# CO781 / QIC890 Lec 04, Sept 20, 2016

3 further comments on TP, qbits & nonsignaling:

① Connection between TP & quantum encryption QEnc

② An example of "non-composable-qbit":

remote state preparation

③ Beyond QM ....

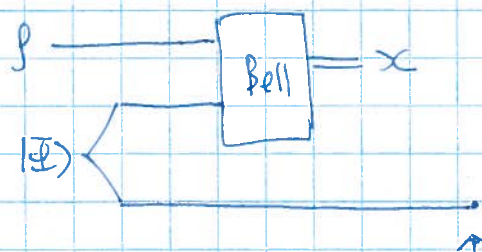
References:


① Ambainis-Mosca-Tapp-de-Wolf 2000, Boykin-Roychowdhury 00, Leung-Shor 2002

② Lo 99, Bennett-DiVincenzo-Shor-Smolin-Terhal-Wootters 00, Devetak 01, Leung-Shor 02, Bennett-Hayden-Leung-Shor-Winter 03

## Connection between TP & QEnc :

Recall TP :




state $= \sigma_x \rho \sigma_x^\dagger$

By evaluating Bob's state before receiving $x$ :

$$\underbrace{\frac{I}{2}}_{\text{Half of } |\Phi\rangle} = \underbrace{\frac{1}{4}}_{\text{prob of each } x} \sum_x \underbrace{\sigma_x \rho \sigma_x^\dagger}_{\substack{\text{state conditioned} \\ \text{on message} = x.}}$$

This gives an encryption scheme QEnc :

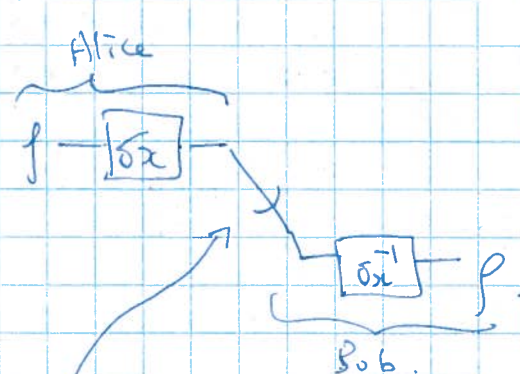
Alice and Bob share a secret key $x$,

$\forall x \in \{0,1,2,3\}$, $\Pr(x) = \frac{1}{4}$.

Alice applies $\sigma_x$ to $\rho$

She transmits $\sigma_x \rho \sigma_x^\dagger$ to Bob.

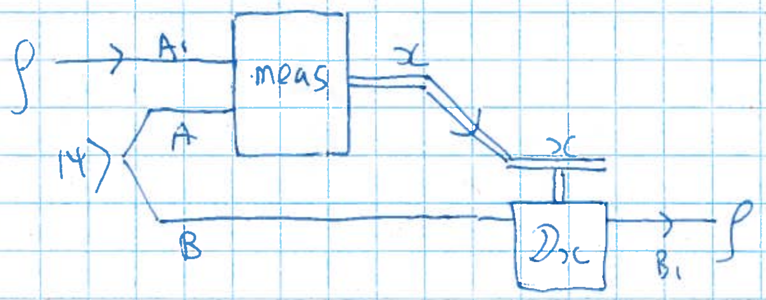
Bob decodes by inverting $\sigma_x$.




An eavesdropper without knowledge of $x$ sees $\mathcal{E}(\rho) = \frac{1}{4}\sum_x \sigma_x \rho \sigma_x^\dagger = \frac{I}{2}$

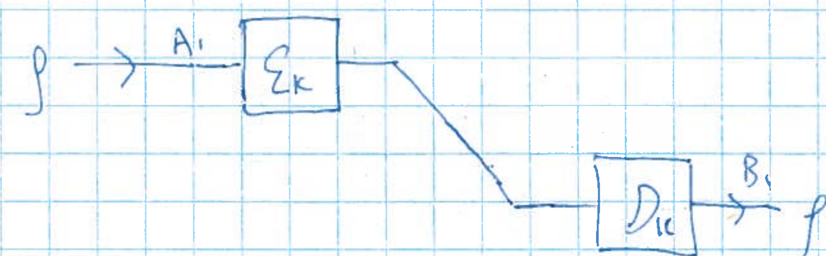
that is independent of $\rho$.

• Consider generalized Teleportation (using entanglement & cbits to achieve qbits):




(NB: meas indep of $\rho$)
$(A, B : d'\text{-dim})$
($\rho$: d dim, $d \le d'$)
part of $|\phi\rangle_{RA_1}$

• Consider generalized encryption (using secret key & qbits to achieve private q. comm):




Alice & Bob share a key $K$ where $p_K = \text{prob}(K=k)$.

To communicate $\rho$ to Bob:

Alice applies $\mathcal{E}_k$ and sends $\mathcal{E}_k(\rho)$ to Bob, and

Bob applies $D_k$ to retrieve $\rho$, such that:

① $\forall k \quad D_k \mathcal{E}_k = I$ (correctness)

② $R(\rho) := \underbrace{\sum_k p_k \, \mathcal{E}_k(\rho)}_{\text{what Eve can see without knowing } k} = \rho_0$ (indep of $\rho$)

eg. $\mathcal{E}_k(\rho) = \sigma_k \rho \sigma_k^\dagger$, $\rho_0 = \frac{I}{2}$

Natural correspondences:

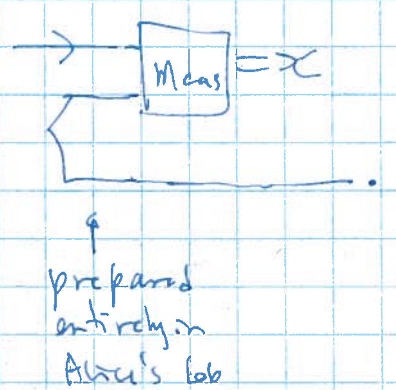
| Generalized teleportation: | Generalized q. encryption: |
|---|---|
| Measurement outcome $x$<br>Sent via given cbits | Key $k$<br>pre-shared secret |
| Bob's half of ent state | The state being eavesdropped |
| Bob's state upon receiving $x$<br>$\rho_x$ | The state transmitted knowing $k$.<br>$\mathcal{E}_k(\rho)$. |

- Consider exact schemes (will return to this issue).

Thm 1: given any generalized teleportation protocol TP' for transmitting any $d$-dim q state using an entangled state $|\psi\rangle$ with local dim $d'$ and transmitting a message $x \in \{1, 2, \ldots, m\}$, there is an encryption scheme QEnc' using a key $K \in \{1, 2, \ldots, m\}$ and $\log d'$ qbits.

Pf: We need to find $\mathcal{E}_x$ for the encryption scheme:

A tempting idea that doesn't work:




$$\sum_x p_x \, |x\rangle\langle x| \otimes \mathcal{E}_x(\rho).$$

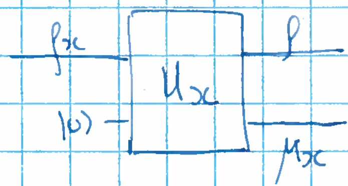
Problem: Alice cannot control the outcome $x$, and that is NOT her key shared with Bob.

Idea that works:

Consider Bob's decoding operation in the given TP':

$$\forall x: \quad \underset{\rho_x}{\overset{d'\text{ dim}}{\longrightarrow}} \boxed{D_x} \underset{\rho}{\overset{d\text{ dim}}{\longrightarrow}} \qquad \text{and} \quad \sum_x p_x \, \rho_x = \mathrm{Tr}_A \, |\psi\rangle\langle\psi|.$$

Using the isometric extension of $D_x$, $\exists$ unitary $U_x$, $\exists$ state $\mu_x$ s.t.




Furthermore, output $= \rho \otimes \mu_x$ is a product state with $\mu_x$ independent of $\rho$ (otherwise, TP' would not have transmitted $\rho$ perfectly).

So this gives an encryption scheme where:

- $pr(K=k) = p_x$ = prob of getting outcome k in TP'.
- $\mathcal{E}_K(\rho) = Tr_2\ U_x^{\dagger}(\rho \otimes \mu_x)\, U_x$

m such values suffice i.e. log m key bits

$\underset{\rho_K}{\parallel}$

d' dim

Alice prepares $\mu_x$

applies $U_x^{\dagger}$ to $\rho \otimes \mu_x$

sends first sys to Bob.

Then
- $D_K\, \mathcal{E}_K(\rho) = \rho$ by correctness of TP'.
- $\sum_k p_k\, \mathcal{E}_k(\rho) = tr_A |\psi\rangle\langle\psi| = \rho_0$ indep of $\rho$.

Thm 2: given any generalized encryption scheme QEnc′ encrypting a d-dim sys to an average state $\rho_0$, using a key $k \in \{1, 2, \ldots, m\}$, there is a generalized teleportation protocol TP′ using log m cbits and log d′ ebits to achieve log d qbits.

Pf (see quant-ph/0201008 for $\rho_0 = \frac{I}{d'}$, PRL vol 90 127905, 2003 for general $\rho_0$).

Here we prove for the simpler case: $d = d'$, $\rho_0 = \frac{I}{d}$,

$$\mathcal{E}_k(\varphi) = U_k \varphi U_k^\dagger, \quad D_k(\varphi) = U_k^\dagger \varphi U_k.$$

$$R(\varphi) = \sum_k p_k U_k \varphi U_k^\dagger = \frac{I}{d}, \quad \forall \varphi \in B(\mathbb{C}^d).$$

Claim: Let $|\Phi_d\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle|i\rangle$.

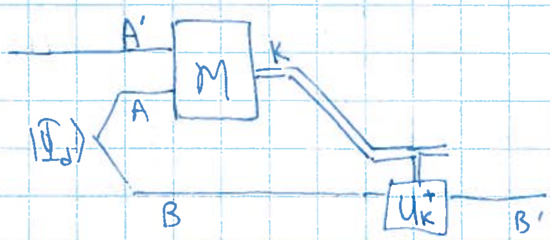
Almost a meas along $\{U_k^* \otimes I |\Phi_d\rangle\}_k$ ← Replaces the Bell measurement

Let $M_k = U_k^\dagger \otimes I \, |\Phi_d\rangle\langle\Phi_d| \, U_k \otimes I \; p_k \, d^2$

Then: ① $\{M_k\}_{k=1}^m$ is a POVM in $B(\mathbb{C}^d \otimes \mathbb{C}^d)$

(corresponding to some meas M on 2 d-dim sys)

② TP′ defined as




Transmits log d qbits from A′ to B′

Pf ①: for each $k$, clearly $M_k \geq 0$.

$$\sum_k M_k = \left(\sum_k p_k\, U_k^\dagger \otimes I\, |\Phi_d\rangle\langle\Phi_d|\, U_k \otimes I\right) d^2$$

$$= R \otimes I(\,|\Phi_d\rangle\langle\Phi_d|\,) \cdot d^2$$ ← uses properties of the exact randomizing map

$$= \left(\frac{I}{d} \otimes \frac{I}{d}\right) d^2 = I \otimes I$$

$\therefore \{M_k\}$ is a POVM.

② Let $\rho$ be the state in $A'$

$\rho_k$ . . . . . . . in $B$ if measurement outcome is $k$.

Then $p_k \rho_k = \mathrm{tr}_{A'A}\left[ M_{k\,A'A} \otimes I_B \left(\rho \otimes |\Phi_d\rangle\langle\Phi_d|\right)\right]$

$$= p_k d^2\, \mathrm{tr}_{A'A}\left(\left(\left(U_{k\,A'}^\dagger \otimes I_A\, |\Phi_d\rangle\langle\Phi_d|_{A'A}\, U_{k\,A'} \otimes I_A\right) \otimes I_B\right)\left(\rho_{A'} \otimes |\Phi_d\rangle\langle\Phi_d|_{AB}\right)\right)$$

$$\overset{\text{lemma}}{=} p_k d^2\, \mathrm{tr}_{A'A}\left(|\Phi_d\rangle\langle\Phi_d|_{A'A} \otimes I_B\right)\left(\left(U_k \rho U_k^\dagger\right)_{A'} \otimes |\Phi_d\rangle\langle\Phi_d|_{AB}\right)$$

no correction outcome in TP. new input

$$\overset{\text{TP}}{=} p_k d^2 \cdot \frac{1}{d^2}\left(U_k \rho U_k^\dagger\right)_B.$$ (Alternative pf: write $|\Phi_d\rangle\langle\Phi_d| = \sum_{i,j} |i\rangle\langle j| \otimes |i\rangle\langle j|$

$$= p_k \left(U_k \rho U_k^\dagger\right)_B.$$

$\therefore$ prob $(k) = p_k$, conditioned on outcome $k$,

Bob has $U_k \rho U_k^\dagger$. So applying $U_k^\dagger$ returns the correct state $\rho$

Lemma: $\mathrm{tr}_1 \left(N_1 \otimes I_2\right)\left(Y_{12}\right) = \mathrm{tr}_1 \left(Y_{12}\right)\left(N_1 \otimes I_2\right)$

Pf: by linearity, it suffices to check

for $N_1 = |i\rangle\langle j|$ and $Y_{12} = |k\rangle\langle \ell| \otimes |m\rangle\langle n|$

$LHS = \mathrm{Tr}_1 \left(|i\rangle\langle j|k\rangle\langle \ell|\right) \otimes |m\rangle\langle n| = \delta_{jk}\ \delta_{i\ell}\ |m\rangle\langle n|$

$RHS = \mathrm{tr}_1 \left(|k\rangle\langle \ell|i\rangle\langle j|\right) \otimes |m\rangle\langle n| = \delta_{jk}\ \delta_{i\ell}\ |m\rangle\langle n|.$

$\therefore$ Lemma holds $\forall\ N, Y$.

Cor: to encrypt a $d$-dim quantum sys (with average $\frac{I}{d}$)

the key has to take $d^2$ values

Taking into account data compression (next topic)

$2\log d$ key bits are needed.

NB: $\log d$ key bits are necessary and <u>sufficient</u>

for encrypting a $d$-state classical message.

Pf (cor): from thm 2, if, by contradiction, there is

an encryption scheme with fewer than $d^2$ key states

then, we can transmit $\log d$ qbits using fewer

than $2\log d$ cbits, contradicting optimality of

generalized teleportation.

NB: Thms 1-2 show that there is a 1-1 correspondence between generalized teleportation & generalized

quantum encryption.