

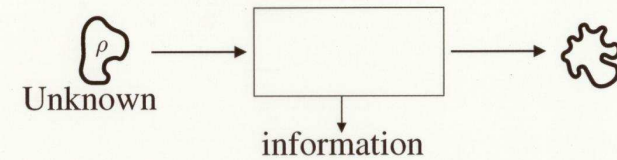
What can be done  
without disturbing states of a system?

Masato Koashi

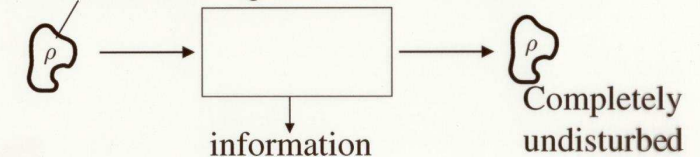
SOKEN (The Graduate University for Advanced Studies, Japan)

- Introduction
- Cloning of quantum states
- Quantum cryptography
- What are the operations that leaves the marginal density operator undisturbed?
  - Degrees of freedom are classified into 3 parts -- classical, nonclassical, and redundant.

## A fundamental property of quantum systems

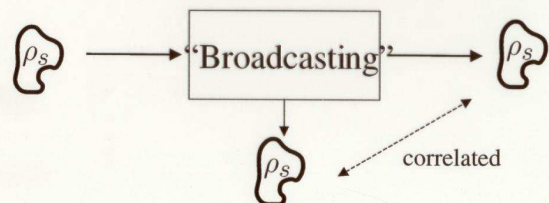
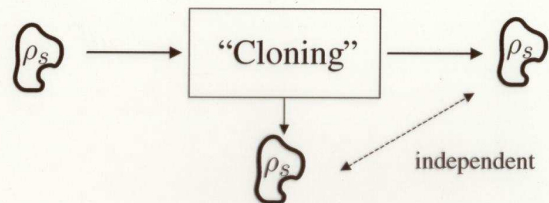


If some information is given... (ex.  $\rho$  is either  $\rho_0$  or  $\rho_1$  )

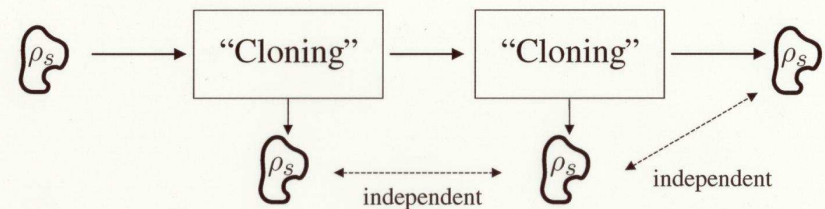


Sometimes it's possible. So when?

## Making a copy of a system



### Cloning and distinguishability



Repeating this, we may obtain infinite number of **independent** samples of  $\rho_s$

→ We can determine  $\rho_S$  from a single copy

If  $\rho_0 \neq \rho_1$ , we can distinguish the two states by a single copy.

Different states can be “cloned”.  $\longleftrightarrow$  The states are distinguishable.  
= orthogonal

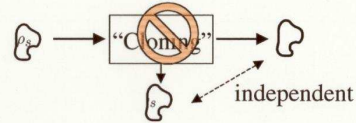
Different, but not completely distinguishable states cannot be “cloned”.

### Nonorthogonal pure states

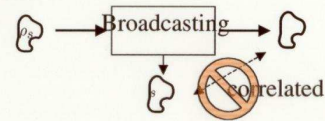
$$\rho_0 = |u_0\rangle\langle u_0| \quad \langle u_0|u_1\rangle \neq 0, 1$$

$$\rho_1 = |u_1\rangle\langle u_1|$$

They are not completely distinguishable.



Pure states cannot be correlated to other systems.



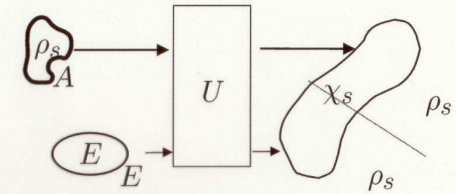
We cannot make a copy of nonorthogonal pure states by **any** means.

### Nonorthogonal mixed states may be broadcast

$$\rho_s \otimes E \longrightarrow \chi_s$$

$$\text{Tr}_E(\chi_s) = \rho_s$$

$$\text{Tr}_A(\chi_s) = \rho_s$$



When is it possible, and when is it not?

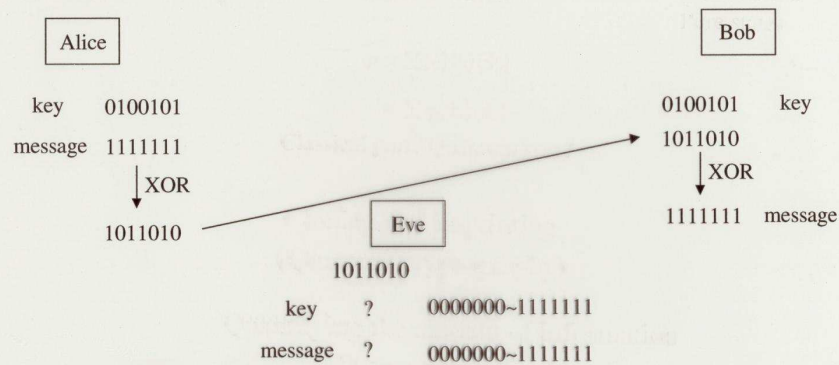
$$[\rho_0, \rho_1] = 0$$

Barnum et al., PRL **76**, 2818(1996)

### Quantum cryptography (Quantum Key Distribution)

Secret key

Random bit sequence shared by Alice and Bob



This scheme is perfectly secure if the key is used only once.

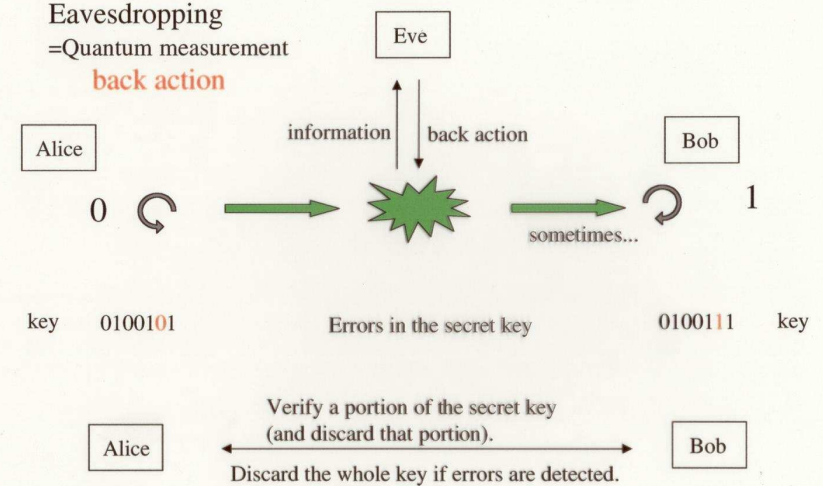
How to distribute the key? ← Quantum mechanics

### Quantum cryptography (Quantum key distribution)

Eavesdropping

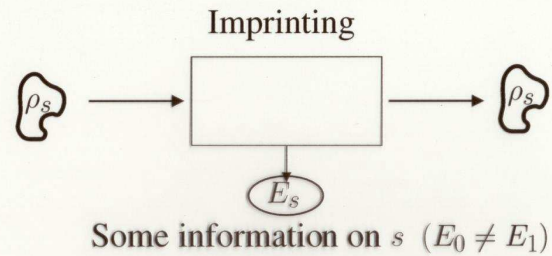
=Quantum measurement

**back action**





## Eavesdropping in Quantum key distribution



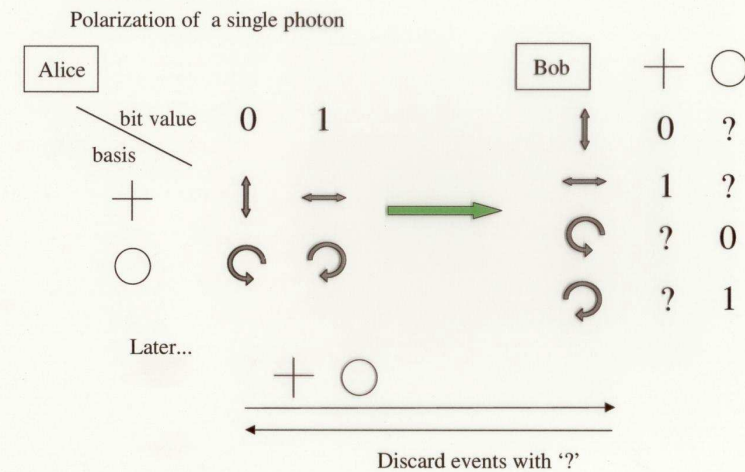
### No-imprinting principles

Conditions on  $\rho_0$  and  $\rho_1$  such that  
any attempt to read out  $s$  induces disturbance

## Quantum cryptography (Quantum Key Distribution)

### BB84 protocol

Bennett and Brassard (1984)



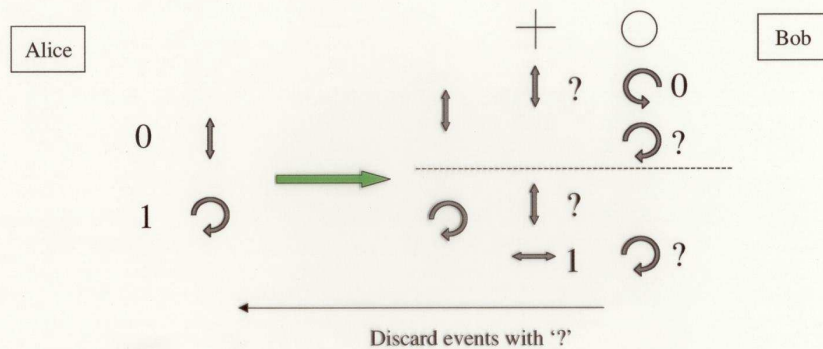
## Quantum cryptography (Quantum Key Distribution)

### B92 protocol

$|u_0\rangle, |u_1\rangle$

$\langle u_0 | u_1 \rangle \neq 0$

Bennett, PRL **68**,  
3121(1992)



'Nonorthogonal'

### Pure states

Bennett, Brassard, Mermin, PRL **68**,557(1992)

$$\rho_0 = |u_0\rangle\langle u_0|$$

$$\rho_1 = |u_1\rangle\langle u_1|$$

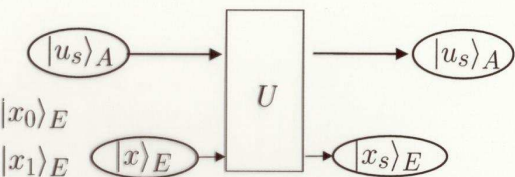
$$U(|u_0\rangle_A |x\rangle_E) = |u_0\rangle_A |x_0\rangle_E$$

$$U(|u_1\rangle_A |x\rangle_E) = |u_1\rangle_A |x_1\rangle_E$$

$$\langle u_0 | u_1 \rangle = \langle u_0 | u_1 \rangle \langle x_0 | x_1 \rangle$$

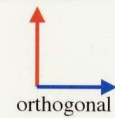
$$\langle u_0 | u_1 \rangle \neq 0 \longrightarrow |x_0\rangle = |x_1\rangle$$

no-imprinting condition = nonorthogonal



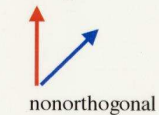
2 pure states

Extracting information



intact

classical



disturbed

nonclassical



no information

redundant

## Quantum cryptography (Quantum Key Distribution)

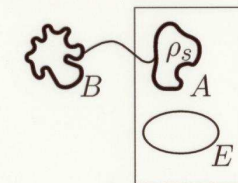
Quantum cryptography with **orthogonal states**

$$\begin{aligned} & \chi_s \quad \rho_s \\ & \begin{pmatrix} |1\rangle_A |0\rangle_B + |0\rangle_A |1\rangle_B \\ |1\rangle_A |0\rangle_B - |0\rangle_A |1\rangle_B \\ |0\rangle_A |0\rangle_B \end{pmatrix} / \sqrt{2} \end{aligned}$$

Goldenberg & Vaidman,  
PRL 75, 1239(1995)

$$(T \neq 0, 1/2, 1) \quad \begin{pmatrix} \sqrt{T} |1\rangle_A |0\rangle_B + \sqrt{1-T} |0\rangle_A |1\rangle_B \\ \sqrt{1-T} |1\rangle_A |0\rangle_B - \sqrt{T} |0\rangle_A |1\rangle_B \end{pmatrix}$$

Koashi & Imoto,  
PRL 79, 2383(1997)



Extracting contents of A  
and correlation to B

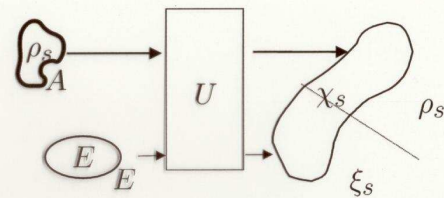
## Mixed states (imprinting)

$$\rho_s \otimes E \longrightarrow \chi_s$$

$$\text{Tr}_E(\chi_s) = \rho_s$$

$$\text{Tr}_A(\chi_s) = \xi_s$$

$$F(\xi_0, \xi_1) \neq 1$$

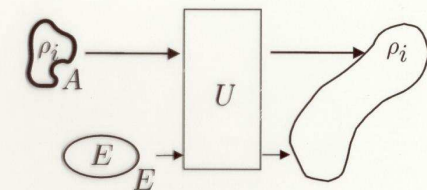


What kind of information can be extracted without disturbance?

What kind of choices of  $\rho_s$  ensures that any attempt to read out information causes disturbances?

## Approach

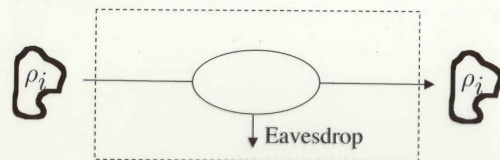
Given initial states  $\{\rho_i\}$ ,  
find the condition for the  
allowed operations.



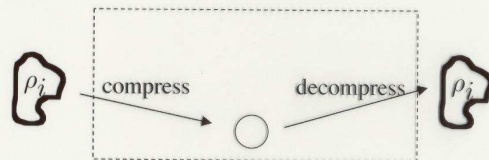
A principle that states what one can do, and what one cannot  
do, without disturbing the marginal density operators.

## The operations that do not disturb $\{\rho_i\}$

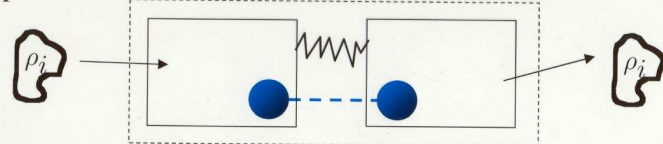
### Quantum cryptography



### Compression



### Teleportation



## Principle

$$\rho_i = \begin{pmatrix} q^{(i,1)} \times \rho^{(i,1)} & 0 \\ q^{(i,2)} \times \rho^{(i,2)} & 0 \\ 0 & q^{(i,3)} \times \alpha \rho^{(i,3)} \\ 0 & q^{(i,3)} \times \beta \rho^{(i,3)} \end{pmatrix}$$

$$\rho_J^{(i,3)} = \rho^{(i,3)}$$

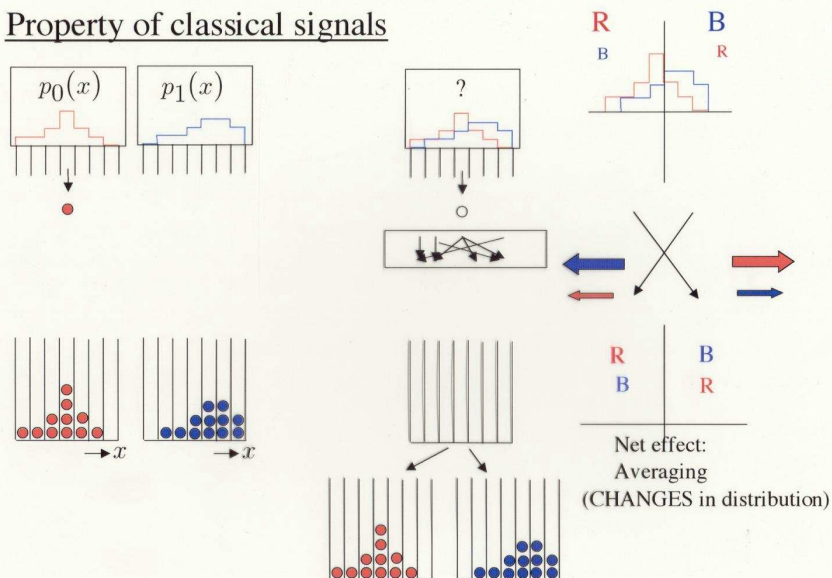
$$\rho_K^{(i,3)} = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$$

$$\mathcal{H} = \sum_l \mathcal{H}_J^{(l)} \otimes \mathcal{H}_K^{(l)}$$

$$\rho_i = \sum_l q^{(i,l)} \rho_J^{(i,l)} \otimes \rho_K^{(l)}$$

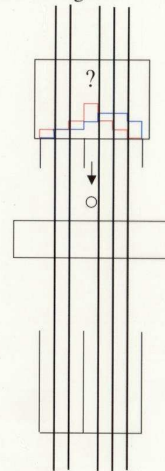
$$U = \sum_l 1_J^{(l)} \otimes U_{KE}^{(l)}$$

## Property of classical signals



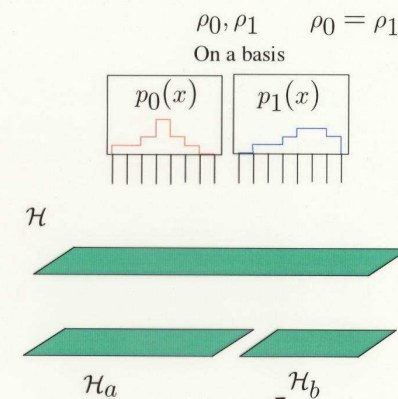
## Property of classical signals

For classical signals...



Unique decomposition

For quantum signals...

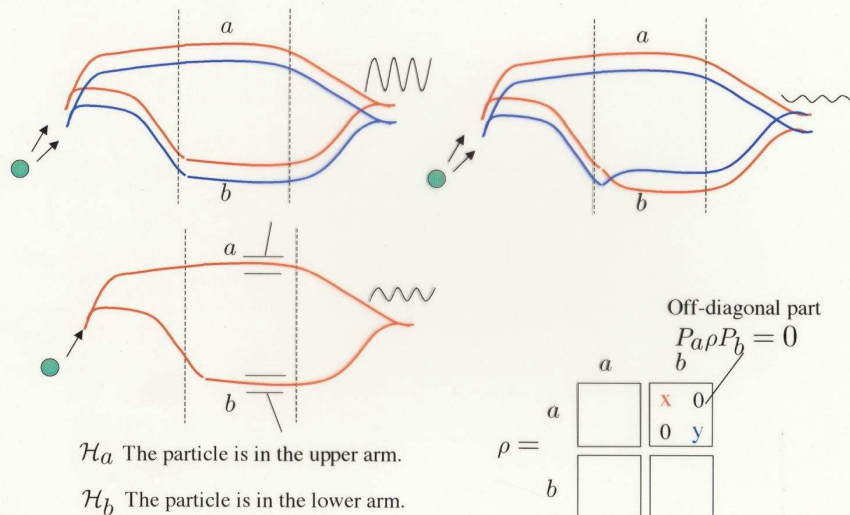


Operations must affect independently. This can be repeated, but not unique.

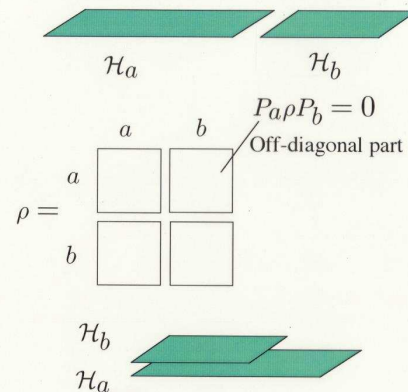


## Property of quantum signals

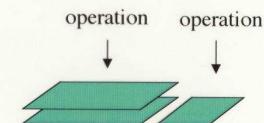
"Obtaining which-path information degrades the visibility of interference."



## Property of quantum signals



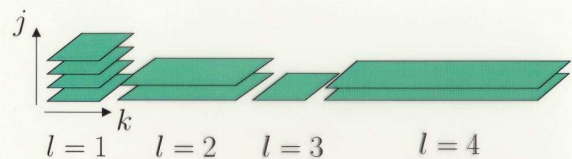
To preserve the off-diagonal part, the operation on the two space must be **identical**.



## Combining the two properties

Different states on a pile  $\longrightarrow$  SPLIT!

Nonzero off-diagonal part  $\longrightarrow$  PILE UP!



$$\mathcal{H} = \sum_l \mathcal{H}_J^{(l)} \otimes \mathcal{H}_K^{(l)}$$

$$\rho_i = \sum_l q^{(i,l)} \rho_J^{(i,l)} \otimes \rho_K^{(l)}$$

Allowed operation:  $U = \sum_l 1_J^{(l)} \otimes U_{KE}^{(l)}$

$U_{KE}^{(l)}$  acting on  $\mathcal{H}_K^{(l)} \otimes \mathcal{H}_E$

## Principle

$$\mathcal{H} = \sum_l \mathcal{H}_J^{(l)} \otimes \mathcal{H}_K^{(l)}$$

$$\rho_i = \sum_l q^{(i,l)} \rho_J^{(i,l)} \otimes \rho_K^{(l)}$$

$$U = \sum_l 1_J^{(l)} \otimes U_{KE}^{(l)}$$

Information of the state number  $i$

$\mathcal{H}_J^{(l)}$       quantum  
 $l$               classical  
 $\mathcal{H}_K^{(l)}$            none

What one can do without changing  $\rho_i$

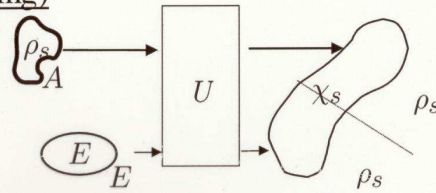
none  
classical  
quantum

### Mixed states (broadcasting)

$$\rho_s \otimes E \longrightarrow \chi_s$$

$$\text{Tr}_A(\chi_s) = \rho_s$$

$$\text{Tr}_E(\chi_s) = \rho_s$$



Broadcasting = Extracting *all* contents of  $\rho_s$

$$\rho_s = \sum_l q^{(s,l)} \rho_J^{(s,l)} \otimes \rho_K^{(l)}$$

We cannot see this part.

Broadcasting is possible  $\longrightarrow \dim \mathcal{H}_J^{(l)} = 1$

$$\rho_s = \sum_l q^{(s,l)} \rho_K^{(l)}$$

$\{\rho_s\}$  are simultaneously diagonalized.

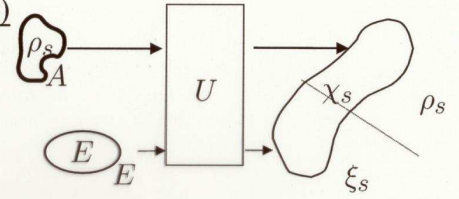
### Mixed states (imprinting)

$$\rho_s \otimes E \longrightarrow \chi_s$$

$$\text{Tr}_E(\chi_s) = \rho_s$$

$$\text{Tr}_A(\chi_s) = \xi_s$$

$$F(\xi_0, \xi_1) \neq 0$$



No imprinting = No information on  $s$  is available

$$\rho_s = \sum_l q^{(s,l)} \rho_J^{(s,l)} \otimes \rho_K^{(l)}$$

The index  $l$  is the only clue

no-imprinting condition

$$q^{(0,l)} = q^{(1,l)}$$

$\rho_0$  and  $\rho_1$  have the same trace for each block.

### Quantum cryptography (Quantum Key Distribution)

What Eve can do is

$\mathcal{H}_J^{(l)}$  none

$l$  classical

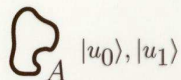
$\mathcal{H}_K^{(l)}$  quantum

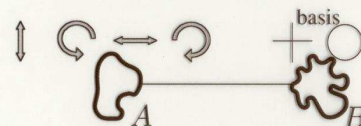
There are three ways to hide the bit info.


(1) on  $\mathcal{H}_J^{(l)}$

(2) on correlations through  $\mathcal{H}_J^{(l)}$

(3) on quantum correlations through  $l$

(1)   $\langle u_0 | u_1 \rangle \neq 0$  B92

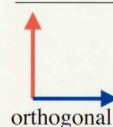
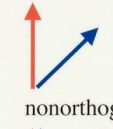

(2)  BB84

(3)  Goldenberg & Vaidman, PRL 75, 1239(1995)

$(T \neq 0, 1/2, 1)$   $\frac{\sqrt{T}|1\rangle_A|0\rangle_B + \sqrt{1-T}|0\rangle_A|1\rangle_B}{\sqrt{1-T}|1\rangle_A|0\rangle_B - \sqrt{T}|0\rangle_A|1\rangle_B}$  Koashi & Imoto, PRL 79, 2383(1997)

Structure of quantum information  $\mathcal{H} = \sum_l \mathcal{H}_J^{(l)} \otimes \mathcal{H}_K^{(l)}$

$$\rho_i = \sum_l q^{(i,l)} \rho_J^{(i,l)} \otimes \rho_K^{(l)}$$

2 pure states	Mixed states $\{p_i, \rho_i\}$	Extracting information	
	$l$	intact	classical
	$\mathcal{H}_J^{(l)}$	disturbed	nonclassical
	$\mathcal{H}_K^{(l)}$	no information	redundant