^{\sum_{r\geq 2} p_{1r}(j+q)k_r} \omega^{\sum_{2\geq r\geq h} p_{rh}k_r k_h} |k_2, ..., k_n\rangle . \tag{26}$$

Which is labeled entangled state and can be cast in the form

$$|\phi_j\rangle = \frac{1}{\sqrt{d^{m-2}}} \sum_{k_2,...,k_{m-1}} |k_2\rangle ... |k_{m-1}\rangle |\tilde{\phi}(k, j)\rangle ; \tag{27}$$

with $|\tilde{\phi}(k, j)\rangle = \frac{1}{\sqrt{d^{n-m+2}}}\sum_{k_2,...,k_n}\omega^{\sum_{r\geq 2} p_{1r}(j+q)k_r}\omega^{\sum_{2\geq r\geq h} p_{rh}k_r k_h}|k_m, ..., k_n\rangle$. The dealer informs the players of their measurement result (l, q), then a set of players (authorized players) apply a correction operator $U_{mn} = \mathbb{K}^{-nN_1^{-1}}\mathbb{Z}^{-mA_1^{-1}}$ to obtain the state

$$|\chi\rangle = \sum_j \alpha_j |O_j\rangle ; \text{ where } |O_j\rangle \cong \sum_{k_2,...,k_n} \omega^{\sum_{r\geq 2} p_{1r}(j+q)k_r} \omega^{\sum_{2\geq r\geq h} p_{rh}k_r k_h} |k_2, ..., k_n\rangle , \tag{28}$$

which is maximally mixed state. Then, the parts of the authorized set A_1 can perform a joint quantum operation to recover the secret $|S\rangle = \sum_j \alpha_j |i\rangle_j$.

Conclusion

One application for k-uniform maximally mixed multi-qubit states is to construct quantum secret sharing (QSS) protocols. In a quantum secret sharing protocol, a secret is encoded into a quantum state shared between n players P such that certain subsets of P, the *authorized* sets, are able to recover the secret by performing joint quantum operations. In the detailed work [7] we have described quantum secret sharing protocols and we have constructed threshold quantum secret sharing schemes by using particular states that are maximally mixed across any arbitrary bipartition.