Quantum Cryptography and Computing Workshop

Fields Institute, October 2006

Private Quantum Channels

by

Alain Tapp

in collaboration with

Andris Ambainis
Michele Mosca
Ronald de Wolf

Entropy (Shannon)

Let X be a random variable taking values $i \in \{1, \ldots, n\}$ with probability p_i .

$$H(X) := \sum_{i=1}^{n} -p_i \log p_i$$

Let X and Y be two random variables with joint distribution $p_{(x,y)}$ where $1 \leq x \leq n$ and $1 \leq y \leq m$. Note that $p_{(x|y)} = p_{(x,y)}/p_y$.

$$H(X,Y) := \sum_{x,y} -p_{(x,y)} \log p_{(x,y)}$$

$$H(X|Y) := \sum_{x,y} -p_{(x,y)} \log p_{(x|y)}$$

Entropy (Shannon)

$$0 \leq H(X) \leq \log n$$

$$H(X) = 0 \text{ iff } \exists i, p_i = 1$$

$$H(X) = \log n \text{ iff } \forall i, p_i = 1/n$$

$$H(X,Y) = H(X) + H(Y|X)$$

$$H(Y|X) = H(X,Y) - H(X)$$

$$H(X,Y|Z) = H(X|Z) + H(Y|X,Z)$$

Theorem: [Shannon49]
For the private transmission of an n bit message it is sufficient and necessary to share a private random key having n bits of entropy.

Proof (sufficient):
M =message, C =ciphertext, K =private key
Vernam's cipher or *one time pad*.

$$\begin{array}{rcccccc} M & = & 0 & 0 & 1 & 0 & 1 & 1 \\ K & = & 1 & 0 & 0 & 1 & 1 & 0 \\ \hline M \oplus K = C & = & 1 & 0 & 1 & 1 & 0 & 1 \\ \hline C \oplus K = M & = & 0 & 0 & 1 & 0 & 1 & 1 \end{array}$$

Knowing only C, every possible message M' is consistent with the use of the key $K' = M' \oplus C$.

Theorem: [Shannon49]
For the private transmission of an n bit message it is sufficient and necessary to share a private random key having n bits of entropy.

Proof (sufficient):
M =message, C =ciphertext, K =private key

$$H(K) = n \quad \rightarrow H(C|M) = n \quad \rightarrow H(C) = n$$

$$\begin{aligned} H(M|C) &= H(M,C) - H(C) \\ &= H(M,C) - n \\ &= H(C|M) + H(M) - n \\ &= n + H(M) - n \\ &= H(M) \end{aligned}$$

Theorem: [Shannon49]
For the private transmission of an n bit message it is sufficient and necessary to share a private random key having n bits of entropy.

Proof (necessary):
M =message, C =ciphertext, K =private key
and H is the Shannon entropy function.

$$H(M|C,K) = 0 \qquad H(M|C) = H(M)$$

$$H(M,K|C) =$$

$$H(K|C) + H(M|K,C) = H(M|C) + H(K|M,C)$$

$$H(K|C) = H(M) + H(K|M,C)$$

$$H(K) \geq H(M)$$

Main result

Theorem [AMTW00]:
For the private transmission of an n qubit message it is sufficient and necessary to share a private random key having $2n$ bits of entropy.

Private Quantum Channels (PQC)

$$[\mathcal{S} \subseteq \mathcal{H}_{2^n},\ \mathcal{E} = \{(p_i, U_i) | 0 \leq i < N\},\ \rho_a \in \mathcal{H}_{2^m},\ \rho_0 \in \mathcal{H}_{2^{m+n}}]$$

form a PQC iff

$$\forall\ |\psi\rangle \in \mathcal{S}, \quad \mathcal{E}(|\psi\rangle\langle\psi| \otimes \rho_a) = \sum_{i=0}^{N-1} p_i U_i (|\psi\rangle\langle\psi| \otimes \rho_a) U_i^\dagger = \rho_0$$

The private key:

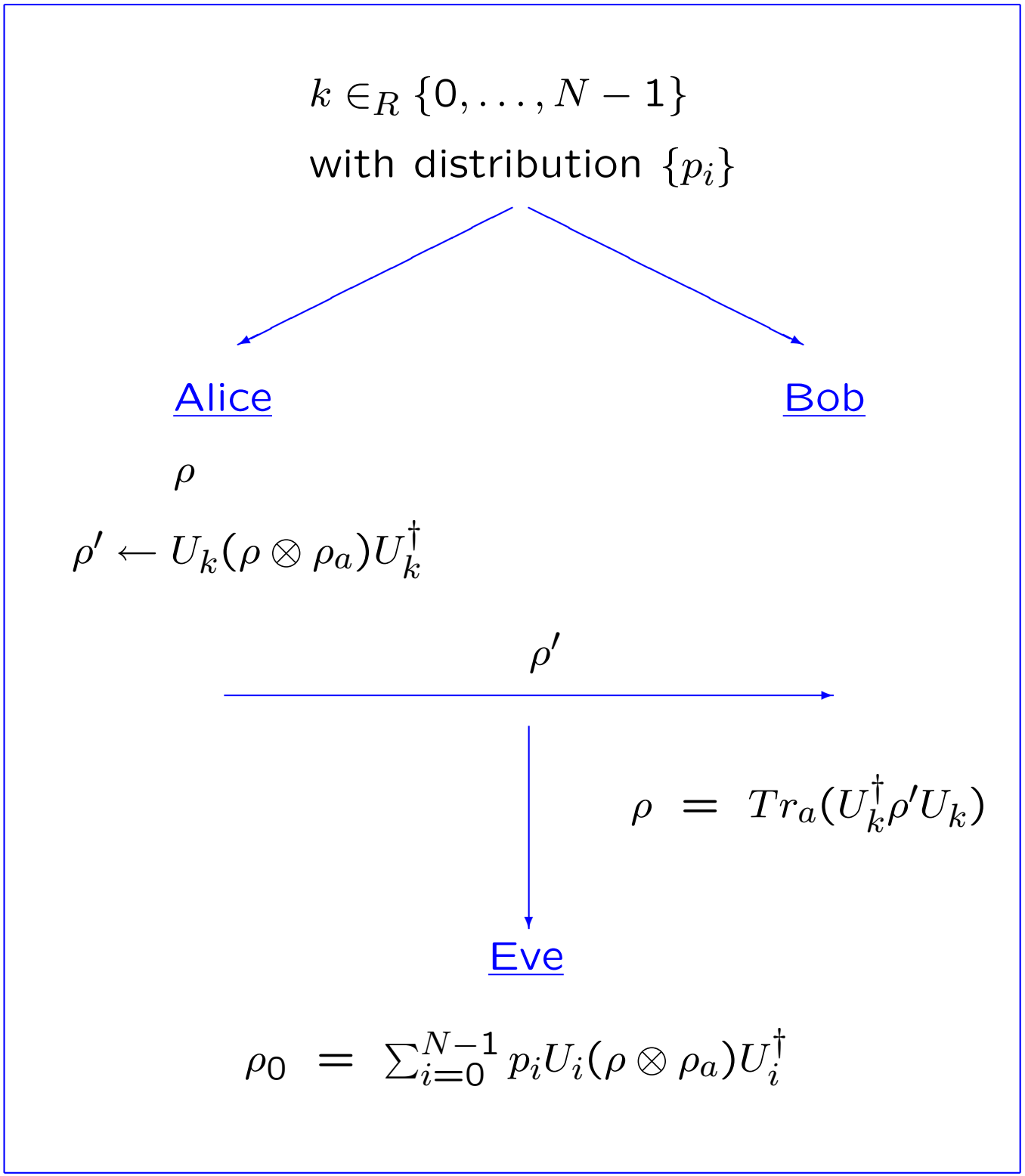
$k \in_R \{i \mid 0 \leq i < N\}$ with distribution $\{p_i\}$.

Encryption:

$$E(\rho, k) \ = \ U_k(\rho \otimes \rho_a)U_k^\dagger \ = \ \rho'$$

Decryption:

$$D(\rho', k) \ = \ \mathrm{Tr}_a(U_k^\dagger \rho' U_k) \ = \ \rho$$


$k \in_R \{0, \ldots, N-1\}$
with distribution $\{p_i\}$
Alice
Bob
ρ
$\rho' \leftarrow U_k(\rho \otimes \rho_a)U_k^\dagger$
ρ'
$\rho = Tr_a(U_k^\dagger \rho' U_k)$
Eve
$\rho_0 = \sum_{i=0}^{N-1} p_i U_i(\rho \otimes \rho_a)U_i^\dagger$

Pauli Matrices

$$
\begin{aligned}
I &= \sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\
X &= \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\
Y &= \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \\
Z &= \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}
\end{aligned}
$$

$$\forall i, \quad \sigma_i = \sigma_i^\dagger$$

$$\forall i, j, (i \neq 0 \neq j \neq i) \quad \sigma_i \sigma_j = -\sigma_j \sigma_i$$

$$\sigma_1 \sigma_2 = i\sigma_3 \quad \sigma_3 \sigma_1 = i\sigma_2 \quad \sigma_2 \sigma_3 = i\sigma_1$$

PQC: Example 1

$$\mathcal{S} = \{|0\rangle, |1\rangle\} \qquad \rho_a = 1$$

$$\mathcal{E} = \{(1/2, I), (1/2, X)\}$$

$$\rho_0 = \frac{1}{2} I \qquad H(\{p_i\}) = 1$$

Clearly this forms a **PQC** since

$$\begin{aligned}
\mathcal{E}(|0\rangle\langle 0|) &= \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2} X|0\rangle\langle 0| X = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| \\
&= \frac{1}{2} I = \rho_0 \\
&= \frac{1}{2}|1\rangle\langle 1| + \frac{1}{2}|0\rangle\langle 0| = \frac{1}{2}|1\rangle\langle 1| + \frac{1}{2} X|1\rangle\langle 1| X \\
&= \mathcal{E}(|1\rangle\langle 1|)
\end{aligned}$$

PQC: Example 2

$$\mathcal{S} = \{|0\rangle, \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\} \qquad \rho_a = 1$$

$$\mathcal{E} = \{(1/2, I), (1/2, W)\}$$

$$\rho_0 = \begin{pmatrix} 3/4 & 1/4 \\ 1/4 & 1/4 \end{pmatrix} \qquad H(\{p_i\}) = 1$$

$$W = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = W^\dagger$$

$$W|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$W^2 = I$$

PQC: Example 2

Clearly this forms a **PQC** since

$$\begin{aligned}
\mathcal{E}(|0\rangle\langle 0|) &= \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}W|0\rangle\langle 0|W \\
&= \begin{pmatrix} 3/4 & 1/4 \\ 1/4 & 1/4 \end{pmatrix} \\
&= \rho_0 \\
&= \frac{1}{2}W|0\rangle\langle 0|W + \frac{1}{2}W^2|0\rangle\langle 0|W^2 \\
&= \mathcal{E}(W|0\rangle\langle 0|W) \\
&= \mathcal{E}\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\ \frac{1}{\sqrt{2}}(\langle 0| + \langle 1|)\right)
\end{aligned}$$

PQC: Example 3

$$\mathcal{S} = \{\cos\theta|0\rangle + \sin\theta|1\rangle \mid 0 \leq \theta < 2\pi\}$$

$$\rho_a = 1 \qquad \mathcal{E} = \{(1/2, I), (1/2, Y)\}$$

$$\rho_0 = \frac{1}{2}I \qquad H(\{p_i\}) = 1$$

Clearly this forms a **PQC** since

$$\begin{aligned} \rho &= \begin{pmatrix} \cos^2\theta & \cos\theta\sin\theta \\ \sin\theta\cos\theta & \sin^2\theta \end{pmatrix} \\ Y\rho Y &= \begin{pmatrix} \sin^2\theta & -\cos\theta\sin\theta \\ -\sin\theta\cos\theta & \cos^2\theta \end{pmatrix} \end{aligned}$$

$$\mathcal{E}(\rho) = \frac{1}{2}I\ \rho\ I + \frac{1}{2}Y\ \rho\ Y = \frac{1}{2}I$$

PQC: Example 4

$$\mathcal{S} = \mathcal{H}_2 \qquad \rho_a = 1$$

$$\mathcal{E} = \{(1/4, I), (1/4, \sigma_x), (1/4, \sigma_y), (1/4, \sigma_z)\}$$

$$\rho_0 = \frac{1}{2}I \qquad H(\{p_i\}) = 2$$

Clearly this forms a **PQC** since for all ρ

$$\begin{aligned}
\mathcal{E}(\rho) &= \frac{1}{4}I\ \rho\ I + \frac{1}{4}X\rho X + \frac{1}{4}Y\rho Y + \frac{1}{4}Z\rho Z \\
&= \frac{1}{4}\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \frac{1}{4}\begin{pmatrix} d & c \\ b & a \end{pmatrix} + \frac{1}{4}\begin{pmatrix} d & -c \\ -b & a \end{pmatrix} + \frac{1}{4}\begin{pmatrix} a & -b \\ -c & d \end{pmatrix} \\
&= \frac{1}{2}I
\end{aligned}$$

Lemma 1:
If $\frac{1}{2^n}I \in \mathcal{S}$ and $\rho_a = 1$ then $\rho_0 = \frac{1}{2^n}I$.

Proof:

$$\rho_0 = \mathcal{E}(\frac{1}{2^n}I) = \sum_{i=0}^{N-1} p_i U_i \left(\frac{1}{2^n}I\right) U_i^\dagger = \frac{1}{2^n}I$$

Lemma 2:
If $\forall\ |\psi\rangle \in \mathcal{H}_{2^n},\ \mathcal{E}(|\psi\rangle\langle\psi| \otimes \rho_a) = \rho_0$ then
$\mathcal{E}(|x\rangle\langle y| \otimes \rho_a) = 0$ whenever $x \neq y$.

Proof:

$$
\begin{aligned}
1)\ \rho_0 &= \mathcal{E}(\frac{1}{2}(|x\rangle\langle x| + |y\rangle\langle y|) \\
&= \frac{1}{2}(\mathcal{E}(|x\rangle\langle x|) + \mathcal{E}(|y\rangle\langle y|)) \\
2)\ \rho_0 &= \mathcal{E}(\frac{1}{\sqrt{2}}(|x\rangle + |y\rangle)\ \frac{1}{\sqrt{2}}(\langle x| + \langle y|)) \\
&= \frac{1}{2}(\mathcal{E}(|x\rangle\langle x|) + \mathcal{E}(|x\rangle\langle y|) + \mathcal{E}(|y\rangle\langle x|) + \mathcal{E}(|y\rangle\langle y|)) \\
3)\ \rho_0 &= \mathcal{E}(\frac{1}{\sqrt{2}}(|x\rangle + i|y\rangle)\ \frac{1}{\sqrt{2}}(\langle x| - i\langle y|)) \\
&= \frac{1}{2}(\mathcal{E}(|x\rangle\langle x|) + \mathcal{E}(|y\rangle\langle y|) - i\mathcal{E}(|x\rangle\langle y|) + i\mathcal{E}(|y\rangle\langle x|))
\end{aligned}
$$

By 1) and 2) $\Rightarrow\ \mathcal{E}(|x\rangle\langle y|) + \mathcal{E}(|y\rangle\langle x|) = 0$
By 1) and 3) $\Rightarrow\ \mathcal{E}(|x\rangle\langle y|) - \mathcal{E}(|y\rangle\langle x|) = 0$
and thus $\mathcal{E}(|x\rangle\langle y|) = \mathcal{E}(|y\rangle\langle x|) = 0$.

Theorem [concatenation]
If $[\mathcal{H}_{2^n}, \mathcal{E}, \rho_a, \rho_0]$ and $[\mathcal{H}_{2^m}, \mathcal{E}', \rho'_a, \rho'_0]$ are PQC then $[\mathcal{H}_{2^{n+m}}, \mathcal{E} \otimes \mathcal{E}', \rho_a \otimes \rho'_a, \rho_0 \otimes \rho'_0]$ is a PQC.

Proof:

$$
\begin{aligned}
(\mathcal{E} \otimes \mathcal{E}')(|\psi\rangle\langle\psi|) &= (\mathcal{E} \otimes \mathcal{E}') \left(\sum_{x,y} \alpha_{x,y} |x\rangle|y\rangle \right) \left(\sum_{x',y'} \alpha^*_{x',y'} \left\langle x' \right| \left\langle y' \right| \right) \\
&= (\mathcal{E} \otimes \mathcal{E}') \left(\sum_{x,y,x',y'} \alpha_{x,y} \ \alpha^*_{x',y'} \, |x\rangle \left\langle x' \right| \otimes |y\rangle \left\langle y' \right| \right) \\
&= \sum_{x,y,x',y'} \alpha_{x,y} \ \alpha^*_{x',y'} \ \mathcal{E}(|x\rangle \left\langle x' \right|) \otimes \mathcal{E}'(|y\rangle \left\langle y' \right|) \\
&\stackrel{*}{=} \sum_{x,y} \alpha_{x,y} \ \alpha^*_{x,y} \ \mathcal{E}(|x\rangle\langle x|) \otimes \mathcal{E}'(|y\rangle\langle y|) \\
&= \sum_{x,y} |\alpha_{x,y}|^2 \ \rho_0 \otimes \rho'_0 \\
&= \rho_0 \otimes \rho'_0
\end{aligned}
$$

Theorem [AMTW00, sufficient]:
For the private transmission of an n qubit message it is sufficient to share a private random key having $2n$ bits of entropy.

Proof: By theorem [concatenation], to encode an n qubit register we can use the one qubit encoding method of example 4 several times.

Equivalent super operator

Every equivalent super operators are unitarely related.

For the two encryption scheme $\mathcal{E}$ and $\mathcal{E}'$,

$$\mathcal{E} = \{(p_i, U_i) | 1 \leq i \leq N\}$$

$$\mathcal{E}' = \{(p'_i, U'_i) | 1 \leq i \leq N' \leq N\}$$

there exists a N by N *unitary* matrix A such that

$$\sqrt{p_i} U_i = \sum_{i=1}^{N} A_{i,j} \sqrt{p'_j} U'_j$$

with $U'_j = 0$ for $j > N'$.

Matrix vector space

The N by N operators form a N^2 dimentionnal vector space with the inner product

$$\langle M, M' \rangle \;=\; Tr(M^\dagger M')/N$$

and norm

$$\|M\| = \sqrt{\langle M, M \rangle}$$

For $x \in \{0,1,2,3\}^n$ we define (the base 4 representation)

$$\overline{\sigma_x} \;=\; \sigma_{x_1} \otimes \sigma_{x_2} \otimes \cdots \otimes \sigma_{x_n}$$

The $\overline{\sigma_x}$ form an orthonormal basis of the vector space.

$$\forall x, \|\overline{\sigma_x}\| = 1$$

$$\forall x \neq y, \langle\, \overline{\sigma_x}, \overline{\sigma_y} \rangle = 0$$

Theorem

If $[\mathcal{S} = \mathcal{H}_{2^n}, \mathcal{E} = \{(p_i, U_i) \mid 0 \leq i < N\}, 1, \rho_0]$ is a **PQC** then $H(\{p_i\}) \geq 2n$.

Proof:

Since $I_{2^n} \in \mathcal{H}_{2^n}$ by lemma 1 we must have $\rho_0 = I_{2^n}$. Let $[\mathcal{S} = \mathcal{H}_{2^n}, \mathcal{E}' = \{(1/2^n, \overline{\sigma_i})\ 0 \leq i < 2^n\}, 1, I_{2^n}]$ be the **PQC** given by theorem (sufficient).

If $i > N$ then $U_i = 0$ and if $i > 2^{2n}$ then $\overline{\sigma_i} = 0$

$$p_i = \|\sqrt{p_i}U_i\|^2 = \|\sum_x A_{i,x}\sqrt{p'_i}\frac{1}{\sqrt{2^{2n}}}U_i\|^2 = \frac{1}{2^{2n}}\sum_x |A_{i,x}|^2 \leq \frac{1}{2^{2n}}$$

Hence $N \geq 2^{2n}$ and $H(\{p_i\}) \geq 2n$.

What append if the encryption scheme uses an encilla?

Von Neumann entropy

Definition:
Let

$$\rho = \sum_{i=1}^{N} p_i \left|\phi_i\right\rangle \left\langle\phi_i\right|$$

for $|\phi_i\rangle$ an orthonormal basis then the *Von Neumann entropy* of ρ is

$$S(\rho) = H(p_1, \ldots, p_N) = -\sum_{i=1}^{N} p_i \log p_i,$$

where H is the classical entropy function.

Von Neumann entropy

Some properties of $S(\rho)$

1) $S(|\phi\rangle\langle\phi|) = 0$, for every pure state $|\phi\rangle$.

2) $S(\rho_1 \otimes \rho_2) = S(\rho_1) + S(\rho_2)$.

3) $S(U\rho U^\dagger) = S(\rho)$.

4) If $\lambda_i \geq 0$ and $\sum_i \lambda_i = 1$ then $\quad S(\sum_i \lambda_i \rho_i) \geq \sum_i \lambda_i S(\rho_i)$

5) If $\rho = \sum_{i=1}^N p_i \, |\phi_i\rangle\langle\phi_i|$ with the $|\phi_i\rangle$ not necessarily orthogonal, then $S(\rho) \leq H(p_1, \ldots, p_N)$.

6) $S\left(\frac{1}{2^n} I\right) = n$.

Theorem [classical channel]
If $[\mathcal{S} = \{|i\rangle \mid 0 \leq i < 2^k\}, \mathcal{E} = \{(p_i, U_i)\}, \rho_a, \rho_0]$ is a PQC then $H(\{p_i\}) \geq k$.

Proof:
Let $\rho_a = \sum_{j=0}^{M-1} q_j \left|\Psi_j\right\rangle \left\langle\Psi_j\right|$ then

$$\begin{aligned}
S(\rho_0) &= S(\mathcal{E}(|0\rangle\langle 0|)) \\
&= S\left(\sum_{i=0}^{N-1} p_i U_i |0\rangle\langle 0| \otimes \rho_a U_i^\dagger\right) \\
&= S\left(\sum_{i=0}^{N-1}\sum_{j=0}^{M-1} p_i q_j U_i |0\rangle\langle 0| \otimes \left|\Psi_j\right\rangle \left\langle\Psi_j\right| U_i^\dagger\right) \\
&\leq H(p_0 q_0, p_0 q_1, \ldots, p_{N-1} q_{M-1}) \\
&= H(\{p_i\}) + H(\{q_i\}) \\
&= H(\{p_i\}) + S(\rho_a)
\end{aligned}$$

Again $\rho_a = \sum_{j=0}^{M-1} q_j \left|\Psi_j\right\rangle\left\langle\Psi_j\right|$ then

$$\begin{aligned} S(\rho_0) &= S(\mathcal{E}(\frac{1}{2^k}I)) \\ &= S\left(\sum_{i=0}^{N-1} p_i U_i(\frac{1}{2^k}I \otimes \rho_a)U_i^\dagger\right) \\ &\geq \left(\sum_{i=0}^{N-1} p_i S(\frac{1}{2^k}I \otimes \rho_a)\right) \\ &= k + S(\rho_a) \end{aligned}$$

Since we have $S(\rho_0) \leq H(\{p_i\}) + S(\rho_a)$ and $S(\rho_0) \geq k + S(\rho_a)$ we conclude that $H(\{p_i\}) \geq k$.

Theorem [AMTW00, necessary]:
If $[\mathcal{S} = \mathcal{H}_{2^n}, \mathcal{E} = \{(p_i, U_i)\}, \rho_a, \rho_0]$ is a **PQC** then $H(\{p_i\}) \geq 2n$.

Proof:
$[\mathcal{S}' = \{|x\rangle | 0 \leq x < 2^{2n}\}, \mathcal{E}', \rho_a, \left(\frac{1}{2^n} I\right) \otimes \rho_0]$
is a **PQC** where

$$\mathcal{E}' = \{(p_i, (I_{2^n} \otimes U_i)(U \otimes I_{2^k})) \mid 0 \leq i < N\}$$

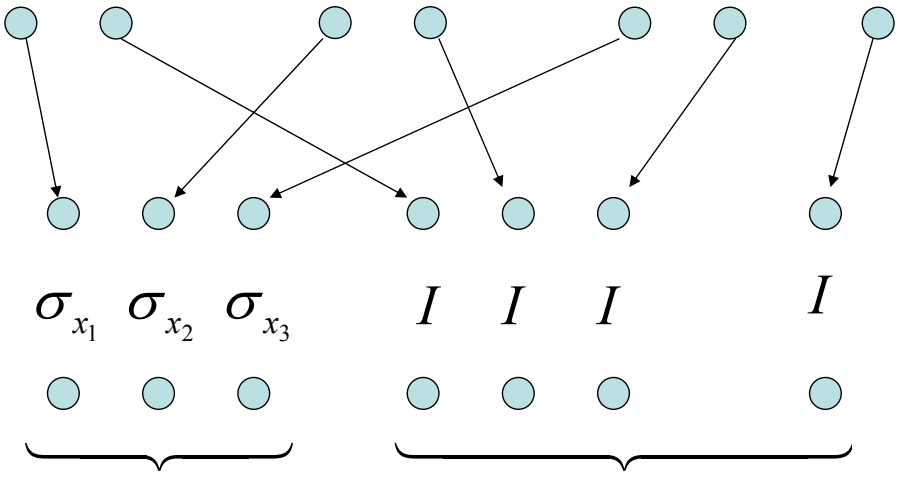
$$U|x\rangle \rightarrow (\sigma_{x_1} \otimes \cdots \otimes \sigma_{x_n} \otimes I_{2^n}) \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n - 1} |i\rangle |i\rangle$$

and $\{0, \ldots, 2^{2n} - 1\} \equiv \{0, 1, 2, 3\}^n$.

This **PQC** convey $2n$ classical bit therefor from the previous theorem we conclude that

$$H(\{p_i\}) \geq 2n.$$

$$|x\rangle \qquad \left(\frac{|00\rangle+|11\rangle}{\sqrt{2}}\right)\otimes\left(\frac{|00\rangle+|11\rangle}{\sqrt{2}}\right)\otimes\left(\frac{|00\rangle+|11\rangle}{\sqrt{2}}\right)\otimes\rho$$



$$I_{2^n}\otimes\rho_0$$

$$
\begin{aligned}
&\mathcal{E}'(|x\rangle\langle x|) \\
&= \sum_{i=1}^{N} p_i (I_{2^n} \otimes U_i)(U \otimes I_{2^k}) \ (|x\rangle\langle x| \otimes \rho_a) \ (U \otimes I_{2^k})^\dagger (I_{2^n} \otimes U_i)^\dagger \\
&= \sum_{i=1}^{N} p_i (I_{2^n} \otimes U_i) \ ([U|x\rangle\langle x|U^\dagger] \otimes \rho_a) \ (I_{2^n} \otimes U_i)^\dagger \\
&= \sum_{i=1}^{N} p_i (I_{2^n} \otimes U_i) \left[(\overline{\sigma_x} \otimes I_{2^n}) \left(\frac{1}{\sqrt{2^n}} \sum_{y=0,z=0}^{2^n-1} |y\rangle|y\rangle\langle z|\langle z| \right) (\overline{\sigma_x} \otimes I_{2^n})^\dagger \right] \otimes \rho_a \ (I_{2^n} \otimes U_i)^\dagger \\
&= \sum_{i=1}^{N} p_i (I_{2^n} \otimes U_i) \left[(\overline{\sigma_x} \otimes I_{2^{n+k}}) \left(\frac{1}{\sqrt{2^n}} \sum_{y=0,z=0}^{2^n-1} |y\rangle|y\rangle\langle z|\langle z| \otimes \rho_a \right) (\overline{\sigma_x} \otimes I_{2^{n+k}})^\dagger \right] \ (I_{2^n} \otimes U_i)^\dagger \\
&= (\overline{\sigma_x} \otimes I_{2^{n+k}}) \left[\frac{1}{2^n} \sum_{i=1}^{N} p_i (I_{2^n} \otimes U_i) \left(\sum_{y,z \in \{0,2^n-1\}} |y\rangle\langle z| \otimes |y\rangle\langle z| \otimes \rho_a \right) (I_{2^n} \otimes U_i)^\dagger \right] (\overline{\sigma_x} \otimes I_{2^{n+k}})^\dagger \\
&= (\overline{\sigma_x} \otimes I_{2^{n+k}}) \left[\frac{1}{2^n} \sum_{y,z \in \{0,2^n-1\}} |y\rangle\langle z| \otimes \left(\sum_{i=1}^{N} p_i U_i (|y\rangle\langle z| \otimes \rho_a) U_i^\dagger \right) \right] (\overline{\sigma_x} \otimes I_{2^{n+k}})^\dagger
\end{aligned}
$$

$$
\begin{aligned}
&\mathcal{E}'(|x\rangle\langle x|) \\
&= (\overline{\sigma_x} \otimes I_{2^{n+k}}) \left[\frac{1}{2^n} \sum_{y,z \in \{0,2^n-1\}} |y\rangle\langle z| \otimes \left(\sum_{i=1}^{N} p_i U_i (|y\rangle\langle z| \otimes \rho_a) U_i^\dagger \right) \right] (\overline{\sigma_x} \otimes I_{2^{n+k}})^\dagger \\
&= (\overline{\sigma_x} \otimes I_{2^{n+k}}) \left[\frac{1}{2^n} \sum_{y,z \in \{0,2^n-1\}} |y\rangle\langle z| \otimes \mathcal{E}(|y\rangle\langle z|) \right] (\overline{\sigma_x} \otimes I_{2^n})^\dagger \\
&\overset{*}{=} (\overline{\sigma_x} \otimes I_{2^n}) \left[\frac{1}{2^n} \sum_{y=0}^{2^n-1} |y\rangle\langle y| \otimes \mathcal{E}(|y\rangle\langle y|) \right] (\overline{\sigma_x} \otimes I_{2^{n+k}})^\dagger \\
&= (\overline{\sigma_x} \otimes I_{2^n}) \left[\tilde{I}_{2^n} \otimes \rho_0 \right] (\overline{\sigma_x} \otimes I_{2^n})^\dagger \\
&= \tilde{I}_{2^n} \otimes \rho_0 .
\end{aligned}
$$

Conclusion

Theorem: [Shannon49]
For the private transmission of an n bit message it is sufficient and necessary to share a private random key having n bits of entropy.

Theorem: [AMTW00]
For the private transmission of an n qubit message it is sufficient and necessary to share a private random key having $2n$ bits of entropy.