Private quantum subsystems and error correction

Sarah Plosker

Department of Mathematics and Computer Science
Brandon University

September 26, 2014
Outline

1. Classical Versus Quantum Setting
   - Classical Setting
   - Quantum Setting

2. Thought Experiments (1930’s)

3. QIT: States and Channels

4. Quantum Cryptography
   - Private Quantum Subsystem
   - Example

5. Connection with Quantum Error Correction
   - Complementarity of Q. Cryptography and QEC
   - From QEC to QCrypto?

6. Conclusion
The Setup

Alice (Sender) \[\Phi\] Bob (Receiver)

Input Message \[\text{noise}\] Output Message

Private quantum subsystems and error correction
States

**Definition**

A *bit* is a variable that can take as value either 0 or 1. Its realized value is called the *state* of the system (on/off, up/down, +/−, true/false, ...).
States

Definition

A *bit* is a variable that can take as value either 0 or 1. Its realized value is called the *state* of the system (on/off, up/down, +/−, true/false, . . .).

Classically: 00101010101010111110000111...2 (KABOOM!)
States

**Definition**

A *qubit* is a system that is the quantum analogue of a bit. Its state is a two-dimensional complex vector

\[ |\phi\rangle = \alpha |0\rangle + \beta |1\rangle, \]

where \( \alpha \) and \( \beta \) are *probability amplitudes*, meaning \( |\alpha|^2 + |\beta|^2 = 1 \), \( \alpha, \beta \in \mathbb{C} \), and \( |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \), using Dirac (bra-ket) notation.
A *qubit* is a system that is the quantum analogue of a bit. Its state is a two-dimensional complex vector

\[ |\phi\rangle = \alpha|0\rangle + \beta|1\rangle, \]

where \( \alpha \) and \( \beta \) are *probability amplitudes*, meaning \( |\alpha|^2 + |\beta|^2 = 1 \), \( \alpha, \beta \in \mathbb{C} \), and \( |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \), using Dirac (bra-ket) notation.

Thus a quantum system is in a state that, with probability \( |\alpha|^2 \), will be measured as \(|0\rangle\), and with probability \( |\beta|^2 \), will be measured as \(|1\rangle\); though it is truly a *superposition* of both of the states.
Copenhagen Interpretation

Interpretation of quantum mechanics by Bohr and Heisenberg, supported by von Neumann, Pauli. Opposed by Einstein, Schrödinger, Russell.

1. **The Uncertainty Principle** (also called the Indeterminacy Principle) of Heisenberg: The state of every particle is described by a wavefunction. The act of measurement causes the probabilities of the wavefunction to “collapse” to the value defined by the measurement.

2. **Principle of Complementarity** of Bohr: Wave-particle duality: light, electrons, ..., in short, all energy (and thus all matter) exhibits both wave-like and particle-like properties.
Schrödinger’s Cat

Thought experiment (1935): A cat is put in a sealed box, along with a small amount of radioactive substance and a flask of poison. If any radioactive decay is detected, the flash of poison is broken and the cat dies. If no radioactive decay is detected, then nothing happens. After a while, the cat is simultaneously dead and alive. Yet, when we look in the box, we see the cat either dead or alive, not both.

\[
|\text{cat}\rangle = \frac{1}{\sqrt{2}}|\text{dead}\rangle + \frac{1}{\sqrt{2}}|\text{alive}\rangle
\]
Schrödinger’s Cat (cont.)

IN UR QUANTUM BOX...

...MAYBE.
Schrodinger improves accuracy

wif increased sample size
EPR Paradox

Entangled states violate the classical principle of locality—the idea that an object is directly influenced only by its immediate surroundings.
EPR Paradox

Entangled states violate the classical principle of locality—the idea that an object is directly influenced only by its immediate surroundings.

The easiest way to see evidence of entanglement is to measure one component of an entangled state. This measurement fixes the value of the other component of the state, implying non-local communication between the two parts.
Entangled states violate the classical principle of locality—the idea that an object is directly influenced only by its immediate surroundings.

The easiest way to see evidence of entanglement is to measure one component of an entangled state. This measurement fixes the value of the other component of the state, implying non-local communication between the two parts.

Entanglement can be used as a resource in order to implement quantum teleportation.
Example of Entanglement

Electron spin, when measured, can be either of two states: spin up $\uparrow$ or spin down $\downarrow$.

In the absence of measurement, electron spin is in a superposition of the two states $\uparrow / \downarrow$ (even without entanglement).
Example of Entanglement

Electron spin, when measured, can be either of two states: spin up \( \uparrow \) or spin down \( \downarrow \).

In the absence of measurement, electron spin is in a superposition of the two states \( \uparrow / \downarrow \) (even without entanglement).

Consider an entangled electron pair; suppose the state of one of the electrons is measured as “spin up”. This measurement fixes the state of the other electron—it will be “spin down”.

S. Plosker

Private quantum subsystems and error correction
Example of Entanglement

Electron spin, when measured, can be either of two states: spin up ↑ or spin down ↓.

In the absence of measurement, electron spin is in a superposition of the two states ↑ / ↓ (even without entanglement).

Consider an entangled electron pair; suppose the state of one of the electrons is measured as “spin up”. This measurement fixes the state of the other electron—it will be “spin down”.

In this sense, even when spatially separated, entangled electron pairs behave as a single quantum object.
States

- pure state: $|\psi\rangle$ unit vector in $\mathbb{C}^n$
- rank one projection associated to a pure state:
  \[ \rho_{\psi} = |\psi\rangle \langle \psi| \in \mathcal{M}_n \]
- mixed state (density matrix):
  \[ \rho = \sum_i p_i |\psi\rangle \langle \psi| \geq 0, \quad Tr\rho = 1. \]
In quantum mechanics, one often looks at tensor product quantum systems, for which different users (Alice, Bob, Charlie, ...) have access to the individual tensored Hilbert spaces.
In quantum mechanics, one often looks at tensor product quantum systems, for which different users (Alice, Bob, Charlie, ... ) have access to the individual tensored Hilbert spaces.

A pure state $|\psi\rangle \in \mathbb{C}^m \otimes \mathbb{C}^n$ is called *separable* if it can be written as an elementary tensor: $|\psi\rangle = |\varphi\rangle \otimes |\phi\rangle$ where $|\varphi\rangle \in \mathbb{C}^m, |\phi\rangle \in \mathbb{C}^n$. Otherwise, $|\psi\rangle$ is said to be *entangled*. 
Separable vs Entangled Mixed States

In the case of mixed states, we say that \( \rho \in \mathcal{M}_m \otimes \mathcal{M}_n \) is separable if it can be written as a convex combination of separable pure states:

\[
\rho = \sum_i p_i \rho_{\varphi_i} \otimes \rho_{\phi_i},
\]

where \( \rho_{\varphi_i} = |\varphi_i\rangle\langle\varphi_i| \in \mathcal{M}_m \) and \( \rho_{\phi_i} = |\phi_i\rangle\langle\phi_i| \in \mathcal{M}_n \). Otherwise, \( \rho \) is said to be entangled.
We say that a linear map $\Phi : \mathcal{M}_m \rightarrow \mathcal{M}_n$ is completely positive (CP) if the induced mappings $\Phi_d : \mathcal{M}_d \otimes \mathcal{M}_m \rightarrow \mathcal{M}_d \otimes \mathcal{M}_n$, defined by $\Phi_d = \text{id}_d \otimes \Phi$, are positive for all $d$. 
Completely Positive Maps

**Definition**

We say that a linear map \( \Phi : \mathcal{M}_m \to \mathcal{M}_n \) is completely positive (CP) if the induced mappings \( \Phi_d : \mathcal{M}_d \otimes \mathcal{M}_m \to \mathcal{M}_d \otimes \mathcal{M}_n \), defined by \( \Phi_d = \text{id}_d \otimes \Phi \), are positive for all \( d \).

A map is called trace preserving if \( \text{Tr}(\Phi(X)) = \text{Tr}(X) \) for all \( X \).
Quantum Channels

Definition

A (quantum) channel $\Phi$ is a linear, CP, trace preserving (CPTP) map.
Quantum Channels

Definition

A \textit{(quantum) channel} $\Phi$ is a linear, CP, trace preserving (CPTP) map.

We can always write a quantum channel in the form

$\Phi(\rho) = \sum_i V_i \rho V_i^*$, where $\sum_i V_i^* V_i = I$. We call $V_i$ the

Choi/Kraus operators of $\Phi$. 
Random Unitary Channels

A quantum channel \( \Phi : \mathcal{M}_m \rightarrow \mathcal{M}_m \) is called a \textit{unitary channel} if we can write

\[
\Phi(\rho) = U\rho U^* \quad \text{for all } \rho \in \mathcal{M}_m.
\]

Such a channel has a single Kraus operator \( U \in \mathcal{M}_m \). Trace-preservation forces \( U \) to be unitary.
Random Unitary Channels

A quantum channel \( \Phi : \mathcal{M}_m \to \mathcal{M}_m \) is called a unitary channel if we can write

\[
\Phi(\rho) = U\rho U^* \quad \text{for all} \quad \rho \in \mathcal{M}_m.
\]

Such a channel has a single Kraus operator \( U \in \mathcal{M}_m \). Trace-preservation forces \( U \) to be unitary.

As a natural generalization of this example, a channel \( \Phi \) is called a random unitary channel if it admits a decomposition

\[
\Phi(\rho) = \sum_i p_i U_i \rho U_i^* \quad \text{for all} \quad \rho,
\]

where \( p_i \) form a probability distribution and \( U_i \) are unitary operators.
Definition

The map $\text{Tr}_k : \mathcal{M}_m \otimes \mathcal{M}_k \rightarrow \mathcal{M}_m$ defined by

$$\text{Tr}_k = \text{id}_m \otimes \text{Tr}$$

is called the partial trace (with respect to $\mathcal{M}_k$) and we say that we “trace out” the system $\mathcal{M}_k$.

We could similarly define the partial trace with respect to $\mathcal{M}_m$.

The partial trace is in fact a linear, trace preserving, completely positive map, and as such it is a quantum channel.
Stinespring’s theorem—Schrödinger picture

**Theorem**

Suppose that \( \Phi : \mathcal{M}_m \rightarrow \mathcal{M}_n \) is a completely positive trace preserving linear map. Then for some \( k \leq mn \), there exists a partial isometry \( U \in \mathcal{M}_{nk \times mk} \), and a pure state \( |\psi\rangle \in \mathbb{C}^k \) such that

\[
\Phi(\rho) = \text{Tr}_k(U(\rho \otimes \rho_\psi)U^*) \quad \text{for all} \quad \rho \in \mathcal{M}_m.
\] (1)
This is the Schrödinger picture for the (discrete) time evolution of quantum states.

If we define $V|\phi\rangle := U(|\phi\rangle \otimes |\psi\rangle)$ for all pure states $|\phi\rangle \in \mathbb{C}^m$, for some fixed pure state $|\psi\rangle \in \mathbb{C}^k$, then we can write equation (1) more succinctly as

$$\Phi(\rho) = \text{Tr}_k(V \rho V^*).$$

The general form for $U$ is

$$U = (V \mid \ast), \text{ where } V = \begin{pmatrix} V_1 \\ V_2 \\ \vdots \\ V_k \end{pmatrix}.$$
Purification of Mixed States

Fix a density operator $\rho_0 \in \mathcal{M}_m$, and consider the quantum channel $\Phi : \mathbb{C} \to \mathcal{M}_m$ defined by

$$\Phi(c \cdot 1) = c \rho_0 \quad \text{for all } c \in \mathbb{C}.$$
Purification of Mixed States

Fix a density operator $\rho_0 \in \mathcal{M}_m$, and consider the quantum channel $\Phi : \mathbb{C} \rightarrow \mathcal{M}_m$ defined by

$$\Phi(c \cdot 1) = c \rho_0 \quad \text{for all } c \in \mathbb{C}.$$ 

Then, with $\mathcal{M}_k = \mathbb{C} \otimes \mathcal{M}_m = \mathcal{M}_m$ and $U \in \mathcal{M}_{m^2 \times m}$, the Stinespring Theorem gives

$$\rho_0 = \Phi(1) = \text{Tr}_k(U(1 \otimes \rho_\psi)U^*) = \text{Tr}_k(\rho_\psi'),$$

where $|\psi'\rangle \in \mathcal{M}_{m^2} = \mathcal{M}_m \otimes \mathcal{M}_m$ is a purification of $\rho_0$, and the freedom in $U$ (and thus in $|\psi\rangle$) yields all possible purifications $\rho_\psi'$ for $\rho_0$. 
Purification of Mixed States

Fix a density operator $\rho_0 \in \mathcal{M}_m$, and consider the quantum channel $\Phi : \mathbb{C} \to \mathcal{M}_m$ defined by

$$\Phi(c \cdot 1) = c \rho_0 \quad \text{for all } c \in \mathbb{C}.$$  

Then, with $\mathcal{M}_k = \mathbb{C} \otimes \mathcal{M}_m = \mathcal{M}_m$ and $U \in \mathcal{M}_{m^2 \times m}$, the Stinespring Theorem gives

$$\rho_0 = \Phi(1) = \text{Tr}_k(U(1 \otimes \rho_\psi)U^*) = \text{Tr}_k(\rho_\psi'),$$

where $|\psi'\rangle \in \mathcal{M}_{m^2} = \mathcal{M}_m \otimes \mathcal{M}_m$ is a purification of $\rho_0$, and the freedom in $U$ (and thus in $|\psi\rangle$) yields all possible purifications $\rho_\psi'$ for $\rho_0$.

This idea of dilation constructions of channels and states is known as “going to the church of the larger Hilbert space”, a phrase credited to John Smolin.
Conjugate/Complementary Channels

Definition

Given a quantum channel \( \Phi : \mathcal{M}_m \to \mathcal{M}_n \), consider the Stinespring representation given by \( V \in \mathcal{M}_{nk \times m} \) and \( \mathcal{M}_k \) for which

\[
\Phi(\rho) = \text{Tr}_k(V\rho V^*).
\]

Then the corresponding **conjugate** (or **complementary**) channel is the quantum channel \( \Phi^\#: \mathcal{M}_m \to \mathcal{M}_k \) given by

\[
\Phi^\#(\rho) = \text{Tr}_n(V\rho V^*).
\]
Computing Kraus Operators for Conjugates

We can compute the Kraus operators of the complementary channel by “stacking” the $j$-th row of each of the Kraus operators $V_i$ of $\Phi$ one below the next, to obtain the $j$-th Kraus operator $R_j$ of $\Phi^\#$. 
Motivation

**Question:** How can we protect information stored in a quantum state from an external observer?
Motivation

**Question:** How can we protect information stored in a quantum state from an external observer?

Quantum cryptography is used to hide information when sending quantum information through a quantum channel so that the original message cannot be recovered by a third party.
Example

- Alice wishes to send a message $\psi$ from a particular set $S$ to Bob without an eavesdropper, Eve, being able to learn the message.
Example

- Alice wishes to send a message $\psi$ from a particular set $S$ to Bob without an eavesdropper, Eve, being able to learn the message.
- Alice can perform any unitary operation from a set $\{U_i\}$ with probability $p_i$ ($\{U_i\}$ and $\{p_i\}$ are known publicly)
Example

- Alice wishes to send a message $\psi$ from a particular set $S$ to Bob without an eavesdropper, Eve, being able to learn the message.
- Alice can perform any unitary operation from a set $\{U_i\}$ with probability $p_i$ ($\{U_i\}$ and $\{p_i\}$ are known publicly)
- Alice and Bob share a key, $i_0$ (privately), and Alice applies $U_{i_0}$ corresponding to $i_0$ to her message $\rho_\psi$; that is, $\rho_\psi \mapsto U_{i_0} \rho_\psi U_{i_0}^*$. 
Example

- Alice wishes to send a message $\psi$ from a particular set $S$ to Bob without an eavesdropper, Eve, being able to learn the message.
- Alice can perform any unitary operation from a set $\{U_i\}$ with probability $p_i$ ($\{U_i\}$ and $\{p_i\}$ are known publicly).
- Alice and Bob share a key, $i_0$ (privately), and Alice applies $U_{i_0}$ corresponding to $i_0$ to her message $\rho_{\psi}$; that is, $\rho_{\psi} \rightarrow U_{i_0}\rho_{\psi}U_{i_0}^*$. 
- Bob receives the output message, and, knowing $i_0$, can undo Alice's operation to recover the original message.
Example

• Alice wishes to send a message $\psi$ from a particular set $S$ to Bob without an eavesdropper, Eve, being able to learn the message.

• Alice can perform any unitary operation from a set $\{U_i\}$ with probability $p_i$ ($\{U_i\}$ and $\{p_i\}$ are known publicly)

• Alice and Bob share a key, $i_0$ (privately), and Alice applies $U_{i_0}$ corresponding to $i_0$ to her message $\rho_\psi$; that is, $\rho_\psi \mapsto U_{i_0}\rho_\psi U_{i_0}^*$. 

• Bob receives the output message, and, knowing $i_0$, can undo Alice’s operation to recover the original message.

• This is secure against Eve, who does not know $i_0$, and always sees the same output $\rho_0 = \sum_i p_i U_i(\rho) U_i^*$ regardless of Alice’s input message.
Example

- Alice wishes to send a message $\psi$ from a particular set $S$ to Bob without an eavesdropper, Eve, being able to learn the message.
- Alice can perform any unitary operation from a set $\{U_i\}$ with probability $p_i$ ($\{U_i\}$ and $\{p_i\}$ are known publicly).
- Alice and Bob share a key, $i_0$ (privately), and Alice applies $U_{i_0}$ corresponding to $i_0$ to her message $\rho_\psi$; that is, $\rho_\psi \mapsto U_{i_0} \rho_\psi U_{i_0}^*$.  
- Bob receives the output message, and, knowing $i_0$, can undo Alice's operation to recover the original message.
- This is secure against Eve, who does not know $i_0$, and always sees the same output $\rho_0 = \sum_i p_i U_i(\rho) U_i^*$ regardless of Alice's input message.
Private Quantum Channels—Definition

**Definition**

Let \( S \subseteq \mathbb{C}^m \) be a subspace of pure states, let \( \Phi : \mathcal{M}_m \otimes \mathcal{M}_k \rightarrow \mathcal{M}_n \) be a quantum channel, let \( \rho_a \in \mathcal{M}_k \) be an auxiliary density matrix, and let \( \rho_0 \in \mathcal{M}_n \). Then \([S, \Phi, \rho_a, \rho_0]\) is a private quantum channel if we have

\[
\Phi(\rho_\psi \otimes \rho_a) = \rho_0 \quad \text{for all } |\psi\rangle \in S.
\]

Motivating class of examples: random unitary channels, where

\[
\Phi(\rho) = \sum_i p_i U_i \rho U_i^*.
\]
Private Quantum Channels

Note: In previous works, the ancilla state $\rho_a$ is used theoretically, but does not appear in physical examples (Ambainis et al, Boykin-Roychowdhury, 2000)

$\rho_0$ is often taken to be the maximally mixed state $\frac{1}{d}I$
(Boykin-Roychowdhury).
The simplest example of a private quantum channel is the completely depolarizing channel $\mathcal{E}$ acting on $\mathcal{M}_2$. Define the Pauli matrices as

\[
X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}
\]
The simplest example of a private quantum channel is the completely depolarizing channel $\mathcal{E}$ acting on $\mathcal{M}_2$. Define the Pauli matrices as

\[
X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}
\]

Then $\mathcal{E}(\rho) = \frac{1}{4}(I \rho I + X \rho X + Y \rho Y + Z \rho Z) = \frac{1}{2} I$.

The completely depolarizing channel sends all density matrices to the maximally mixed state.
We call $A$ and $B$ subsystems of $\mathbb{C}^n$ if we can write
$$\mathbb{C}^n = (A \otimes B) \oplus (A \otimes B)^\perp.$$ The subspaces of $\mathbb{C}^n$ can be viewed as subsystems $B$ for which $A$ is one-dimensional. A subscript on a state will indicate to which subsystem the state belongs, e.g. $\sigma_A$ means the operator belongs to $\mathcal{M}_{n_A}$. 
Private Subsystem

We call $A$ and $B$ subsystems of $\mathbb{C}^n$ if we can write
$\mathbb{C}^n = (A \otimes B) \oplus (A \otimes B)^\perp$.
The subspaces of $\mathbb{C}^n$ can be viewed as subsystems $B$ for which $A$ is one-dimensional. A subscript on a state will indicate to which subsystem the state belongs, e.g. $\sigma_A$ means the operator belongs to $\mathcal{M}_{nA}$.

Subsystem encodings first arose in quantum information in 2004 through the work of Bartlett-Rudolph-Spekkens (quantum cryptography) and Kribs-Laflamme-Poulin (“operator” quantum error correction).
Definition

Let $\Phi : M_n \rightarrow M_n$ be a channel and let $B$ be a subsystem of $\mathbb{C}^n$. Then $B$ is a *completely private subsystem* for $\Phi$ if there is a $\rho_0 \in M_n$ and $\sigma_A \in M_{n_A}$ such that

$$\Phi(\sigma_A \otimes \sigma_B) = \rho_0 \quad \text{for all} \quad \sigma_B.$$ 

Definition

Let $\Phi : M_n \rightarrow M_n$ be a channel and let $B$ be a subsystem of $\mathbb{C}^n$. Then $B$ is a *operator private subsystem* for $\Phi$ if there is a $\rho_0 \in M_n$ such that

$$\Phi(\sigma_A \otimes \sigma_B) = \rho_0 \quad \text{for all} \quad \sigma_A, \quad \text{for all} \quad \sigma_B.$$
Consider the following phase damping channels acting on $\mathcal{M}_4$:

$$\Lambda_i(\rho) = \frac{1}{2}(\rho + Z_i \rho Z_i), \quad \text{for all } \rho \in \mathcal{M}_4,$$

where $Z_1 = Z \otimes I_2$ and $Z_2 = I_2 \otimes Z$.
Phase Damping Channel

Consider the following phase damping channels acting on $\mathcal{M}_4$:

$$\Lambda_i(\rho) = \frac{1}{2}(\rho + Z_i \rho Z_i), \quad \text{for all } \rho \in \mathcal{M}_4,$$

where $Z_1 = Z \otimes I_2$ and $Z_2 = I_2 \otimes Z$.

For $i = 1, 2$, $\Lambda_i$ is not private: the diagonal entries of the input $\rho$ are preserved—Eve would be able to learn some information about the original message based on what diagonal terms she observes.
Let $\Lambda$ be the composition of the application of the maps $\Lambda_1$ and $\Lambda_2$:

$$\Lambda(\rho) = \Lambda_2 \circ \Lambda_1.$$
Privacy for phase damping channel?

Let $\Lambda$ be the composition of the application of the maps $\Lambda_1$ and $\Lambda_2$:

$$\Lambda(\rho) = \Lambda_2 \circ \Lambda_1.$$  

The Kraus operators for $\Lambda$ are $\{\frac{1}{2} I I, \frac{1}{2} I Z, \frac{1}{2} Z I, \frac{1}{2} ZZ\}$. 
Privacy for phase damping channel?

Let \( \Lambda \) be the composition of the application of the maps \( \Lambda_1 \) and \( \Lambda_2 \):

\[
\Lambda(\rho) = \Lambda_2 \circ \Lambda_1.
\]

The Kraus operators for \( \Lambda \) are \( \{ \frac{1}{2} I I, \frac{1}{2} I Z, \frac{1}{2} Z I, \frac{1}{2} ZZ \} \).

Similar to before, we find \( \Lambda \) preserves the diagonal of the input \( \rho \) (in this case the output is a diagonal matrix); no private subspace exists.
However, consider a density matrix

$$\rho_L = \frac{1}{4}(I I + \alpha XX + \beta Y I + \gamma ZX).$$

We note that $\Lambda(\rho_L) = \frac{1}{4}I_2 I_2$, for any $\rho_L$ of this form. Thus $\Lambda$ is private for some set of states, which we can show forms a subsystem.
Common Physical Gates

The $T$-gate,

$$K = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix},$$

$$CNOT_{1,2} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

$$CNOT_{2,1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$
Let $U = CNOT_{1,2} CNOT_{2,1} \circ (K^* \otimes I_2)$. The composition $U(\cdot)U^*$ acts as

$$XX \mapsto IY$$
$$YZ \mapsto IZ$$
$$ZX \mapsto IX.$$  

Thus, we obtain $\rho_L \mapsto \rho' = \frac{1}{4}(I_2 I_2 + \gamma I X + \alpha I Y + \beta I Z)$. We see the set of operators $U\rho_L U^*$ generate the algebra $I_2 \otimes M_2$.

In other words, the set $M_4(S)$ spanned by all $\rho_L$ is isomorphic to $I_2 \otimes M_2$. 

S. Plosker  Private quantum subsystems and error correction
Quantum Error Correction

How can we protect our quantum information against sources of quantum noise?
Quantum Error Correction

How can we protect our quantum information against sources of quantum noise?

Quantum error correction is used to recover information from errors introduced by noise that occurs when sending quantum information through a quantum channel.
Quantum Error Correction

How can we protect our quantum information against sources of quantum noise?

Quantum error correction is used to recover information from errors introduced by noise that occurs when sending quantum information through a quantum channel.

Definition

Let $\Phi : \mathcal{M}_n \to \mathcal{M}_n$ be a channel and let $B$ be a subsystem of $\mathcal{M}_n$. Then $B$ is a correctable subsystem for $\Phi$ if there exists a quantum channel $R$, called a recovery operation, such that for all $\sigma_A$, for all $\sigma_B$, there exists a $\tau_A$ we have

$$R \circ \Phi(\sigma_A \otimes \sigma_B) = \tau_A \otimes \sigma_B.$$
Quantum Error Correction

How can we protect our quantum information against sources of quantum noise?

Quantum error correction is used to recover information from errors introduced by noise that occurs when sending quantum information through a quantum channel.

**Definition**

Let $\Phi : \mathcal{M}_n \to \mathcal{M}_n$ be a channel and let $B$ be a subsystem of $\mathcal{M}_n$. Then $B$ is a correctable subsystem for $\Phi$ if there exists a quantum channel $\mathcal{R}$, called a recovery operation, such that for all $\sigma_A$, for all $\sigma_B$, there exists a $\tau_A$ we have

$$\mathcal{R} \circ \Phi(\sigma_A \otimes \sigma_B) = \tau_A \otimes \sigma_B.$$

Note: For “correctable subspace $S$”, we have $\mathcal{R} \circ \Phi(\rho) = \rho$ for all $\rho \in \mathcal{M}(S)$. 

S. Plosker

Private quantum subsystems and error correction
Complementarity of Private Subspaces

Both quantum error correction and quantum cryptography protect against the unwanted leakage, or loss, of quantum information and there is an established connection between such notions:

Theorem (Kretschmann-Kribs-Spekkens)

*Given a conjugate pair of quantum channels* $\Phi, \Phi^\#$, *a subsystem* $S$ *is error-correctable for one if and only if it is an operator private subsystem for the other.*

The extreme example of this phenomena is given by a unitary channel paired with the completely depolarizing channel – where the entire Hilbert space is the correctable (private) subspace.
For our phase damping channel $\Lambda$, we can easily compute the Kraus operators of $\Lambda^\#$: We find

$$\Lambda^\#(U(\frac{1}{2} I_A \otimes \sigma_B)U^*) = \frac{1}{4} I_2 I_2.$$  

Instead of being correctable on the private subsystem $I_2 \otimes \mathcal{M}_2$, the complementary channel $\Lambda^\#$ (with the proper unitary transformation) is completely depolarizing! All information is lost, so there is no possibility of the channel being quantum error correctable.
Let $\Phi : \mathcal{M}_m \rightarrow \mathcal{M}_n$. Let $(\mathcal{V}_\Phi, \mathcal{M}_k)$ be the Stinespring representation for $\Phi$. 

\[
\mathcal{M}_n \xrightarrow{\Phi} \Phi(\rho) = \rho_0
\] 

\[
\rho \xrightarrow{\mathcal{M}_m} \mathcal{V}_\Phi \xrightarrow{\text{Tr}_k} \rho_0
\] 

\[
\mathcal{M}_k \xrightarrow{\mathcal{U}_\mathcal{R}} \mathcal{R} \circ \Phi^\#(\rho) = \rho
\]
The big picture

- The dotted box (···) represents the mixed state encoding.
- The dashed box (– –) encodes the state $\rho'$ into the mixed state encoding $\rho$.
- The solid box (—) performed the private quantum channel.
From QEC to QCrypto?

**General Program:** Using the “algebraic bridge” given by the notion of conjugate channels, we wish to investigate what results, techniques, special types of codes, applications, etc., from the well-studied field of quantum error correction have analogues or versions in the world of private quantum codes and quantum cryptography. At the least, we can use work from QEC as motivation for studies in this different setting.
Knill-Laflamme Theorem for QEC

**Theorem**

Let $S$ be a subspace of $\mathbb{C}^n$ and let $P$ be the projector onto $\mathcal{M}_n(S)$. Suppose $\Phi$ is a quantum channel with Kraus operators $\{E_i\}$. Then there exists an error-correction operation $R$ correcting $\Phi$ on $S$ if and only if $PE_i^*E_jP = \alpha_{ij}P$ for some Hermitian matrix $\alpha = [\alpha_{ij}]_{ij}$ of complex numbers.
“Knill-Laflamme” Type Conditions for Private Subspaces

Using the bridge between privacy and quantum error correction, we can formulate “Knill-Laflamme” type conditions for the private setting.

Theorem (Kribs–P.)

Let $S$ be a subspace of $\mathbb{C}^n$ and let $P$ be the projector onto $\mathcal{M}_n(S)$. Then $S$ is private for a quantum channel $\Phi$ with output state $\rho_0$; i.e., $\Phi(\rho) = \rho_0$ for all $\rho \in \mathcal{M}(S)$ if and only if

$$\text{for all } X \exists \lambda_X \in \mathbb{C} : P\Phi^*(X)P = \lambda_X P.$$ 

In this case, $\lambda_X = \text{Tr}(\rho_0 X)$, where $\Phi^*(X) = \sum_i V_i^* XV_i$. 
"Knill-Laflamme" Type Conditions for Private Subsystems

**Theorem (Jochym-O’Connor–Kribs–Laflamme–P.)**

A subsystem $B$ is private for a channel $\Phi(\rho) = \sum_i V_i \rho V_i^*$ with fixed $\sigma_A \in \mathcal{M}(\mathcal{H}_A)$ and output state $\rho_0$ if and only if there are complex scalars $\lambda_{ijk\ell}$ forming an isometry matrix $\lambda = (\lambda_{ijk\ell})$ such that $\sqrt{p_k} V_j |\psi_{A,k}\rangle = \sum_{i,\ell} \lambda_{ijk\ell} \sqrt{q_\ell} |\phi_\ell\rangle |\psi_{B,i}\rangle$, where $|\psi_{A,k}\rangle (p_k)$ and $|\phi_\ell\rangle (q_\ell)$ are eigenstates (eigenvalues) of $\sigma_A$ and $\rho_0$ respectively, $|\psi_{B,i}\rangle$ is an orthonormal basis for $B$, and where $|\psi_{A,k}\rangle$ is viewed as a channel from $B$ into $S$. 
Theorem (Jochym-O’Connor–Kribs–Laflamme–P.)

Let $\Phi$ be a quantum channel whose Kraus operators are a set of commuting unitary operators $\{\sqrt{p_i} U_i\}$, where $\sqrt{p_i}$ is a scaling factor such that $\sum_i p_i = 1$. Then there exists no private subspace $S$ for $\Phi$. 
Conclusion

- We’ve seen several variations of private quantum channel/code/subspace/operator subsystem/completely (private) subsystem...
- Knill-Laflamme analogue for private setting via complementary channels.
- The theorem linking QEC with quantum cryptography doesn’t work for completely private subsystems.
- Relaxed definition of conjugate channel?
Over the last 10 years, there’s been lots of progress in QEC motivated by operator algebraic approach.

At this point, much less mathematical development on PQC side; still at an early stage.

Still lots to uncover—in particular, an overarching mathematical formalism of private subsystems, similar to the “Stabilizer formalism” in QEC.