CO781 / QIC 890:

Theory of Quantum Communication

Topic 1, part 4

What is communication of data?
The no-signalling principle
Optimality of superdense coding and teleportation
Cobits, duality of SD and TP,
and unitary gates as bidirectional channels

Equivalence of generalized teleportation
& generalized encryption of quantum states

Non-composable qbit: remote state preparation
& approximation encryption of pure states

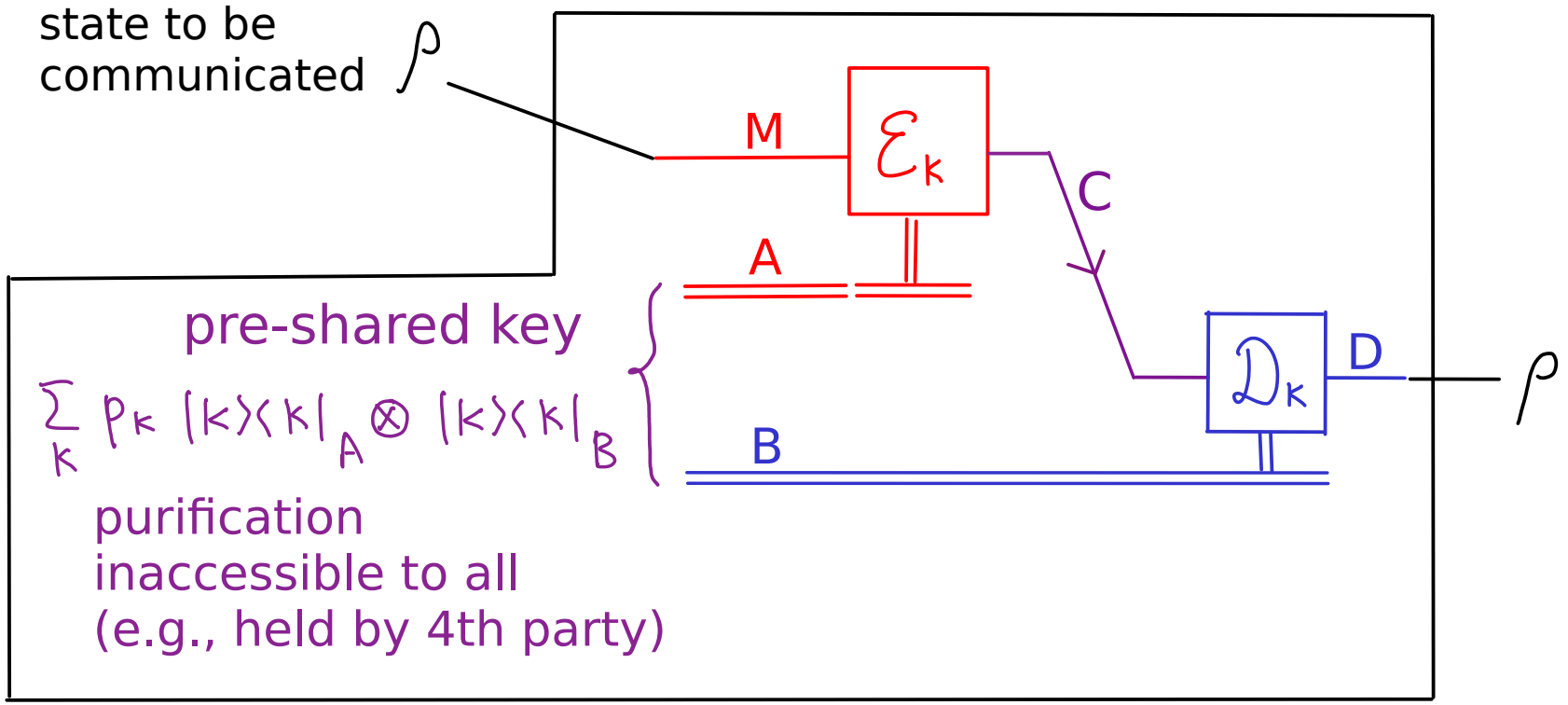
References:

Private quantum channel:
- Ambainis, Mosca, Tapp, deWolf 2000
- Boykin, Roychowdhury 2000

Connecting generalized teleportation
& generalized encryption of quantum states:
- Leung, Shor 2002

Remote state preparation & approx encryption:
- Lo 1999
- Bennett, DiVincenzo, Show, Smolin, Terhal, Wootters 00
- Devetak 2001
- Leung, Shor 2002
- Bennett, Hayden, Leung, Shor, Winter 2003
- Hayden, Leung, Shor, Winter 2003

Encryption of quantum states using a classical key



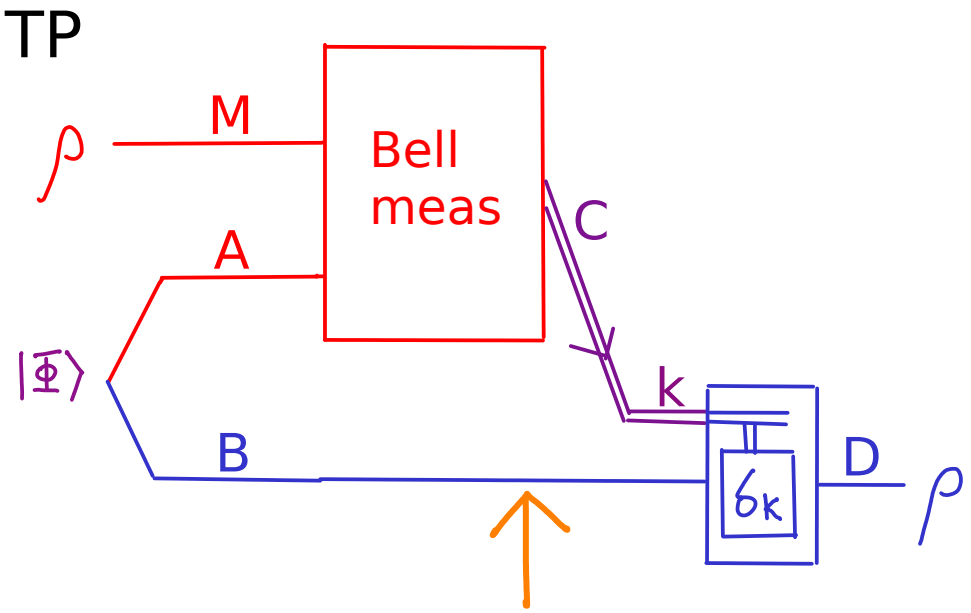
(1) correctness $\forall k,\ \mathcal{D}_k \mathcal{E}_k \approx \mathbb{I}$

(2) privacy: an eavesdropper not knowing k but may tap on C learns nothing about ρ

$\forall \rho \quad \sum_k p_k \mathcal{E}_k(\rho) = \sigma$ state indep of ρ

From self-study material 2020-09-14:

TP



wp 1/4, meas outcome = k

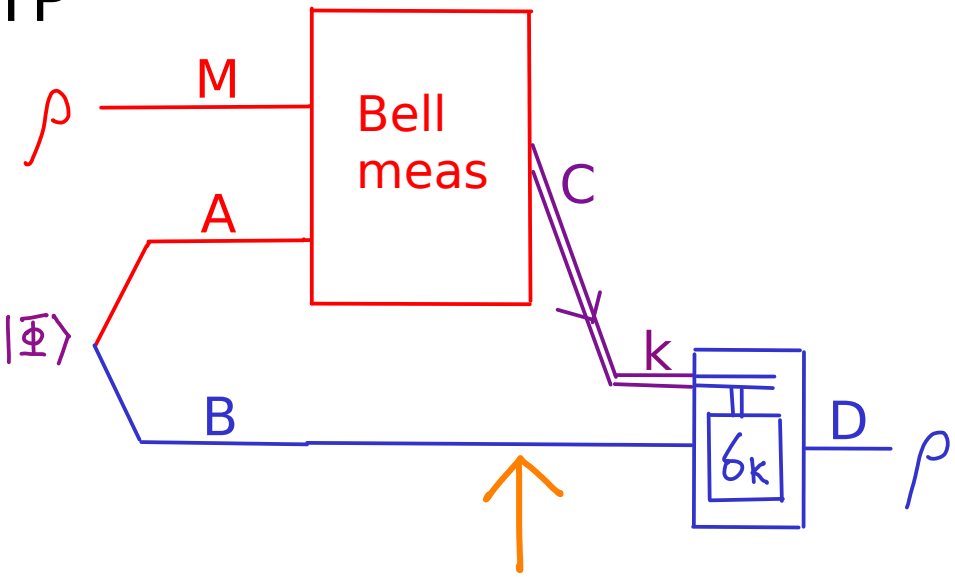
post-meas state on B : $\sigma_k \rho \sigma_k$

not knowing k, state on B : $\frac{1}{4} \sum_{k=0}^{3} \sigma_k \rho \sigma_k$

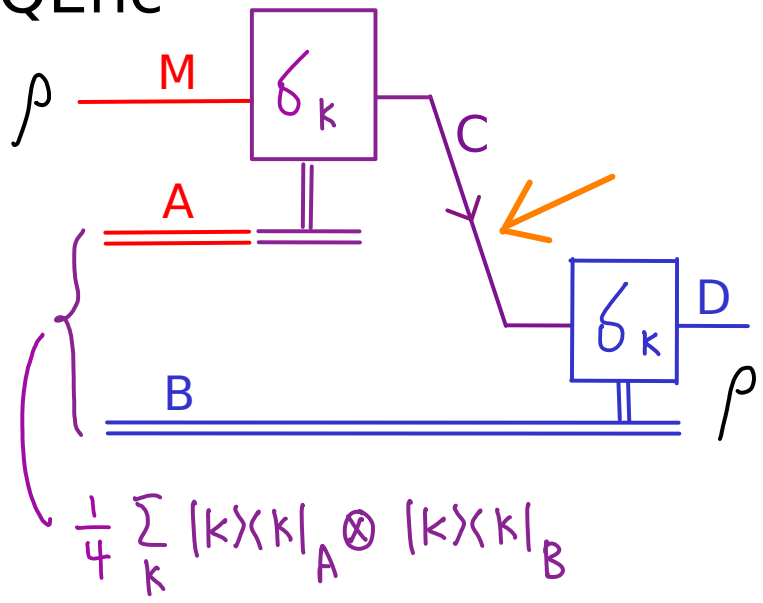
pre-meas state on B : $\frac{I}{2} = \forall \rho$

From self-study material 2020-09-14:

TP



QEnc



wp 1/4, meas outcome = k

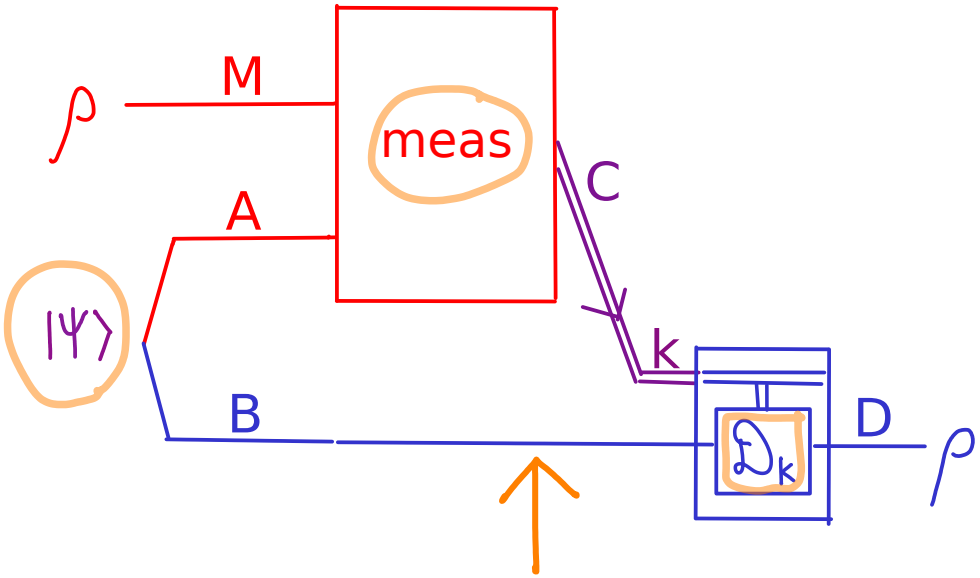
post-meas state on B : $\sigma_k \rho \sigma_k$

not knowing k, state on B : $\frac{1}{4}\sum_{k=0}^{3} \sigma_k \rho \sigma_k$

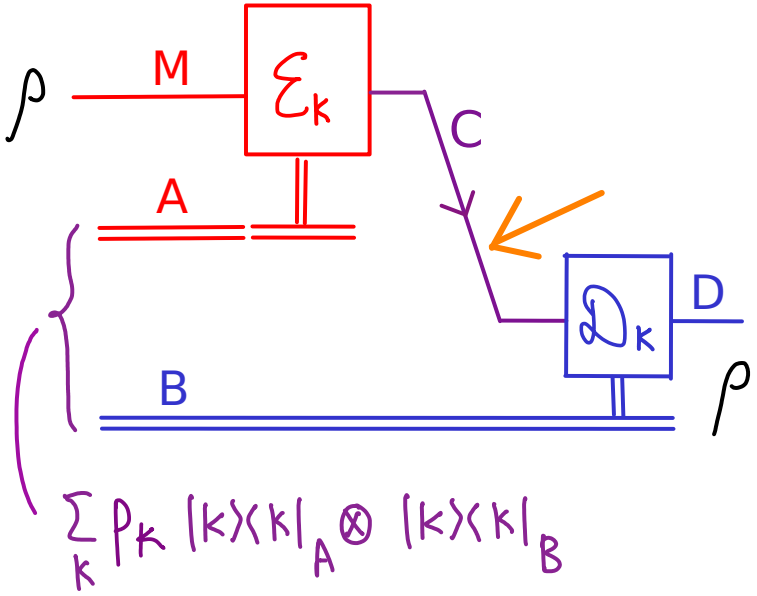
pre-meas state on B : $\frac{I}{2} = \forall \rho$

gives encryption scheme

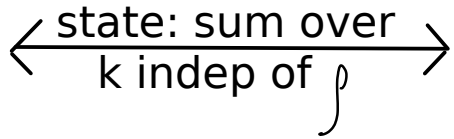
Generalized teleportation:



Generalized encryption:



system B before arrival of message

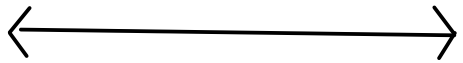


system c subject to eavesdropping

measurement outcome k

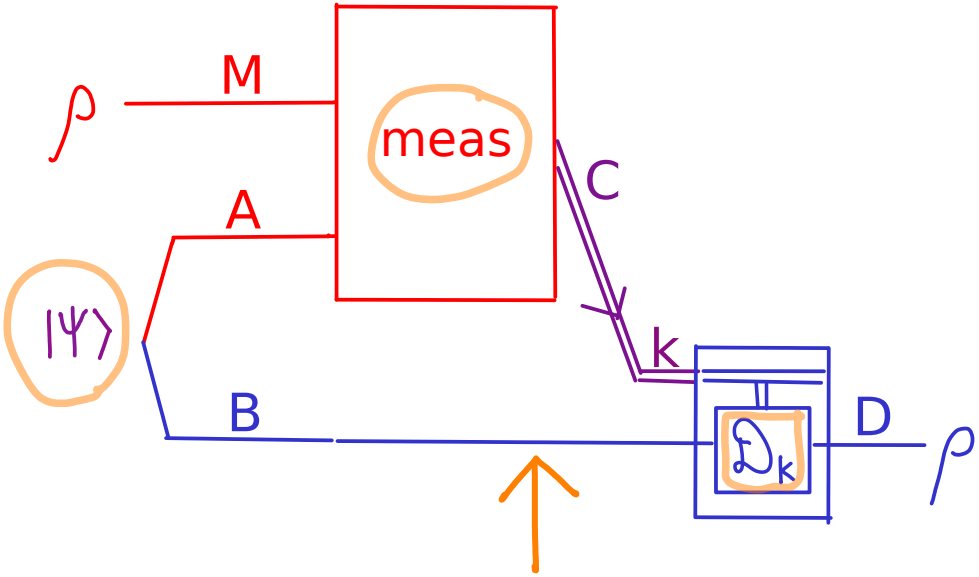
pre-shared secret key k

state in B after arrival of msg , $\mathcal{D}_k^{-1}(\rho)$

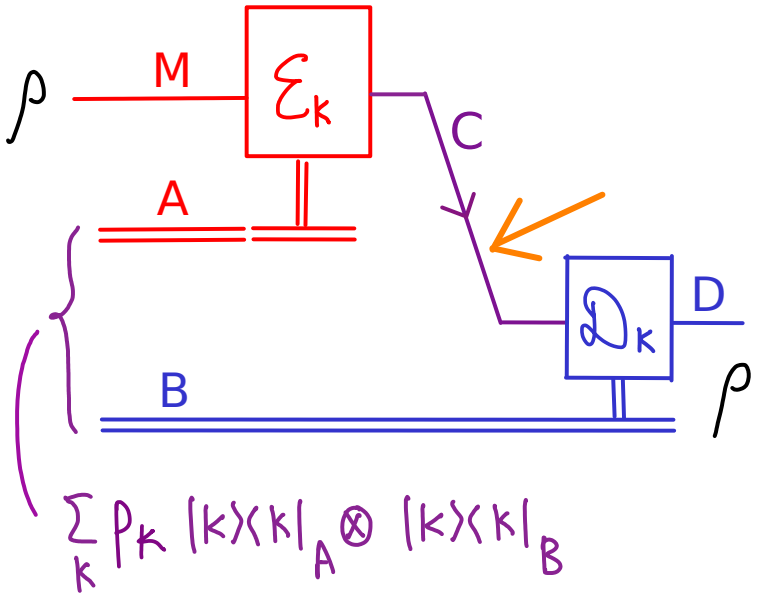


encrypted state given k , $\mathcal{E}_k(\rho)$

Generalized teleportation:



Generalized encryption:



The connection goes further -- any generalized teleportation scheme can be turned into a generalized quantum encryption scheme and vice versa !!

* classical comm cost becomes key-cost and vice versa
* entanglement cost becomes Q comm cost & vice versa

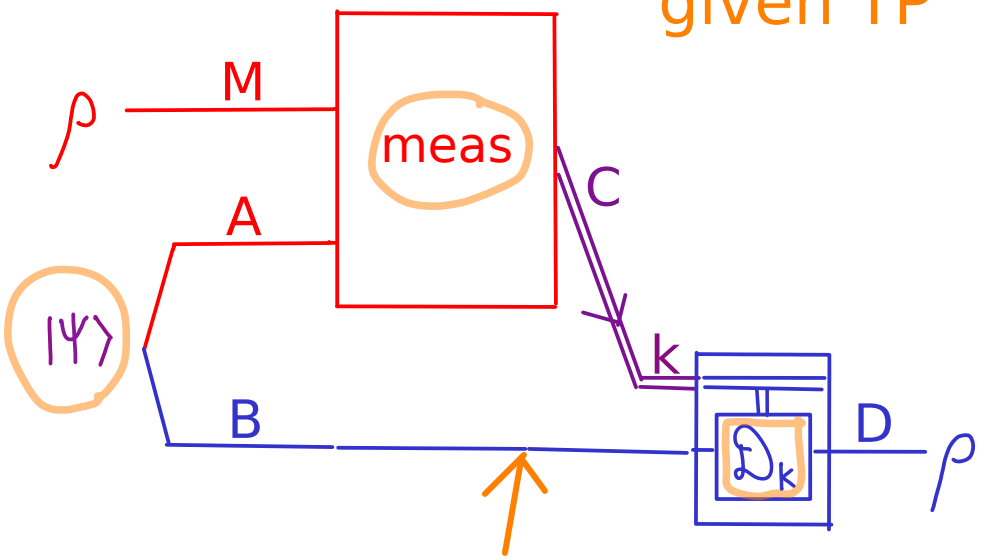
Theorem 1:
For any generalized teleportation protocol TP'
transmitting any d-dim state by consuming
an entangled state $|\psi\rangle$ with local dimension d'
and sending a message $k \in \{1,2,...,m\}$,
there is a generalized encryption scheme QEnc' for d-dim
states consuming a key $k \in \{1,2,...,m\}$ & log d' qbits.

We are given the meas, $|\psi\rangle$, $\mathcal{D}_k$ in TP'.

We need to find $\mathcal{E}_k$, $\mathcal{D}_k$, ρ_k in QEnc'.

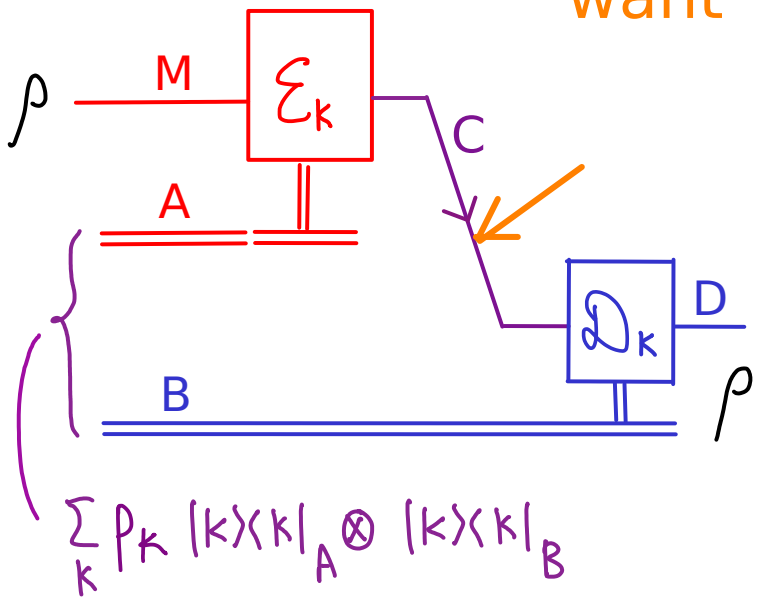
Generalized teleportation:

given TP'



Generalized encryption:

want



take: p_k = prob (outcome k), $\mathcal{D}_k$ as in TP'

want: if key=k, Alice can prepare from a copy of ρ

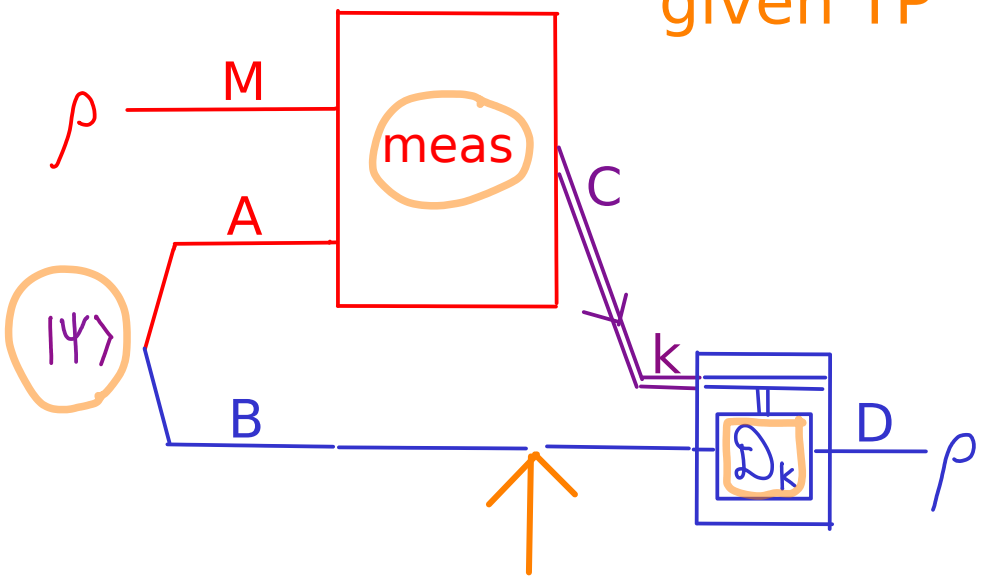
$\mathcal{E}_k(\rho)$ = postmeas state in B given outcome k in TP'

Then (1) correctness is immediate, (2) privacy follows from writing Bob's state in 2 ways before he receives k:

$$\sum_k p_k \mathcal{E}_k(\rho) = \mathrm{tr}_A |\psi\rangle\langle\psi| =: \sigma$$

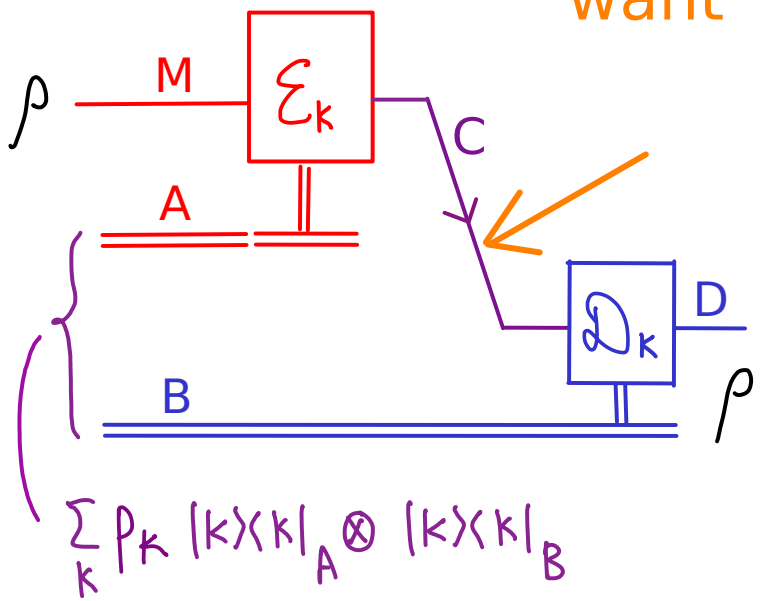
Generalized teleportation:

given TP'



Generalized encryption:

want



take: p_k = prob (outcome k), $\mathcal{D}_k$ as in TP'

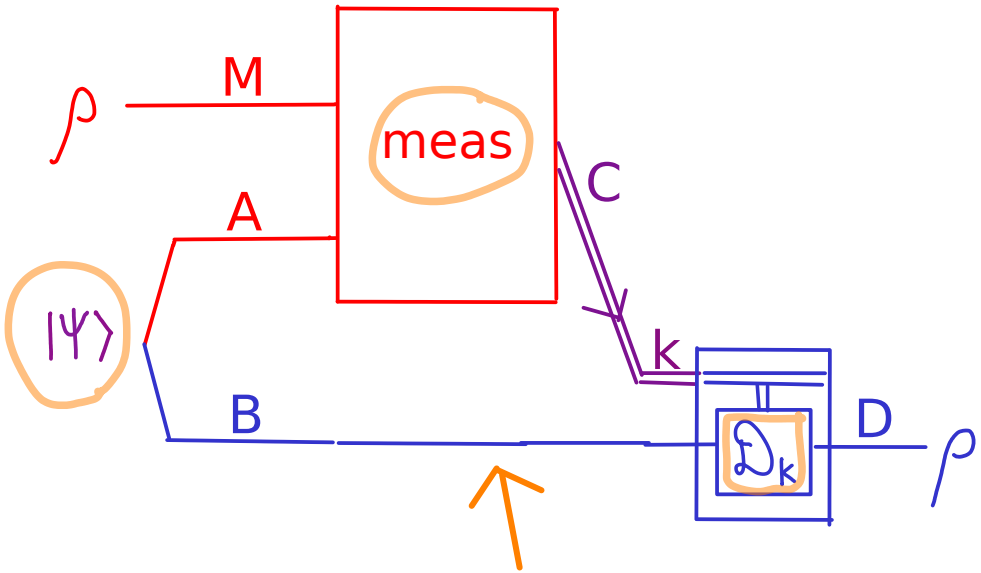
want: if key=k, Alice can prepare from a copy of ρ

$\mathcal{E}_k(\rho)$ = postmeas state in B given outcome k in TP'

Tempting, wrong, idea: Alice prepares $|\psi\rangle_{AC}$ with both AC in her lab, meas MA as in TP', and obtain $\mathcal{E}_k(\rho)$ in C.

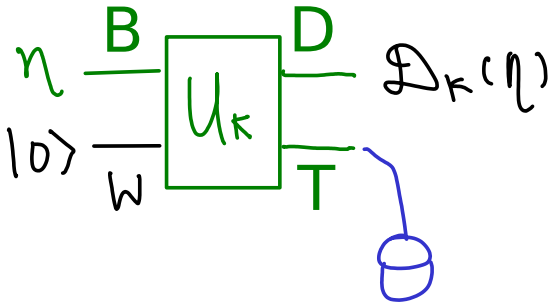
But she cannot control the outcome -- gets $\mathcal{E}_k(\rho)$ only wp p_k.

How to apply $\mathcal{E}_K$ given TP' :



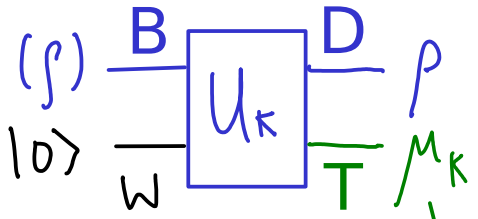
Consider the unitary representation of $\mathcal{D}_K$:

$$\mathcal{D}_K(\eta) = \mathrm{tr}_T\, U_K \left(\eta \otimes |0\rangle\langle 0|\right) U_K^\dagger$$



want $\mathcal{E}_K(\rho)$ = the state on B right before $\mathcal{D}_K$

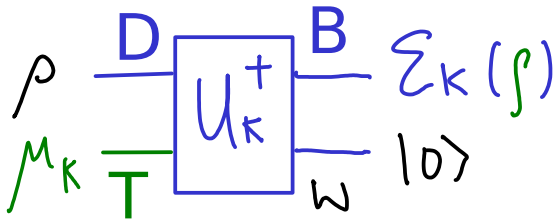
$\therefore$ $\mathcal{E}_K(\rho)$



indep of ρ

,

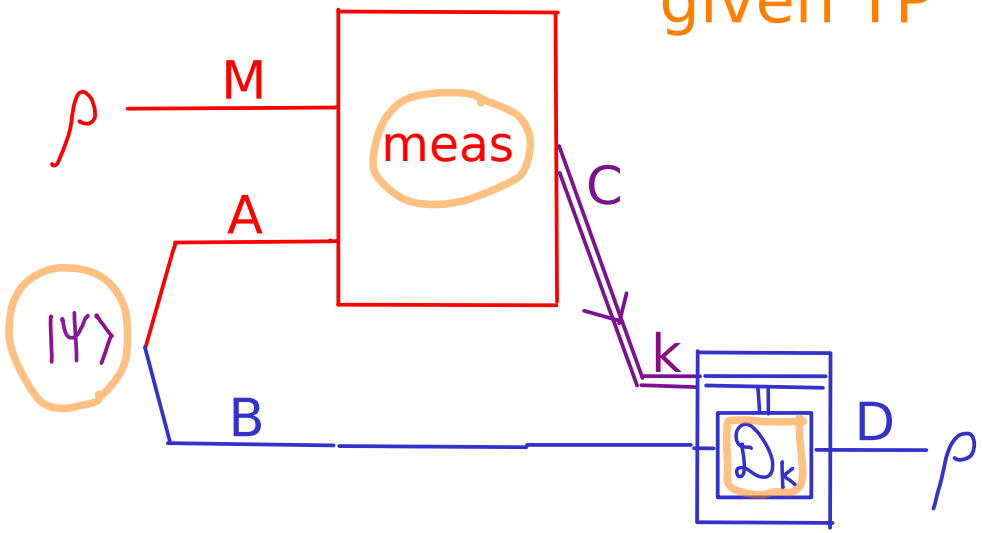
$\therefore$ ρ



$\therefore$ for each k, $\mathcal{E}_K(\rho) = \mathrm{tr}_W\, U_K^\dagger (\rho \otimes \mu_K) U_K$ is valid enc map for Alice

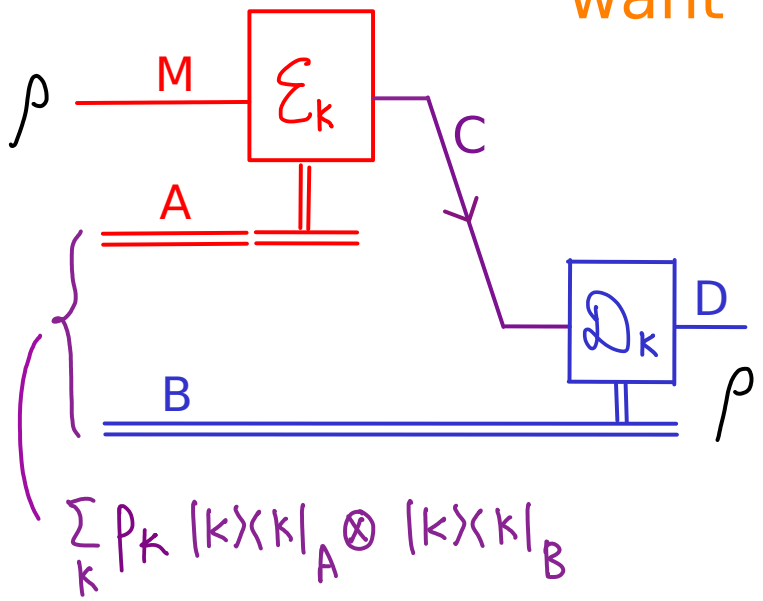
Generalized teleportation:

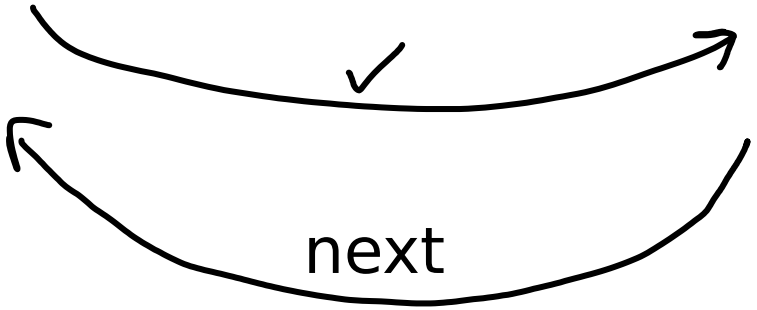
given TP'



Generalized encryption:

want





a bit harder

Theorem 2:
Given a generalized encryption scheme QEnc' encrypting any d-dim state to a d'-dim state σ, consuming a key $k \in \{1,2,...,m\}$ and log d' qbits, there is a generalized teleportation protocol TP' that comm any d-dim state by consuming an entangled state with local dimension d' and sending a message $k \in \{1,2,...,m\}$.

We are given $\mathcal{E}_k, \mathcal{D}_k, p_k$ in QEnc'.

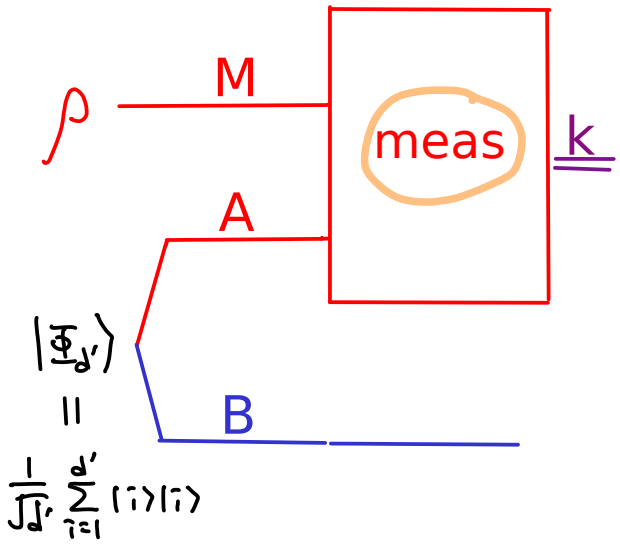
We need to find meas, $|\psi\rangle, \mathcal{D}_k$ in TP'.

We first consider the case when $\sum_k p_k \mathcal{E}_k(\rho) = \frac{I}{d'}$.

(extend to $\sum_k p_k \mathcal{E}_k(\rho) = \sigma$ later)

In TP', choose $|\psi\rangle = |\Phi_{d'}\rangle$ and choose $\mathcal{D}_k$ as in QEnc'.

Want: meas with outcome k with prob p_k postmeas state $\mathcal{E}_k(\rho)$ on B



From QM:

Let meas be defined by POVM $\{M_k\}$.

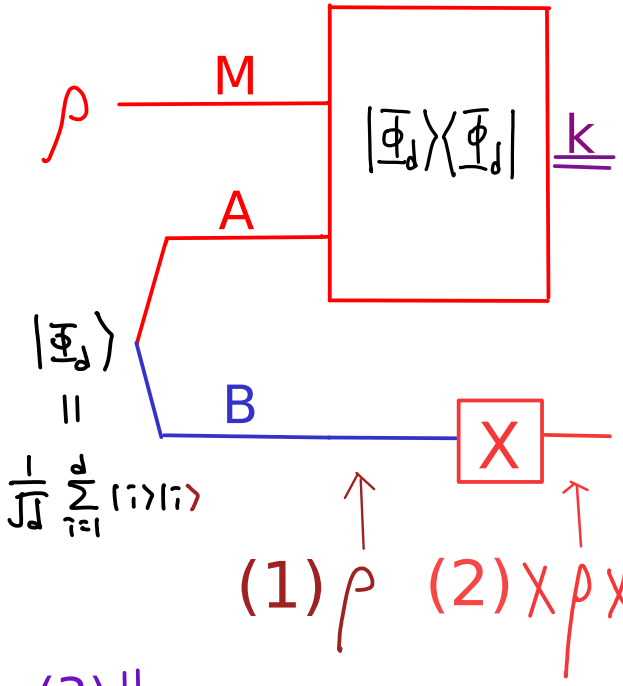
postmeas state be ρ_k conditioned on outcome k. Then,

(†) $p_k \rho_k = \mathrm{tr}_{MA}\left(M_k \otimes I\right)\left(\rho \otimes |\Phi_{d'}\rangle\langle\Phi_{d'}|\right)$

A simpler question: let $X : \mathbb{C}^d \to \mathbb{C}^{d'}$, $d' \geq d$

what M_k makes $p_k \rho_k = X \rho X^\dagger$ in (†) ?

Coming up with the meas for TP':



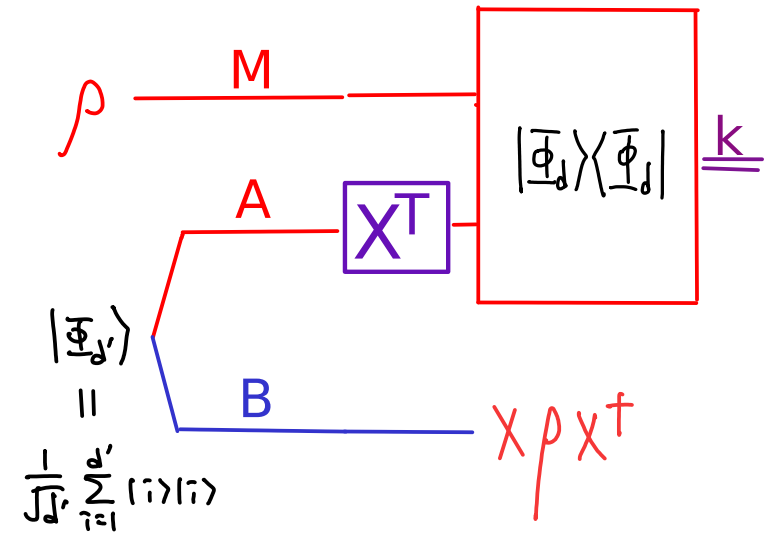
(1) If $M_k \propto |\Phi_d\rangle\langle\Phi_d|$, dim(A)=dim(B)=d
then postmeas state = ρ

(2) further "applying" X to B
results in the state $X\rho X^\dagger$

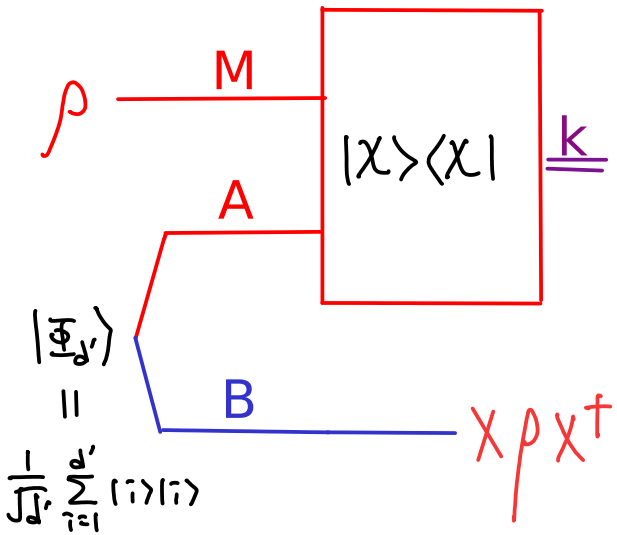
(3) transpose trick (SS 2020-09-21)
(note now dim(A)=dim(B)=d')

(4) absorb X^T into meas (SS)

$|\chi\rangle = I \otimes (X^T)^\dagger |\Phi_d\rangle$



(4) =



Claim: If $M_k = dd' \; I \otimes \overline{X} \; (|\Phi_d\rangle\langle\Phi_d|) \; I \otimes X^T \propto |X\rangle\langle X|$

then $tr_{MA}\left(\rho \otimes |\Phi_{d'}\rangle\langle\Phi_{d'}|\right)\left(M_k \otimes I\right) = X \rho X^\dagger$

(M, A, M, A; M, AB, MA, B, B)

Here, $\overline{X}$ = complex conjugate of X, dim(M)=d, dim(A)=d'.

Claim: If $M_k = \sqrt{d d'}\, I \otimes \bar{X}\, (|\Phi_d\rangle\langle\Phi_d|)\, I \otimes X^T$

then $\mathrm{tr}_{MA}\left(\rho \otimes |\bar{\Phi}_{d'}\rangle\langle\bar{\Phi}_{d'}|\right)(M_k \otimes I) = X \rho X^\dagger$

(M, AB, MA, B)

Proof: $\mathrm{tr}_{MA}\left(\rho \otimes |\bar{\Phi}_{d'}\rangle\langle\bar{\Phi}_{d'}|\right)\left(I \otimes \bar{X}\right)(|\Phi_d\rangle\langle\Phi_d|)\left(I \otimes X^T\right) \otimes I \; d d'$

$(I \otimes |\bar{\Phi}_{d'}\rangle\langle\bar{\Phi}_{d'}|)\; \rho \otimes I \otimes I$

$= \mathrm{tr}_{MA}\left(I \otimes |\bar{\Phi}_{d'}\rangle\langle\bar{\Phi}_{d'}|\right)\left(I \otimes \bar{X}\right)(\rho \otimes I\; |\Phi_d\rangle\langle\Phi_d|)\left(I \otimes X^T\right) \otimes I \; d d'$

partial trace of M (and identity map on AB):

$\sum_i \langle i|_M \otimes I_{AB}\; [\quad]\; |i\rangle_M \otimes I_{AB}$

use $\langle i|_M I_M = \langle i|_M$, $I_M |i\rangle_M = |i\rangle_M$

to move the partial trace of M to $(\rho \otimes I\; |\Phi_d\rangle\langle\Phi_d|)$

Claim: If $M_k = \sum_{d,d'} (I \otimes \bar{X})\,(|\Phi_d\rangle\langle\Phi_{d'}|)\,(I \otimes X^T)$

(M, A on $I \otimes \bar{X}$; M, A on $I \otimes X^T$)

then $\mathrm{tr}_{MA}\left(\rho \otimes |\Phi_{d'}\rangle\langle\Phi_d|\right)(M_k \otimes I) = X \rho X^\dagger$

(ρ: M; $|\Phi_{d'}\rangle\langle\Phi_d|$: AB; M_k: MA; I: B; $X\rho X^\dagger$: B)

Proof: $\mathrm{tr}_{MA}\left(\rho \otimes |\Phi_{d'}\rangle\langle\Phi_d|\right)\left(I \otimes \bar{X}\right)\left(|\Phi_d\rangle\langle\Phi_{d'}|\right)\left(I \otimes X^T\right) \otimes I \; dd'$

$(I \otimes |\Phi_{d'}\rangle\langle\Phi_d|)\;\rho \otimes I \otimes I$

$= \mathrm{tr}_{MA}\left(I \otimes |\Phi_{d'}\rangle\langle\Phi_d|\right)\left(I \otimes \bar{X}\right)\left(\rho \otimes I\; |\Phi_d\rangle\langle\Phi_{d'}|\right)\left(I \otimes X^T\right) \otimes I \; dd'$

$= \mathrm{tr}_{A}\left(\quad |\Phi_{d'}\rangle\langle\Phi_d|\right)\left(\quad \bar{X}\right)\left(\rho \otimes I\; |\Phi_d\rangle\langle\Phi_{d'}|\right)\left(\quad X^T\right) \otimes I \; dd'$

(tr_M)

SS-2020-09-21

Lemma 1

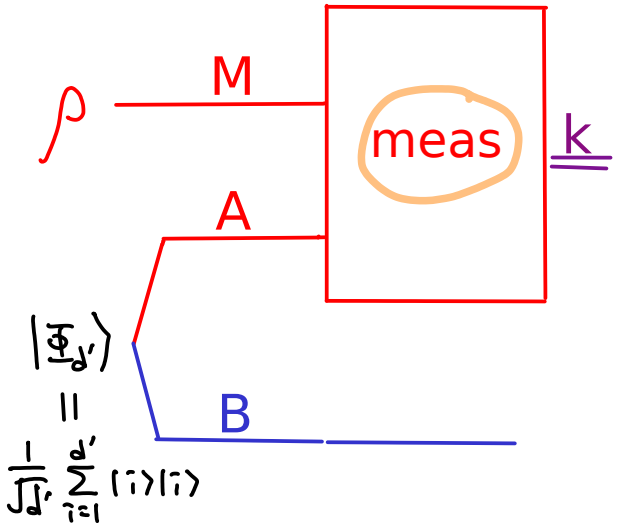
$= \mathrm{tr}_{A}\left(\quad |\Phi_{d'}\rangle\langle\Phi_d|\right)\left(\quad \bar{X}\right)\left(\quad \rho^T \quad\right)\left(\quad X^T\right) \otimes I \; d'$

(AB; A; A; A B)

Lemma 1

$= \left(\bar{X}\,\rho^T X^T\right)^T_B = \left(X \rho X^\dagger\right)_B$

Want: meas with outcome k with prob p_k postmeas state $\mathcal{E}_k(\rho)$ on B



Last page:

If $M_k = d\,d'\ I\otimes\bar{X}\,(|\Phi_d\rangle\langle\Phi_d|)\,I\otimes X^\dagger$

then $\mathrm{tr}_{MA}\,(\rho\otimes|\Phi_{d'}\rangle\langle\Phi_{d'}|)(M_k\otimes I) \underset{\bigstar}{=} X\rho X^\dagger$

To find M_k that gives postmeas state $\mathcal{E}_k(\rho)$ wp p_k:

use Kraus rep for $\mathcal{E}_k$: $\forall\rho,\ \mathcal{E}_k(\rho) = \sum_\ell A_\ell^k \rho A_\ell^{k\dagger}$

Choose $M_k = p_k \sum_\ell d\,d'\ I\otimes\overline{A_\ell^k}\,(|\Phi_d\rangle\langle\Phi_d|)\,I\otimes A_\ell^{k\dagger}$

then $\mathrm{tr}_{MA}\,(\rho\otimes|\Phi_{d'}\rangle\langle\Phi_{d'}|)(M_k\otimes I)$ ← linear in M_k

$= p_k \sum_\ell$ LHS of $\bigstar$ with $X = A_\ell^k = p_k \sum_\ell A_\ell^k \rho A_\ell^{k\dagger} = p_k\,\mathcal{E}_k(\rho)$

To complete the construction of the protocol TP', we now show that $\{M_k\}$ is a POVM.

① $\forall k,\ M_k = p_k \sum_\ell d\, d'\ I \otimes \overline{A_\ell^k}\, (|\Phi_d\rangle\langle\Phi_d|)\, I \otimes A_\ell^{k\dagger} \geq 0$

② $\sum_k M_k = \sum_k p_k \sum_\ell d\, d'\ I \otimes \overline{A_\ell^k}\, (|\Phi_d\rangle\langle\Phi_d|)\, I \otimes A_\ell^{k\dagger}$

$= \sum_k p_k\, d\, d'\ I \otimes \overline{\mathcal{E}_k}\, (|\Phi_d\rangle\langle\Phi_d|)$ where $\overline{\mathcal{E}_k}(\eta) = \sum_\ell \overline{A_\ell^k}\, \eta\, A_\ell^{k\dagger}$

$= d\, d'\ I \otimes \sum_k p_k \overline{\mathcal{E}_k}\, (|\Phi_d\rangle\langle\Phi_d|)$

PTO

$= I \otimes I$

d-dim d'-dim

From the privacy condition of QEnc':

$$\forall \rho \quad \sum_k p_k \mathcal{E}_k(\rho) = \sigma = \frac{I}{d'}$$

$$\forall \eta, \text{ let } \rho = \bar{\eta}, \quad \sum_k p_k \mathcal{E}_k(\bar{\eta}) = \sigma \text{ from above}$$

$$\| $$

$$\sum_k p_k \sum_\ell A_\ell^k \bar{\eta} A_\ell^{k\dagger}$$

Taking complex conjugate on both sides:

$$\forall \eta, \sum_k p_k \sum_\ell \overline{A_\ell^k} \eta \overline{A_\ell^{k\dagger}} = \bar{\sigma} \quad \text{ie} \sum_k p_k \bar{\mathcal{E}}_k(\eta) = \bar{\sigma} \quad \text{constant}$$

$$\therefore I \otimes \left(\sum_k p_k \bar{\mathcal{E}}_k\right)\left(|\bar{\Phi}_d\rangle\langle\bar{\Phi}_d|\right)$$

$$= \mathrm{tr}_2\left(|\bar{\Phi}_d\rangle\langle\bar{\Phi}_d|\right) \otimes \bar{\sigma} = \frac{I}{d} \otimes \frac{I}{d'}$$

What if $\sum_k p_k \mathcal{E}_k(\rho) = \sigma$ in QEnc' ?

We will eventually take $|\Psi\rangle = I \otimes \sqrt{\sigma}\sqrt{d'}\,|\Phi_{d'}\rangle$ in TP'.

But for now, instead, let $\widetilde{\mathcal{E}}_k(\rho) = \frac{\sigma^{-\frac{1}{2}}}{\sqrt{d'}}\,\mathcal{E}_k(\rho)\,\frac{\sigma^{-\frac{1}{2}}}{\sqrt{d'}}$

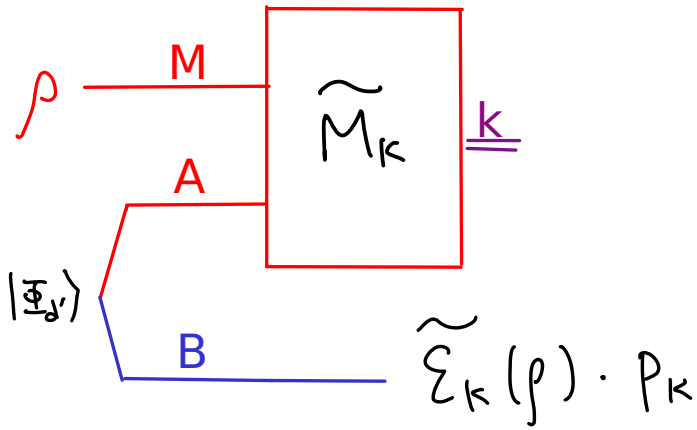
which is completely positive but not trace preserving

$$\mathcal{E}_k(\rho) = \sum_l A_l^k \rho A_l^{k\dagger}, \quad \widetilde{\mathcal{E}}_k(\rho) = \sum_l \frac{\sigma^{-\frac{1}{2}}}{\sqrt{d'}} A_l^k \rho A_l^{k\dagger} \frac{\sigma^{-\frac{1}{2}}}{\sqrt{d'}}$$

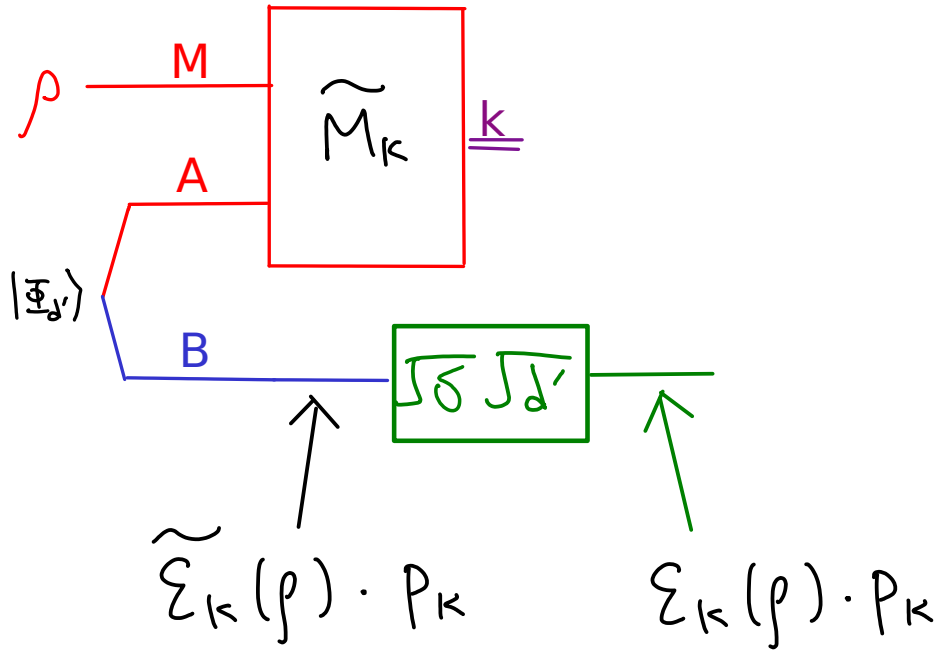
Now $\sum_k p_k \widetilde{\mathcal{E}}_k(\rho) = \frac{I}{d'}$ so, earlier case applies.

take $\widetilde{M}_k = p_k \sum_l d\,d'\; I \otimes \overline{\frac{\sigma^{-\frac{1}{2}}}{\sqrt{d'}}}\;\overline{A_l^k}\,(|\Phi_d\rangle\langle\Phi_d|)\, I \otimes A_l^{k\dagger}\,\overline{\frac{\sigma^{-\frac{1}{2}}}{\sqrt{d'}}}$

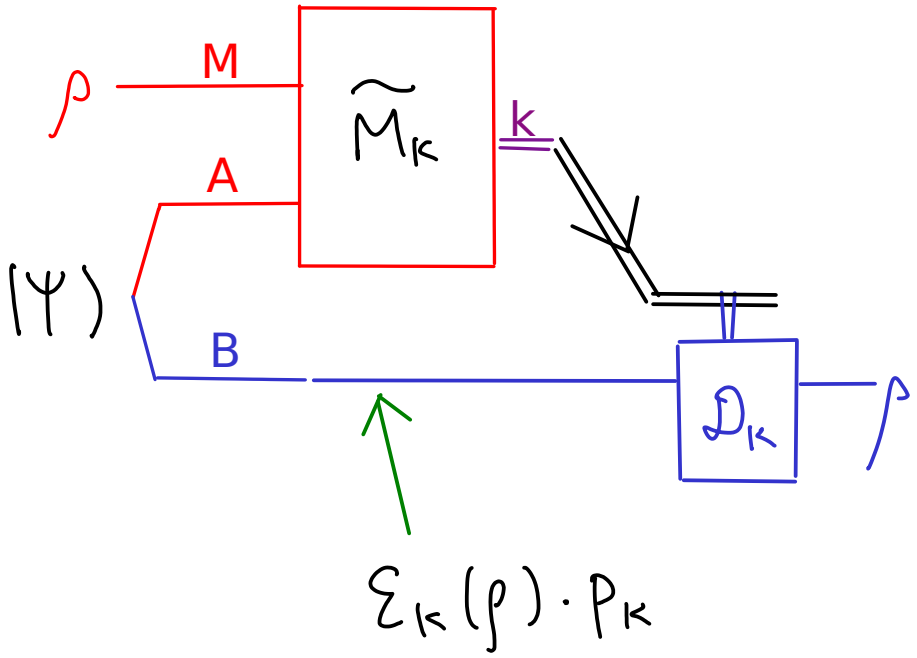
so, $\{\widetilde{M}_k\}$ is a POVM and



Now, "apply" $\sqrt{\delta}\sqrt{\delta'}$ to B



So, here's TP' :



but $|\Psi\rangle = I\otimes\sqrt{\delta}\sqrt{\delta'}\,|\Phi_{d'}\rangle$

Consequence 1:

The encryption of a d-dim quantum state requires a key that ranges over d^2 values.

Proof: suppose, by contradiction, there is a protocol with a key that ranges over fewer than d^2 values.

This gives a generalized teleportation scheme to comm a d-dim quantum state consuming entanglement and comm of a classical message with fewer than d^2 values, contradicting the optimality of standard teleportation.

Consequence 2:

d^2 key values are sufficient due to teleportation.

NB. Such a key is called "log d" key-bits (kbits).

Preview:

To encrypt a classical message with d possible values, log d kbits are sufficient.

Why quantum encryption incurs a factor of 2?

1. We will see that quantum encryption of pure quantum states of d-dim requires only log d kbits, so, the factor of 2 comes from having to break the entanglement with a purification of the state to be encrypted.

This comes from remote state preparation (a discounted teleportation-like scheme).

2. Probably won't have time for this ...
Barnum, Crepeau, Gottesman, Smith, Tapp (2002) compose a small quantum error detecting code (chosen randomly with log key size) to QEnc. This gives a quantum message authentication scheme, with small prob(no error detected and message altered).

In 2004 (arXiv 2016), Hayden, Mayers, and I showed that key recycling (of the encryption key) (and also the auth scheme) is composably secure if no error is detected. This requires 1 authenticated cbit backwards, but allows the catalytic (or amortized) key cost to be negligible in message length (if no one tampers with the transmission).

Both proofs rely on relating teleportation with encryption, and secure ebits.

Today's lecture came from an attempt to lower bound the cost for remote state preparation ...