

$$\Phi: M_n \rightarrow M_m$$

Theorem For every quantum operation on an open system $\Phi : M_n \rightarrow M_m$ there exist $r \in \mathbb{N}$ and $F_1, \dots, F_r \in M_{m,n}$ such that $\sum_{j=1}^r F_j^\dagger F_j = I_n$ and

$$\Phi(A) = \sum_{j=1}^r F_j A F_j^\dagger \quad \text{for all } A \in M_n.$$

$m \times n$

$m \times m$

This is called the operator sum representation of the quantum operation. The matrices F_1, \dots, F_r are called the Kraus operators of the operations.

Proof. Suppose $\Phi : M_n \rightarrow M_m$ is a quantum operation.

We may assume that $\Phi(\rho)$ is the partial trace of

$$U(\sigma \otimes \rho)U^\dagger \in M_{nk} \quad \text{with } nk = mr.$$

Here U may depend on t . By purification, we may assume that $\sigma = E_{11}$ so that

$$U(\sigma \otimes \rho)U^\dagger = U \begin{pmatrix} \rho & 0 \\ 0 & 0 \end{pmatrix} U^\dagger = \begin{pmatrix} F_1 \\ \vdots \\ F_r \end{pmatrix} \rho (F_1^* | \dots | F_r^*)$$

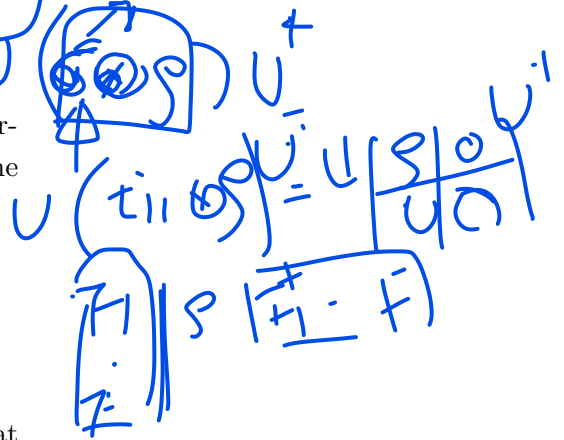
with diagonal blocks $F_1 \rho F_1^\dagger, \dots, F_r \rho F_r^\dagger$ so that

$$\text{tr}_1(U(\sigma \otimes \rho)U^\dagger) = \sum_{j=1}^r F_j \rho F_j^\dagger.$$

Here $(F_1^\dagger, \dots, F_r^\dagger)$ are the first n rows of U^\dagger .

Thus, $\sum_{j=1}^r F_j^\dagger F_j = I_n$.

$$\Phi(A) =$$

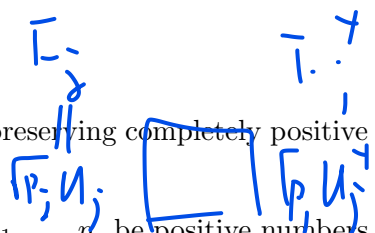


Remark quantum channels are trace preserving completely positive linear maps.

Example Let $U_1, \dots, U_r \in U(n)$ and p_1, \dots, p_r be positive numbers summing up to 1. Then $\Phi : M_n \rightarrow M_n$ defined by

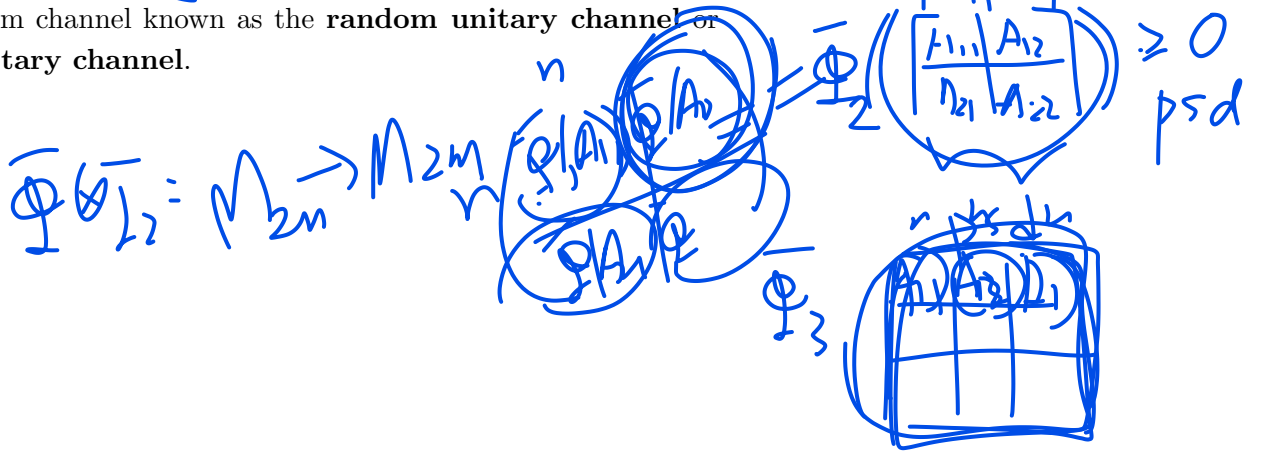
$$\Phi(A) = \sum_{j=1}^r p_j U_j A U_j^\dagger \quad \text{for all } A \in M_n$$

is a quantum channel known as the **random unitary channel** or **mixed unitary channel**.



$$\Phi(\rho) = \sigma$$

$$\rho \otimes \Phi(A) = B$$



Quantum channels and Measurements

When a quantum state ρ is transmitted through a quantum channel, it will interact with the external environment. So, we may regard the transmission as a process of letting the quantum state going through a quantum operation of an open system, and assume the received state has the form

$$\hat{\rho} = \sum_{j=1}^r F_j \rho F_j^\dagger.$$

Here F_1, \dots, F_r are the Kraus operators caused by the influence of the environment on ρ . In this context, F_1, \dots, F_r are known as the **error operators**.

Positive Operator-Valued Measure (POVM)

- Eigenprojections of A .

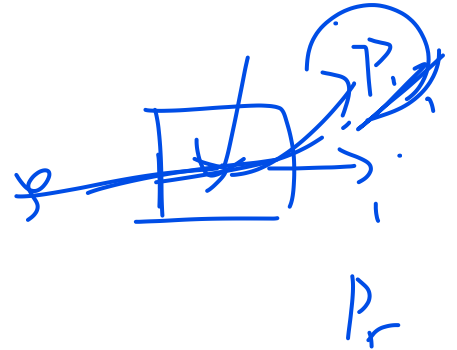
Quantum measurements can be viewed as quantum operations on open systems. As mentioned before a Hermitian matrix $A = \sum_{j=1}^n \lambda_j |\lambda_j\rangle\langle\lambda_j|$ is associated with an observable. If a state $\rho \in D_n$ goes through the measurement process corresponding to A , the state ρ will “collapse” to one of the pure states $|\lambda_j\rangle\langle\lambda_j|$ with a probability $\text{tr}(A\rho)$.

- Projective measurement.

In general, if $A = \sum_{j=1}^s \lambda_j P_j$, where P_j is the projection operator corresponding to the eigenvalue λ_j for the distinct eigenvalues $\lambda_1, \dots, \lambda_s$ of A . In such a case, the **projective measurement** of ρ under the measurement associated with A is the quantum operation

$$\rho \mapsto \sum_j P_j \rho P_j, \quad F_j^\dagger = F_j$$

where $p_j = \text{tr}(P_j \rho P_j) = \text{tr}(\rho P_j)$ and the set $\{P_1, \dots, P_r\}$ satisfies the completeness relation $\sum_j P_j P_j^\dagger = \sum_j P_j = I$.

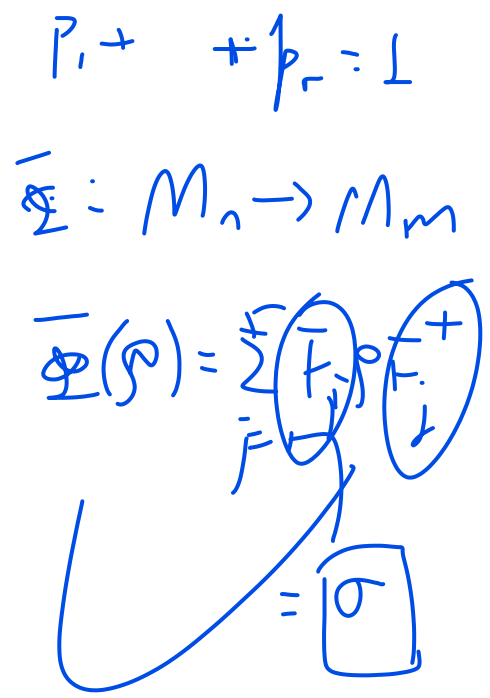
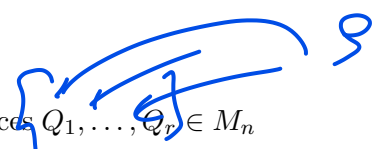


- POVM. for any positive semidefinite matrices $Q_1, \dots, Q_r \in M_n$ such that $Q_1 + \dots + Q_r = I_n$, there are $M_1, \dots, M_r \in M_n$ such that $M_j^\dagger M_j = Q_j$. The measurement operators are then associated with the quantum operation

$$\rho \mapsto \sum_{j=1}^r M_j \rho M_j^\dagger$$

so that ρ will change to the quantum state $\frac{1}{p_j} M_j \rho M_j^\dagger$ with a probability $p_j = \text{tr}(M_j \rho M_j^\dagger) = \text{tr}(\rho Q_j)$. The set $\{Q_1, \dots, Q_r\} = \{M_1^\dagger M_1, \dots, M_r^\dagger M_r\}$ is known as the **positive operator-valued measure (POVM)**.

Example Suppose Bob will be given a quantum state chosen from the linearly independent set of unit vectors $\{|\psi_1\rangle, \dots, |\psi_m\rangle\}$, which may not be orthonormal. He can construct the following POVM $\{Q_1, \dots, Q_{m+1}\}$ such that he will know for sure that $|\psi_j\rangle$ is sent to him if the measurement of the received state yields Q_j if $Q_j = |\phi_j\rangle\langle\phi_j|/m$, where $\langle\phi_j|\phi_j\rangle = 1$ and $\langle\phi_j|\psi_i\rangle = 0$ for all $i \neq j$ for $j = 1, \dots, m$ and $Q_{m+1} = I - \sum_{j=1}^m Q_j$. Evidently, a measurement of $|\psi_j\rangle\langle\psi_j|$ will yield Q_j or Q_{m+1} .



Fidelity

Definition Let $\rho_1, \rho_2 \in D_n$. Then the fidelity is defined by

$$F(\rho_1, \rho_2) = \left\{ \text{tr} \left(\sqrt{\sqrt{\rho_1} \rho_2 \sqrt{\rho_1}} \right) \right\}^2$$

$$\sum \lambda_i |\lambda_i| > \langle x, 1 \rangle$$

Here, $\sqrt{\rho_1}$ is the positive semi-definite square root of ρ_1 , and $\sqrt{\rho_1} \rho_2 \sqrt{\rho_1}$ is positive semi-definite so that we can take its positive semi-definite square root.

Theorem Let $\rho_1, \rho_2 \in \mathcal{S}(\mathcal{H})$. If $\rho_1^{1/2} \rho_2^{1/2}$ has singular values $s_1 \geq \dots \geq s_n$, then

$$\rho_2^{1/2} = \sqrt{\rho_2}$$

$$F(\rho_1, \rho_2) = F(\rho_2, \rho_1) = \left[\sum_{j=1}^n s_j \right]^2$$

and the following conditions hold.

- (1) For any unitary U , $F(U\rho_1 U^\dagger, U\rho_2 U^\dagger) = F(\rho_1, \rho_2)$.
- (2) If ρ_1 or ρ_2 is a pure state, then $F(\rho_1, \rho_2) = \text{tr}(\rho_1 \rho_2)$.
- (3) We have

$$F(\rho_1, \rho_2) \in [0, 1].$$

The equality $F(\rho_1, \rho_2) = 1$ holds if and only if $\rho_1 = \rho_2$. The equality $F(\rho_1, \rho_2) = 0$ holds if and only if $\text{tr}(\rho_1 \rho_2) = 0$, equivalently, $\sigma_1^r \sigma_2^s = 0$ for any positive numbers r, s .

$$\langle \rho_1, \rho_2 \rangle = \text{tr}(\rho_1 \rho_2)$$

$$\sigma_1^r \sigma_2^s = 0$$

Other numerical functions on a mixed states

- The trace distance: $\|\rho - \sigma\|_{\text{tr}}$ is the sum of the singular values of $\rho - \sigma$. $0 \leq \|\rho - \sigma\|_{\text{tr}} \leq 2$

$$U \begin{bmatrix} \rho & \\ & \sigma \end{bmatrix} U^\dagger = \begin{bmatrix} \rho & \\ & \sigma \end{bmatrix}$$

- The relative entropy of two quantum states $\rho, \sigma \in D_n$ defined by

$$S(\rho \parallel \sigma) = -\text{tr} \rho \ln \sigma + \text{tr} \rho \ln \rho = \text{tr} \rho (\ln \rho - \ln \sigma)$$

is another measure of the difference between the two quantum states. If there is $|v\rangle \in \mathbb{C}^n$ such that $\sigma|v\rangle = 0$ and $\langle v|\rho|v\rangle \neq 0$, then $S(\rho \parallel \sigma) = \infty$.

$$S_1 = S_2 = 1$$

$$U \rho U^\dagger = \begin{bmatrix} D_1 & 0 \\ 0 & 0 \end{bmatrix}$$

- The von Neumann entropy of a density matrix is defined as

$$S(\rho) = -\text{tr} (\rho \ln \rho)$$

$$U \sigma U^\dagger = \begin{bmatrix} 0 & 0 \\ 0 & D_2 \end{bmatrix}$$

where \ln is the natural log function.

$$S = -\sum_{i=1}^n \lambda_i \ln \lambda_i$$

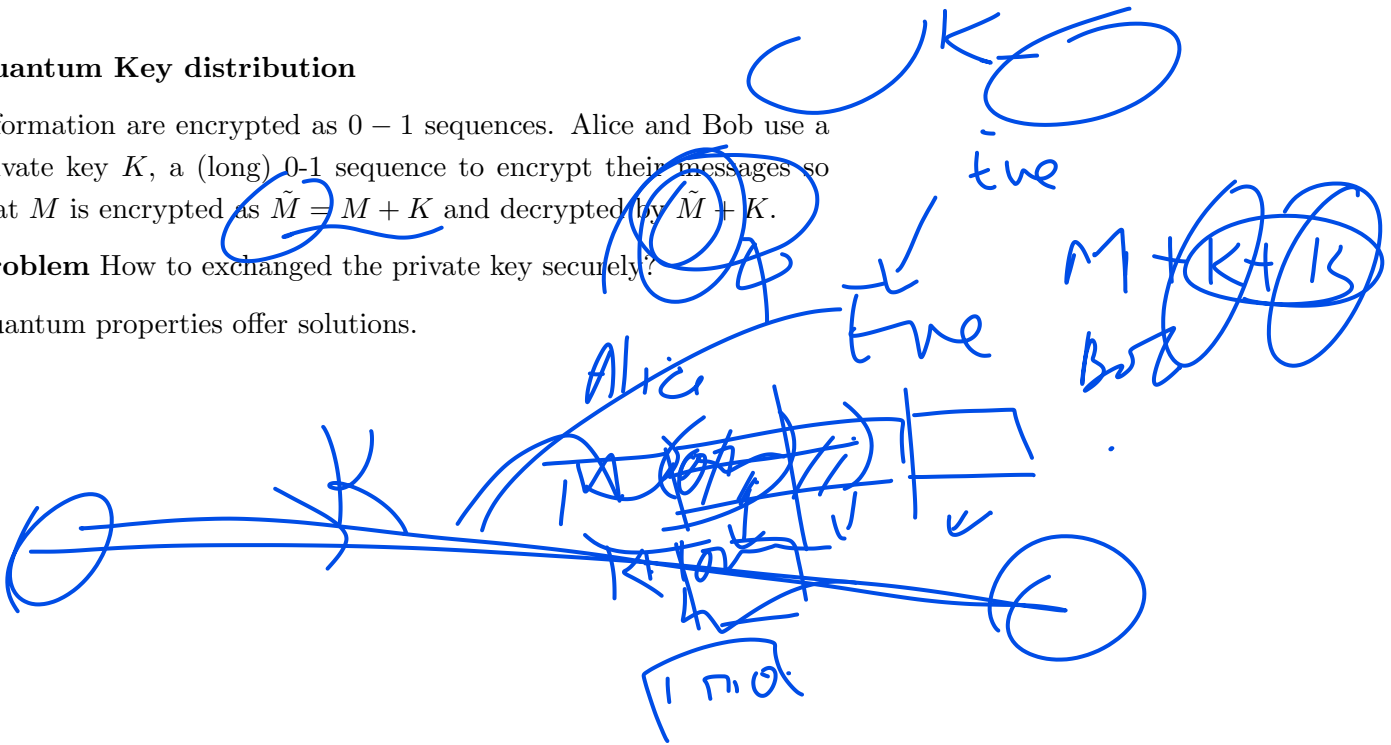
$$S = -\sum_{i=1}^n \lambda_i |\lambda_i\rangle \langle \lambda_i|$$

Quantum Key distribution

Information are encrypted as 0 - 1 sequences. Alice and Bob use a private key K , a (long) 0-1 sequence to encrypt their messages so that M is encrypted as $\hat{M} = M + K$ and decrypted by $\hat{M} + K$.

Problem How to exchanged the private key securely?

Quantum properties offer solutions.



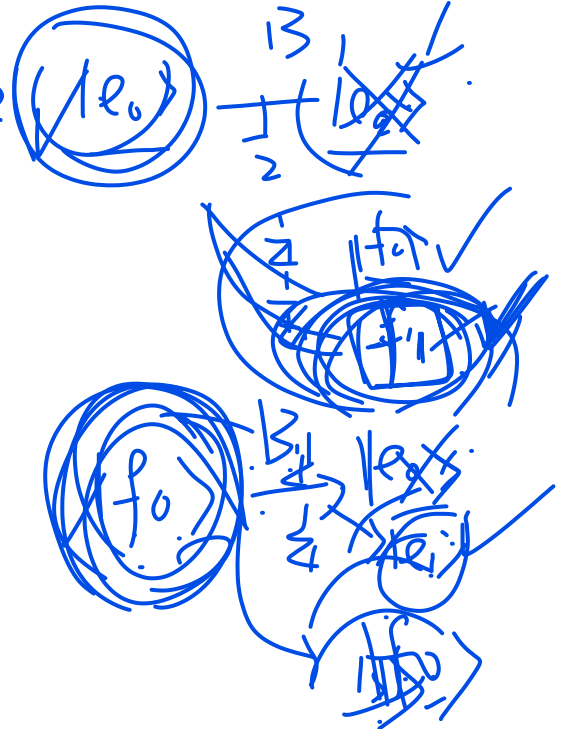
BB84 (Bennett and Brassard, 1984)

- Each of Alice and Bob use two bases for photon states: $B_1 = \{|e_0\rangle, |e_1\rangle\}$, $B_2 = \{|f_0\rangle, |f_1\rangle\}$.
- Alice sends Bob $4N$ photons, each prepared in one of the two bases randomly.
- Bob measures the received photons, each with one of the two bases randomly.
- Then they exchange notes and identify the photons that were sent and measured using the same bases. There should be roughly $2N$ such photons.
- They will use N of them to detect whether there is an eavesdropper, Eve, tampering their information.
- If Eve does intercept, the best things for her to do is to use B_1 and B_2 bases to measure the intercepted qubit, and then sends the measured qubit to Bob, using the same basis she obtains the measured result.
- Now, consider two cases. If Alice and Bob both used B_1 , they should get a perfect match of information. However, if Eve has applied B_1 or B_2 , about $1/2$ of the times she would use B_2 , and sent out the bit so that $1/2$ of the times that Bob will get the measured results agree with the photon sent by Alice.
- The same holds if both Alice and Bob used B_2 . So, roughly $1/4$ of the N -bits would disagree. Alice and Bob would deduce that someone has intercepted the information if there is a huge discrepancy in the N -bits comparison, and should retry the process.



B92 Protocol

- Alice sends $8N$ photons to Bob using $|e_0\rangle$ for 0 and $|f_0\rangle$ for 1.
- Bob measures the received photons using B_1 or B_2 randomly.
- Suppose Alice sends $|e_0\rangle$. If Bob uses B_1 , he will obtain $|e_0\rangle$; if Bob uses B_2 , he will obtain $|f_0\rangle$ or $|f_1\rangle$. If he gets $|f_1\rangle$, he knows that Alice has sent $|e_0\rangle$.
- Suppose Alice send $|f_0\rangle$. If Bob uses B_2 , he will obtain $|f_0\rangle$; if he uses B_1 , he will obtain $|e_0\rangle$ or $|e_1\rangle$. If he gets $|e_1\rangle$, he knows that Alice has sent $|f_0\rangle$.
- There are roughly $2N$ photons that Bob will know with certainty.
- He will use N of them to check the presence of Eve.
- If Eve indeed present, $1/16$ of the bits will fails to match.



Alice	Eve	Bob	Probability	Bob Reports
$ e_0\rangle$	$ e_0\rangle$	$ e_0\rangle$	$1/2 \times 1/2 = 1/4$	$1/8$
		$ f_0\rangle$	$1/4$	$1/16$
		$ f_1\rangle$	$1/4$	$1/16$ ($ e_0\rangle$)
		$ e_1\rangle$	$1/4$	$1/32$
	$ f_0\rangle$	$ e_0\rangle$	$1/4$	$1/32$
		$ e_1\rangle$	$1/4$	$1/32$ ($ f_0\rangle$ (wrong))
		$ f_0\rangle$	$1/2$	$1/16$
		$ f_1\rangle$	$1/4$	$1/32$
	$ f_1\rangle$	$ e_0\rangle$	$1/4$	$1/16$
		$ e_1\rangle$	$1/4$	$1/32$
		$ f_0\rangle$	$1/2$	$1/16$
		$ f_1\rangle$	$1/4$	$1/32$ ($ e_0\rangle$)
	$ f_0\rangle$	$ e_0\rangle$	$1/4$	$1/8$
		$ e_1\rangle$	$1/4$	$1/16$
		$ f_0\rangle$	$1/4$	$1/32$
		$ f_1\rangle$	$1/4$	$1/32$ ($ e_0\rangle$ (wrong))
$ e_1\rangle \rightarrow f_0\rangle$	$ e_0\rangle$	$1/2$	$1/16$	
	$ f_0\rangle$	$1/4$	$1/16$	
	$ e_0\rangle$	$1/4$	$1/32$	
	$ e_1\rangle$	$1/4$	$1/32$ ($ f_0\rangle$)	

$8N$
 $2N$

N

$1/16$

There are **E91** and **BBM92** protocols using entangled pairs and Bell-Inequalities to check the presence of Eve.