3 further comments on TP, qubits & nonsignaling:

1. Connection between TP & quantum encryption & Enc

2. An example of "non-composable-qbit":
   - Remote state preparation

3. Beyond QM ...

References:


2. Le 99, Bennett-DiVincenzo-Shor-Smolin-Terhal-Wootters 00
   Demetrescu 01, Leung-Shor 02, Bennett-Hayden-Leung-Shor-Wootters 03
Connection between TP & QEnc:

Recall TP:

\[
\begin{align*}
\begin{array}{c}
\text{Alice} \\
\text{Bob}
\end{array}
\quad \xrightarrow{f} \quad \xrightarrow{\text{Bell}} \quad \xrightarrow{x}
\end{align*}
\]

\[
\text{State} = 0_x f 0_x^t
\]

By evaluating Bob’s state before receiving \( x \):

\[
\frac{1}{2} = \frac{1}{4} \sum_x 0_x f 0_x^t
\]

Half of \( \frac{1}{2} \) prob of each \( x \) State conditioned on message = \( x \)

This gives an encryption scheme QEnc:

Alice and Bob share a secret key \( x \),

\[
\forall x \in \{0, 1, 2, 3\}, \quad P_r(x) = \frac{1}{4}
\]

Alice applies \( 0_x \) to \( f \)

She transmits \( 0_x f 0_x^t \) to Bob.

Bob decodes by inverting \( 0_x \).

An eavesdropper without knowledge of \( x \) sees \( E(f) = \frac{1}{4} \sum_x 0_x f 0_x^t = \frac{1}{2} \)

that is independent of \( f \).
Consider generalized teleportation (using entanglement & qubits to achieve qubits):

\[ A \rightarrow B, \quad D_{c} \rightarrow B', \quad f \]

\[ \text{NB: Measure independent of } f \]
\[ (A, B : d - \text{dim}) \]
\[ (f : d - \text{dim}, \quad d \leq d') \]
\[ \text{Ent part of } |\phi\rangle_p A' \]

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

\[ A \rightarrow B, \quad E_k \]
\[ D_{c} \rightarrow B', \quad f \]

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

To communicate $f$ to Bob:

Alice applies $E_k$ and sends $E_k(f)$ to Bob, and Bob applies $D_k$ to retrieve $f$, such that:

1. $A \rightarrow B, \quad D_k E_k = I$ (correctness)
2. $R(f) := \sum_k P_k E_k (f) = \rho_0$ (Unbreakable $f$)

What Eve can see without knowing $k$:

$\rho_0 \Rightarrow E_k(f) = E_k f^* \Rightarrow \rho_0 = \frac{1}{2}$.
Natural correspondences:

Generalized teleportation:
- Measurement outcome $X$ sent via quantum channel
- Bob's half of ent state
- Bob's state upon receiving $X$ for

Generalized $Q$-amplification:
- Key $k$
- Pre-shared secret
- The state being eavesdropped
- The state transmitted knowing $k$
• Consider exact schemes (will return to this issue).

Think: given any generalized teleportation protocol TP for transmitting any $d$-dim $\mathcal{Q}$ state using an entangled state $|\psi\rangle$ with local dm $d'$ and transmitting a message $x \in \{1, \ldots, m\}$, there is an encryption scheme AEnc using a key $k \in \{1, \ldots, m\}$ and local $d'$ qubits.

**Pf:** We need to find $E_x$ for the encryption scheme:

A tempting idea that doesn’t work:

\[
\begin{array}{c}
\text{Mens} \xrightarrow{x} \sum \rho_{xc} |xx\rangle \otimes E_x(s) \\text{prepar} \\text{e} \text{d} \text{ent} \text{ire} \text{ly} \text{in} \\text{Alice's bob}
\end{array}
\]

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:

\[
\begin{array}{c}
Y_x : D_{sc} \xrightarrow{x} \rho_{sc} \xrightarrow{x} \sum \rho_{xc} \mathcal{F}_x = \mathcal{F}_A \ \text{tr} Y_x Y_x^\dagger,
\end{array}
\]
Using the isometric extension of $Dx$, $\exists$ unitary $Ux$ $\exists$ state $\mu x$ s.t.

Furthermore, output $= p \otimes \mu x$ in a product state with $\mu x$ independent of $f$ (otherwise, $T^\dagger F$ would not have transmitted $f$ perfectly).

So this gives an encryption scheme where:

- $Pr(k = k) = p_k$ = prob of getting outcome $k$ in $F$.

- $E_k(f) = Tr_{x} U^\dagger x (p \otimes \mu x) U x$

Then $D_k E_k(f) = f$ by linearity of $T^\dagger F$.

- $\sum_{k} p_k E_k(f) = Tr_{A}(x|x+1) = p_0$ in $D_k f$. 

Alice prepares $\mu x$

Applies $Ux$ to $p \otimes \mu x$

Sends first $x$ to Bob.
2: Given any generalized encryption scheme for encrypting a d-dim sys to an average state $\rho_s$, using a key $K \in \{1, 2, \ldots, m\}$, there is a generalized teleportation protocol $TP'$ using $\log_2 m$ qubits and $\log_2 d$ qubits to achieve $\log_2 d$ qubits.

**Proof** (See quant-ph/0201008 for $\rho_s = \frac{I}{d^2}$, PRL vol.90 127905, 2003 for general $\rho_s$).

Here we prove for the simpler case: $d = d$, $\rho_s = \frac{I}{d^2}$.

$$E_k(y) = U_k y U_k^\dagger, \quad D_k(y) = U_k^\dagger y U_k.$$ 

$$\sum_k \frac{1}{c_k} Y_{2k} = \frac{1}{d} \sum_k Y_{2k} = \frac{1}{d}, \quad Y_{2k} \in B(C^d).$$

**Claim:** Let $|\psi_d\rangle = \frac{1}{\sqrt{d}} \sum_{c=0}^{d-1} |c\rangle |c\rangle$.

Let $M_k = U_k^\dagger |\psi_d\rangle \langle \psi_d| U_k |I \rangle |I \rangle |I \rangle$ $p_k d^2$.

Then: $\{ M_k \}_{k=1}^m$ is a POVM in $B(C^d \otimes C^d)$ (corresponding to some meas $M$ on 2 d-dim sys).

2. $TP'$ defined as

Transmits $\log_2 d$ qubits from $A'$ to $B'$.  

\[ 
\begin{array}{c}
A' \\
\Downarrow \\
M \\
\Downarrow \\
A \\
\Downarrow \\
B' \\
\Downarrow \\
\text{Transmits $\log_2 d$ qubits from $A'$ to $B'$} \\
\end{array} 
\]
Pf. (i): For each $k$, clearly $M_k \geq 0$.

$$\sum_k M_k = \left( \sum_k p_k M_k \otimes I \right) d^2$$

$$= R \otimes I \left( 1 \otimes \mathbb{E}_k \mathbb{E}_d \right) d^2$$

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

$\therefore$ $M_k$ is a POVM.

(2) Let $\rho$ be the state in $A'$

$p_k \ldots \ldots \text{in } B$ if measurement outcome is $k$.

Then $p_k = \text{Tr}_{A' A} \left[ M_k \otimes I \left( | \varphi_k \rangle \langle \varphi_k | \right) \otimes I \right]$

$$= p_k d^2 \text{Tr}_{A' A} \left( | \varphi_k \rangle \langle \varphi_k | \otimes I \right) \left( M_k \otimes I \right)_{AB}$$

$$= \text{Lemma } p_k d^2 \text{Tr}_{A' A} \left( | \varphi_k \rangle \langle \varphi_k | \right) \left( M_k \otimes I \right)_{AB}$$

$$= Tp_k d^2 \cdot \frac{1}{d^2} (| \varphi_k \rangle \langle \varphi_k |)_{B}$$

$$= Tp_k (| \varphi_k \rangle \langle \varphi_k |)_{B}$$

$$= \text{Prop. } (k) = p_k \text{ conditioned on outcome } k.$$
Lemma: \( \text{tr}_1 \left( N_1 \otimes I_2 \right) (Y_{12}) = \text{tr}_1 (Y_{12}) (N_2 \otimes I_2) \)

\[ \]

Proof: by linearity, it suffices to check for \( N_1 = 1 : X_{ij} \) and \( Y_{12} = 1 : K_{ij} \otimes 1 \times n \times n \).

LHS = \( \text{tr}_2 \left( X_{ij} \otimes 1 \times n \times n \right) = \delta_{jk} \delta_{di} \otimes 1 \times n \times n \)

RHS = \( \text{tr}_2 \left( K_{ij} \otimes 1 \times n \times n \right) = \delta_{jk} \delta_{di} \otimes 1 \times n \times n \).

\( \text{Lemma holds for } N, Y. \)
Let \( R \) be the rate of a d-dim quantum sys (with average \( \frac{1}{d} \))

The key has to take \( d^2 \) values.

Taking into account data compression (next topic), \( \log d \) key bits are needed.

NB: \( \log d \) key bits are necessary and sufficient for encrypting a d-state classical message.

\[ \text{Proof:} \quad \text{from Thm 2.1, if \ by contradiction, \ there \ is an encryption scheme with fewer than } d^2 \ \text{key states, then we can transmit } \log d \ \text{qubits using fewer than } 2\log d \ \text{bits, contradicting optimality of generalized teleportation.} \]

There is a 1:1 correspondence between

NB: Thms 2-2 show that generalized teleportation is generalized quantum encryption.