Ming Hsieh Department of Electrical Engineering

USC Viterbi School of Engineering

M. Marvian, V. Karimipour
Sharif University of Technology

Quantum Secret Sharing & Benchmarking DW-1

Milad Marvian

Daniel Lidar's Group

Quantum Secret Sharing

We provide a secure quantum carrier for distributing a secret (classical symbol encoded into a state or a quantum state) among n parties according to a (k, n) threshold scheme, where 2k − 1 is a prime number.

- Re-usable quantum carrier
- Make use of the results of every round
- Predetermined message can be sent securely

Quantum Carrier: 

(2,3) Scheme, Basic properties

Using this encoding each two participants can retrieve the secret:

$$0 \to |\bar{0}\rangle = |000\rangle + |111\rangle + |222\rangle$$
$$1 \to |\bar{1}\rangle = |012\rangle + |120\rangle + |201\rangle$$
$$2 \to |\bar{2}\rangle = |021\rangle + |102\rangle + |210\rangle.$$

Using CNOT gates

$$\mathcal{C}^0_{a,1}\mathcal{C}^1_{a,2}\mathcal{C}^2_{a,3}|i\rangle_a|\bar{s}\rangle_{1,2,3} = |i\rangle_a|\overline{i+s}\rangle_{1,2,3}$$

$$\mathcal{C}_{b_1,1}\mathcal{C}_{b_2,2}\mathcal{C}_{b_3,3}|\bar{i}\rangle_{a,b,c}|\bar{s}\rangle_{1,2,3} = |\bar{i}\rangle_{b_1,b_2,b_3}|\overline{i+s}\rangle_{1,2,3}$$

Performing Hadamard gate ($H|j\rangle = \sum_k \xi^{jk}|k\rangle$ with $\xi = e^{\frac{2\pi i}{3}}$)

We have:

$$H^{\otimes 3}|\bar{s}\rangle = \sum_x \xi^{-sx}|\bar{x}\rangle$$

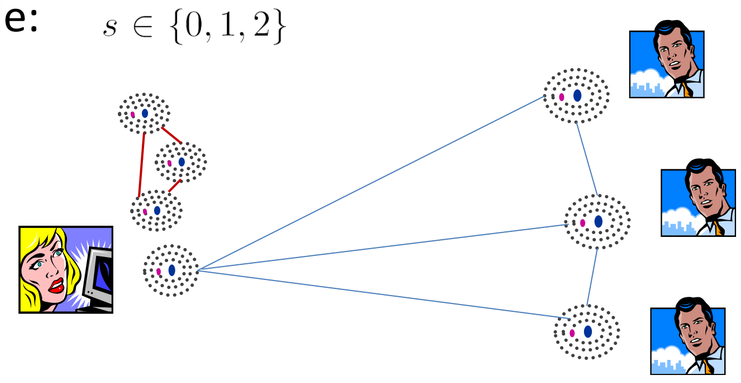
So, on our Carrier:

$$|\Phi\rangle = \sum_i |i\rangle_A|\bar{i}\rangle_{B_1,B_2,B_3}$$

$$H^{\otimes 4}|\Phi\rangle = |\Phi\rangle$$

Scheme

I) Alice chooses the classical secret and prepares the quantum code: $s \in \{0,1,2\}$



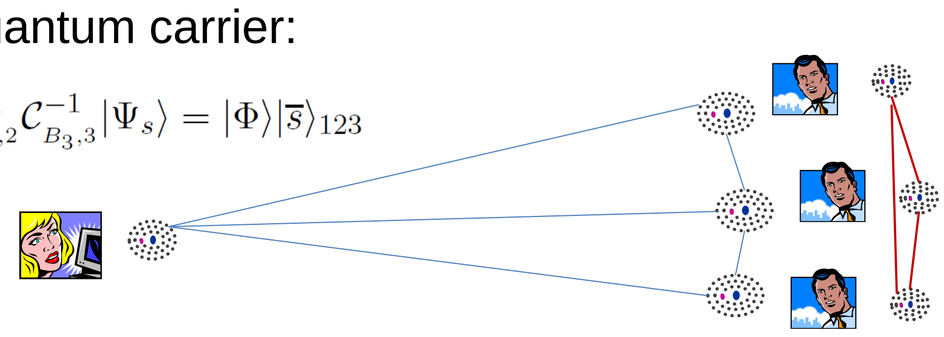
II) Alice hooks the quantum code to the quantum carrier:

$$|\Psi_s\rangle = \mathcal{C}^0_{A,1}\mathcal{C}^1_{A,2}\mathcal{C}^2_{A,3}|\Phi\rangle|\bar{s}\rangle_{123} = \sum_{i=0}^{2}|i\rangle_A|\bar{i}\rangle_{B_1B_2B_3}|\overline{i+s}\rangle_{123}$$

And sends the qutrits to the participants.

III) Each participant locally unhooks his qutrit from quantum carrier:

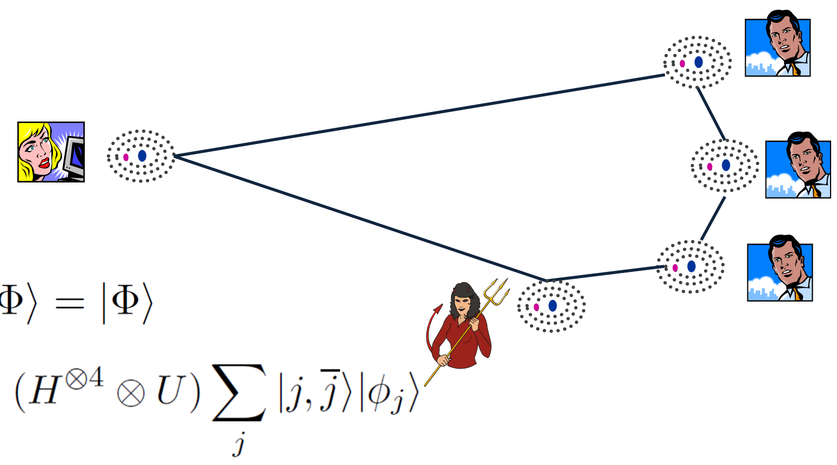
$$\mathcal{C}^{-1}_{B_1,1}\mathcal{C}^{-1}_{B_2,2}\mathcal{C}^{-1}_{B_3,3}|\Psi_s\rangle = |\Phi\rangle|\bar{s}\rangle_{123}$$



IV) Participants measure locally. With collaboration of each two of them the secret can be retrieved.

V) Alice and participants perform Hadamard gates.

Security



$$H^{\otimes 4}|\Phi\rangle = |\Phi\rangle$$

$$|\Phi'\rangle = (H^{\otimes 4} \otimes U)\sum_j |j,\bar{j}\rangle|\phi_j\rangle$$

Betray of a participant:

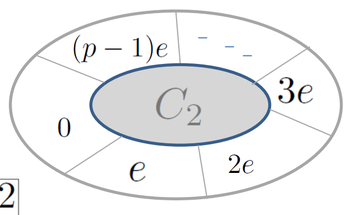
$$\sum_{i,j}|i,j+i,j+2i,j\rangle_{A,B_1,B_2,B_3}|\phi_j\rangle_{B'_3}$$
$$\rho_{B_3,B'_3,1,2,3} = \sum_j |j\rangle\langle j|_{B_3} \otimes |\phi_j\rangle\langle\phi_j|_{B'_3} \otimes \sum_i |\overline{i+s}\rangle\langle\overline{i+s}|$$

Scheme

Using CSS codes: $C_2 \subset C_1$ $k_1 - k_2 = 1$

$$|\overline{\mathbf{w}}\rangle = \frac{1}{\sqrt{p^{k_2}}}\sum_{\mathbf{c}_2\in C_2}|\mathbf{c}_2+\mathbf{w}\rangle \qquad \mathbf{w}\in C_1 \qquad \mathbf{w} = \mathbf{v} + i\mathbf{e}$$

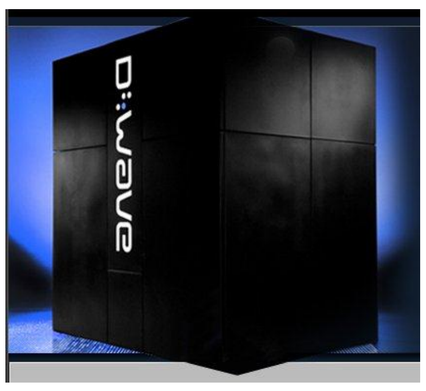
$$|\bar{\mathbf{i}}\rangle = \sum_{\mathbf{v}\in C_2}|\mathbf{v}+i\mathbf{e}\rangle$$

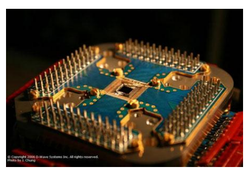


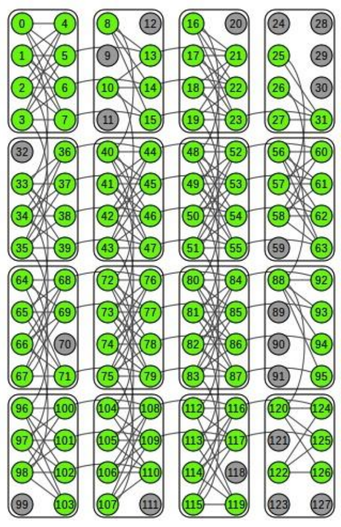
$$\begin{aligned}&\mathbf{e}_i\cdot\mathbf{e}_j = 0 \quad 1\le i,j\le k-2\\ &\mathbf{e}\cdot\mathbf{e}_j = 0 \quad 0\le j\le k-2\\ &\mathbf{e}\cdot\mathbf{e} = -1 \quad .\end{aligned}$$

Ref: http://arxiv.org/abs/1007.2778,In Press(IJQI)

D-Wave one Benchmarking







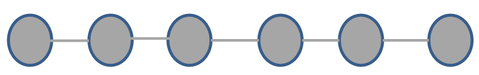
Quantum Adiabatic evolution:

$$H(t) = A(t)\sum\sigma_x + B(t)H_{Ising\ model}$$

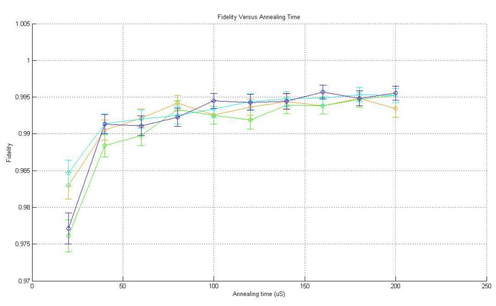
Input & output: h & J Matrices $S_i \in \{-1,1\}$

$$finding\ S^*:\ argmin_{\boldsymbol{s}}\{\sum h_i S_i + \sum J_{i,j}S_iS_j\}$$

1D Ising model



$$H = -J\sum g\hat{\sigma}_i^x + \hat{\sigma}_i^z\hat{\sigma}_i^z$$



Exact spectrum $\varepsilon_k = 2J\sqrt{(1+g^2-2gcos(k))}$

$$k \propto \frac{\pi}{N}$$