Private quantum subsystems and error correction

Tomas Jochym-O'Connor

Institute for Quantum Computing and Department of Physics and Astronomy
University of Waterloo

15 December 2014
QEC 2014 – Zurich

Work in collaboration with David Kribs, Raymond Laflamme, and Sarah Plosker

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

Last time at QEC...

On Complementarity In QEC And Quantum Cryptography

David Kribs

Professor & Chair
Department of Mathematics & Statistics
University of Guelph

Associate Member
Institute for Quantum Computing
University of Waterloo

QEC II — USC — December 2011

Outline

- Review definitions of operator quantum privacy and error correction
- Complementary between privacy and error correction
- Restrictions of operator quantum privacy
- Generalized notion of subsystem privacy
- Recovering the duality with quantum error correction

Notation

- Subsystems: $S = (A \otimes B) \oplus (A \otimes B)^{\perp}$
- Density matrices: Bounded linear operators with trace 1, $\sigma_A \in A,\ \sigma_B \in B,\ \rho \in A \otimes B$
- Quantum channel: Completely positive trace preserving map between linear operators, $\Phi : \mathcal{B}(A) \to \mathcal{B}(C)$
- Complementary channel: Given a quantum channel Φ, there always exists a unitary U_Φ and ancillary state $|\phi\rangle\langle\phi|_K$ such that $\Phi(\rho_A) = \mathrm{Tr}_K\left(U_\Phi(\rho_A \otimes |\phi\rangle\langle\phi|_K)U_\Phi^\dagger\right),\ \forall\ \rho_i$. The **complementary channel** is then defined as:

$$\Phi^\sharp(\rho) = \mathrm{Tr}_C\left(U_\Phi(\rho \otimes |\phi\rangle\langle\phi|_K)U_\Phi^\dagger\right).$$

Operator QEC and privacy

$$S = (A \otimes B) \oplus (A \otimes B)^{\perp}$$

- A subsystem B is an **operator private subsystem** for Φ if there exists ρ_0 such that

$$\Phi(\sigma_A \otimes \sigma_B) = \rho_0, \ \forall \sigma_A, \ \sigma_B$$

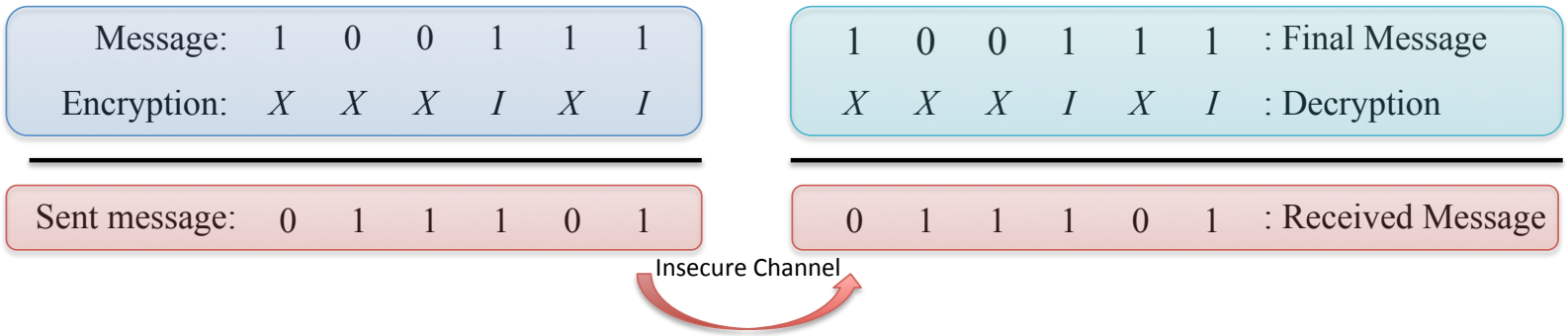
- A subsystem B is **operator quantum error correctable** for $\mathcal{E}$ if there exist $\tau_A(\sigma_A)$, $\mathcal{R}$ such that

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

Random Unitary channels

What type of channels are required to privatize quantum information?

In classical communication, messages can be encrypted using a one-time pad.

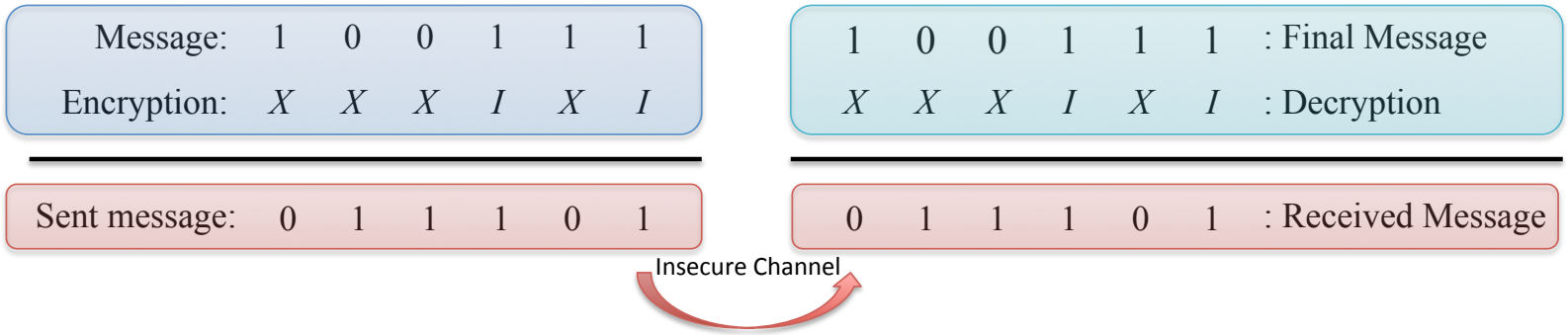


The key property of the one-time pad is the uniform *randomization* of each of the bits of the message.

Random Unitary channels

What type of channels are required to privatize quantum information?

In classical communication, messages can be encrypted using a one-time pad.



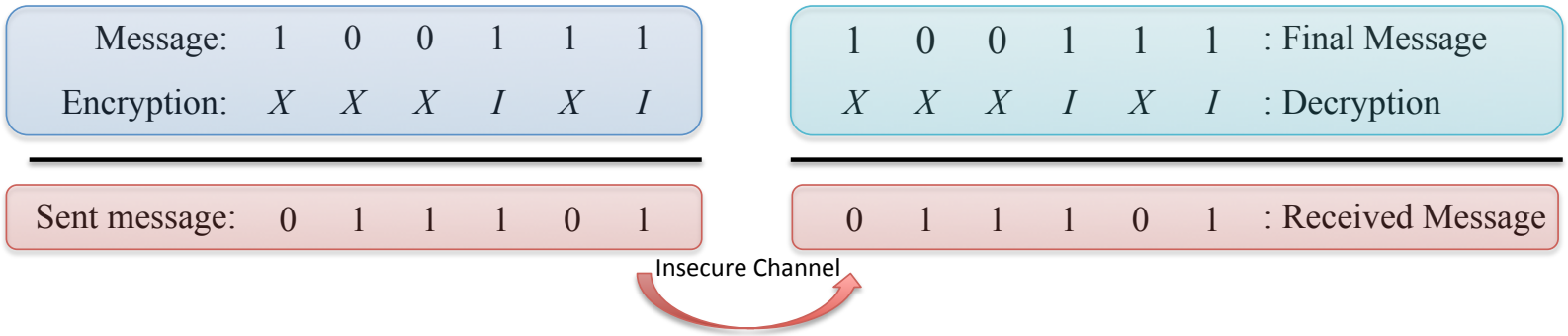
The key property of the one-time pad is the uniform *randomization* of each of the bits of the message.
The state of any given bit of encrypted data x_b is given by a classical probability distribution:

$$\Phi(x_b) = \frac{1}{2}x_b + \frac{1}{2}\overline{x_b}$$

Random Unitary channels

What type of channels are required to privatize quantum information?

In classical communication, messages can be encrypted using a one-time pad.



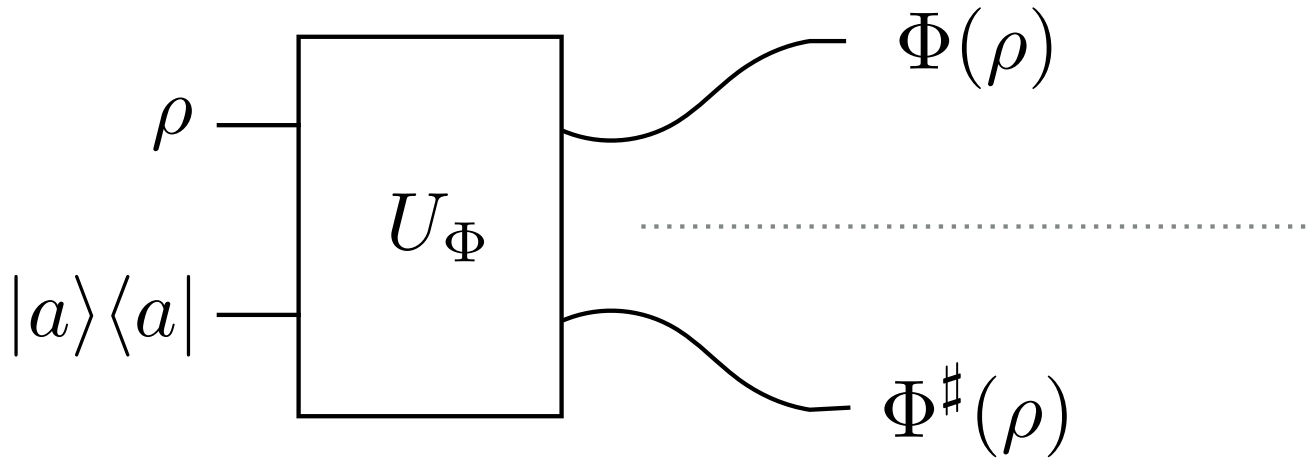
Random unitary channels provide the quantum analogue to the classical one-time pad,

$$\Phi(\rho) = \sum_i p_i U_i \rho U_i^\dagger$$

Operator duality

Theorem (KKS08[1])

A subsystem B is an operator private subsystem for a channel Φ if and only if it is operator QEC for the complementary channel $\Phi^\sharp$.



[1] D. Kretschmann, D. W. Kribs, R. Spekkens, (2008)

Quest for small private channels

Inspiration from quantum error correction!

The dephasing channel is not private on a single qubit:

$$\Lambda_i(\rho) = \frac{1}{2}(\rho + Z_i \rho Z_i) \qquad \forall \rho \in S.$$

How about the same identical channel on multiple qubits?

$$\Lambda(\rho) \quad = \Phi_2 \circ \Phi_1(\rho)$$

Quest for small private channels

Inspiration from quantum error correction!

The dephasing channel is not private on a single qubit:

$$\Lambda_i(\rho) = \frac{1}{2}(\rho + Z_i \rho Z_i) \qquad \forall \rho \in S.$$

How about the same identical channel on multiple qubits?

$$\Lambda(\rho) \quad = \Phi_2 \circ \Phi_1(\rho)$$

The resulting mapping yields:

$$\begin{pmatrix} \alpha_{00} & \alpha_{01} & \alpha_{02} & \alpha_{03} \\ \alpha_{10} & \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{20} & \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{30} & \alpha_{31} & \alpha_{32} & \alpha_{33} \end{pmatrix} \xrightarrow{\Lambda} \begin{pmatrix} \alpha_{00} & 0 & 0 & 0 \\ 0 & \alpha_{11} & 0 & 0 \\ 0 & 0 & \alpha_{22} & 0 \\ 0 & 0 & 0 & \alpha_{33} \end{pmatrix}$$

No-go result for private subspaces

Theorem (JKLP13[2])

Let $\Phi(\rho) = \sum_i p_i U_i \rho U_i^\dagger$ be a random unitary channel with mutually commuting Kraus operators. Then Φ has no private subspace.

[2] TJ, D. W. Kribs, R. Laflamme, S. Plosker (2013)

No-go result for private subspaces

Theorem (JKLP13[2])

Let $\Phi(\rho) = \sum_i p_i U_i \rho U_i^\dagger$ be a random unitary channel with mutually commuting Kraus operators. Then Φ has no private subspace.

- A subsystem B is an **operator private subsystem** for Φ if there exists ρ_0 such that

$$\Phi(\sigma_A \otimes \sigma_B) = \rho_0, \ \forall \sigma_A, \ \sigma_B$$

[2] TJ, D. W. Kribs, R. Laflamme, S. Plosker (2013)

No-go result for private subspaces

Theorem (JKLP13[2])

Let $\Phi(\rho) = \sum_i p_i U_i \rho U_i^\dagger$ be a random unitary channel with mutually commuting Kraus operators. Then Φ has no private subspace.

- A subsystem B is an **operator private subsystem** for Φ if there exists ρ_0 such that

$$\Phi(\sigma_A \otimes |\psi\rangle\langle\psi|) = \rho_0, \ \forall \sigma_A, \ |\psi\rangle\langle\psi|$$

Therefore, the channel $\Lambda = \Lambda_2 \circ \Lambda_1$ **cannot** be operator quantum private

[2] TJ, D. W. Kribs, R. Laflamme, S. Plosker (2013)

However...

- Consider the following encoding of a quantum state:

$$\rho_L = \frac{1}{2}(I + \alpha XX + \beta YI + \gamma ZX).$$

  ρ_L is privatized by the channel $\Lambda = \Lambda_2 \circ \Lambda_1$. A contradiction?
- It can be shown that the state space defined by the parameters $\alpha,\ \beta,\ \gamma$ is unitarily equivalent to $I_2 \otimes \mathcal{D}_2$, where $\mathcal{D}_2$ is the space of 2-dimensional density matrices.

Where is the loophole?

Λ privatizes the state space $I_2 \otimes \mathcal{D}_2$, why is this not equivalent to operator privacy?
A subsystem B is an **operator private subsystem** for Φ if there exists ρ_0 such that

$$\Phi(\sigma_A \otimes \sigma_B) = \rho_0, \ \forall \sigma_A, \ \sigma_B$$

Where is the loophole?

Λ privatizes the state space $I_2 \otimes \mathcal{D}_2$, why is this not equivalent to operator privacy?
A subsystem B is an **operator private subsystem** for Φ if there exists ρ_0 such that

$$\Phi(\sigma_A \otimes \sigma_B) = \rho_0, \ \forall \sigma_A, \ \sigma_B$$

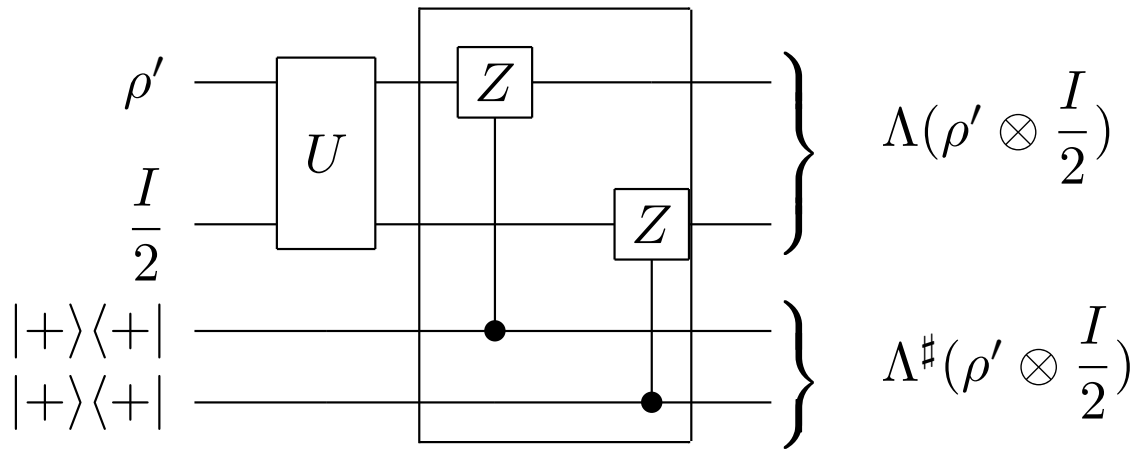
Therefore, fixing the state $\sigma_A = I_2$, is what allows the channel to be private, suggesting a new notion of privacy, **private quantum channels**.

The role of a fixed ancilla

- A subsystem B is a **private quantum subsystem**[3] for Φ if there is a $\rho_0 \in S$ and $\sigma_A \in A$ such that

$$\Phi(\sigma_A \otimes \sigma_B) = \rho_0, \ \forall \sigma_B \in B$$

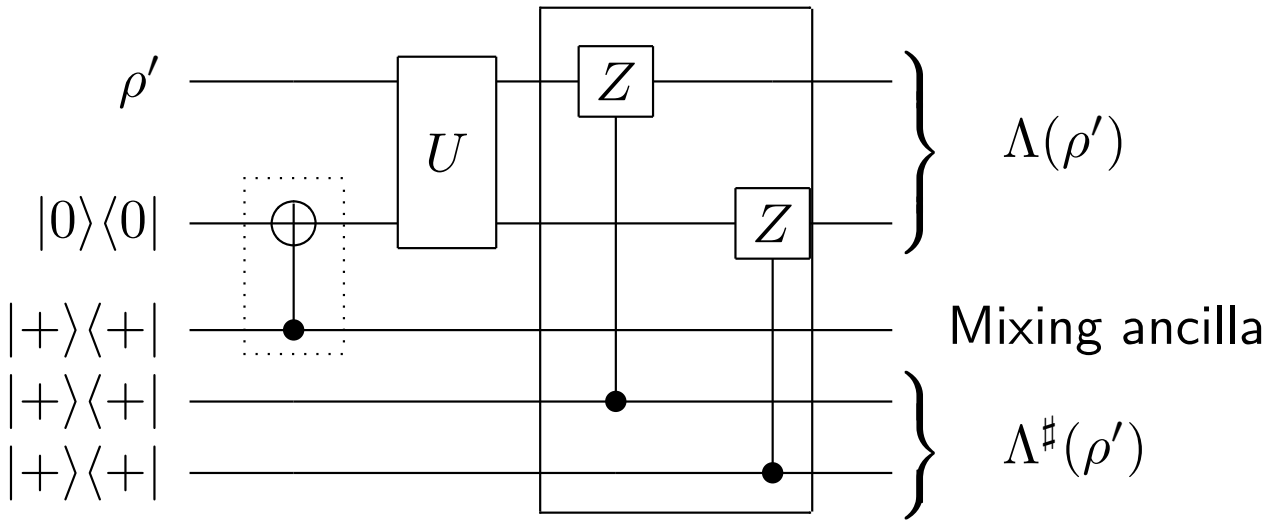
- The conjugate channel to the multi-qubit phase damping channel $\Lambda = \Lambda_2 \circ \Lambda_1$ cannot be operator quantum error correctable. In fact, it is private for the same encoding space.



[3] S. D. Bartlett, T. Rudolph, R. W. Spekkens (2004)

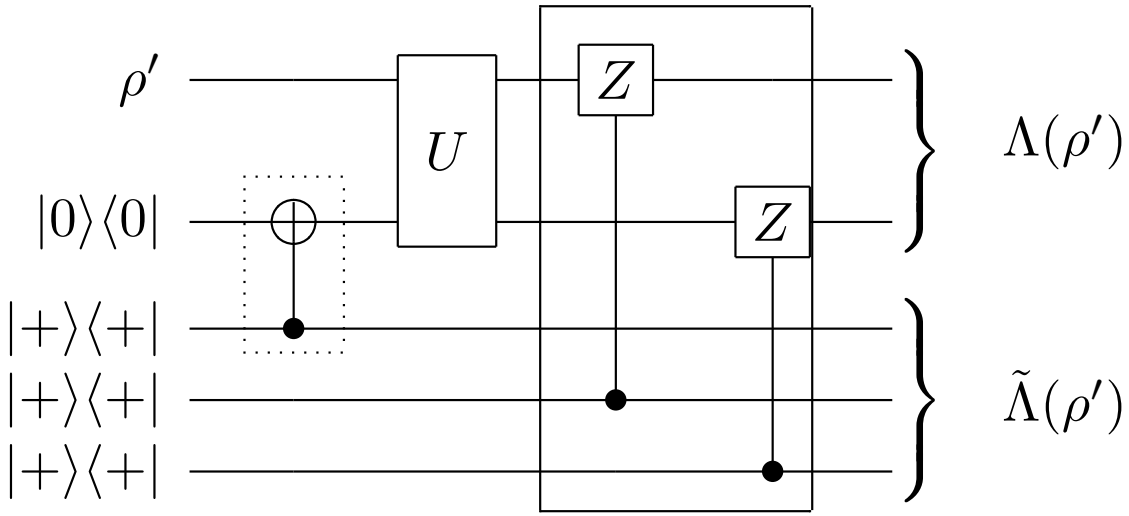
What happens to the duality with error correction?

The mixed state ancilla is the resource allowing for privacy of the channel.



What happens to the duality with error correction?

The mixed state ancilla is the resource allowing for privacy of the channel.



The generalized complementary channel $\tilde{\Lambda}$ must be quantum error correctable by the operator duality that exists on the extended Hilbert space.

Additional degrees of freedom

Operator

$$\alpha \left|0_L\right\rangle_{12} \rightarrow \sum_{ij} \left|ij\right\rangle_{12} \left|E^0_{ij}\right\rangle_K$$

$$\beta \left|1_L\right\rangle_{12} \rightarrow \sum_{ij} \left|ij\right\rangle_{12} \left|E^1_{ij}\right\rangle_K$$

Generalized

$$\alpha \left|0_L\right\rangle_{123} \rightarrow \sum_{ijk} \left|ijk\right\rangle_{123} \left|E^0_{ijk}\right\rangle_K$$

$$\beta \left|1_L\right\rangle_{123} \rightarrow \sum_{ijk} \left|ijk\right\rangle_{123} \left|E^1_{ijk}\right\rangle_K$$

Additional degrees of freedom

Operator

$$\alpha |0_L\rangle_{12} \to \sum_{ij} |ij\rangle_{12} |E^0_{ij}\rangle_K$$

$$\beta |1_L\rangle_{12} \to \sum_{ij} |ij\rangle_{12} |E^1_{ij}\rangle_K$$

Generalized

$$\alpha |0_L\rangle_{123} \to \sum_{ijk} |ijk\rangle_{123} |E^0_{ijk}\rangle_K$$

$$\beta |1_L\rangle_{123} \to \sum_{ijk} |ijk\rangle_{123} |E^1_{ijk}\rangle_K$$

$$\begin{aligned} |ij\rangle\langle kl|_{12} \mathsf{Tr}_E \Big(& |\alpha|^2 |E^0_{ij}\rangle\langle E^0_{kl}| \\ & + \alpha\beta^* |E^0_{ij}\rangle\langle E^1_{kl}| \\ & + \alpha^*\beta |E^1_{ij}\rangle\langle E^0_{kl}| \\ & + |\beta|^2 |E^1_{ij}\rangle\langle E^1_{kl}| \Big) \end{aligned}$$

$$\begin{aligned} \implies \langle E^0_{ij}|E^0_{kl}\rangle &= \langle E^1_{ij}|E^1_{kl}\rangle, \\ \langle E^0_{ij}|E^1_{kl}\rangle &= 0 \end{aligned}$$

Additional degrees of freedom

Operator

$$\alpha |0_L\rangle_{12} \to \sum_{ij} |ij\rangle_{12} |E^0_{ij}\rangle_K$$
$$\beta |1_L\rangle_{12} \to \sum_{ij} |ij\rangle_{12} |E^1_{ij}\rangle_K$$

Generalized

$$\alpha |0_L\rangle_{123} \to \sum_{ijk} |ijk\rangle_{123} |E^0_{ijk}\rangle_K$$
$$\beta |1_L\rangle_{123} \to \sum_{ijk} |ijk\rangle_{123} |E^1_{ijk}\rangle_K$$

$$\begin{aligned}|ij\rangle\langle kl|_{12}\mathsf{Tr}_E\Big(&|\alpha|^2(|E^0_{ij0}\rangle\langle E^0_{kl0}| + |E^0_{ij1}\rangle\langle E^0_{kl1}|)\\ &+ \alpha\beta^*(|E^0_{ij0}\rangle\langle E^1_{kl0}| + |E^0_{ij1}\rangle\langle E^1_{kl1}|)\\ &+ \alpha^*\beta(|E^1_{ij0}\rangle\langle E^0_{kl0}| + |E^1_{ij1}\rangle\langle E^0_{kl1}|)\\ &+ |\beta|^2(|E^1_{ij0}\rangle\langle E^1_{kl0}| + |E^1_{ij1}\rangle\langle E^1_{kl1}|)\Big)\end{aligned}$$

$$\langle E^0_{ij0}|E^0_{kl0}\rangle + \langle E^0_{ij1}|E^0_{kl1}\rangle = \langle E^1_{ij0}|E^1_{kl0}\rangle + \langle E^1_{ij1}|E^1_{kl1}\rangle$$
$$\langle E^0_{ij0}|E^1_{kl0}\rangle = -\langle E^0_{ij1}|E^1_{kl1}\rangle$$

Additional degrees of freedom

Operator

$$\alpha |0_L\rangle_{12} \to \sum_{ij} |ij\rangle_{12} |E^0_{ij}\rangle_K$$
$$\beta |1_L\rangle_{12} \to \sum_{ij} |ij\rangle_{12} |E^1_{ij}\rangle_K$$

Generalized

$$\alpha |0_L\rangle_{123} \to \sum_{ijk} |ijk\rangle_{123} |E^0_{ijk}\rangle_K$$
$$\beta |1_L\rangle_{123} \to \sum_{ijk} |ijk\rangle_{123} |E^1_{ijk}\rangle_K$$

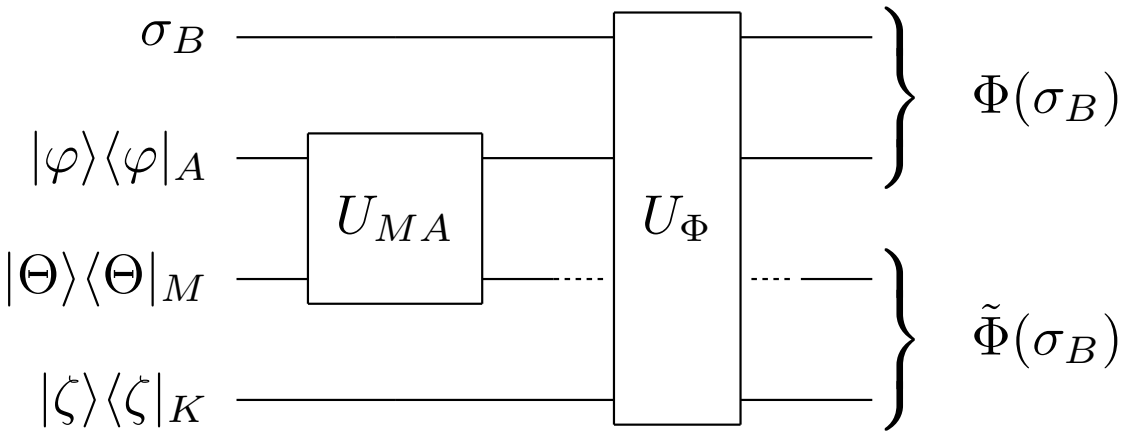
- Operator privacy:

$$\implies \langle E^0_{ij}|E^0_{kl}\rangle = \langle E^1_{ij}|E^1_{kl}\rangle,$$
$$\langle E^0_{ij}|E^1_{kl}\rangle = 0$$

- Generalized operator privacy:

$$\langle E^0_{ij0}|E^0_{kl0}\rangle + \langle E^0_{ij1}|E^0_{kl1}\rangle = \langle E^1_{ij0}|E^1_{kl0}\rangle + \langle E^1_{ij1}|E^1_{kl1}\rangle$$
$$\langle E^0_{ij0}|E^1_{kl0}\rangle = -\langle E^0_{ij1}|E^1_{kl1}\rangle$$

Generalized complementary channel



- By purifying the ancillary space, the duality between privacy and error correction is recovered for private subsystem channels!
- What about a generalized notion of error correction?
  A subsystem B is **generalized operator quantum error correctable** for $\mathcal{E}$ if there exists a channel $\mathcal{R}$, a fixed state σ_A, and a state τ_A such that

$$\mathcal{R} \circ \mathcal{E}(\sigma_A \otimes \sigma_B) = \tau_A \otimes \sigma_B, \ \forall \ \sigma_B$$

New notion of QEC?

A subsystem B is **generalized operator quantum error correctable (GenOQEC)** for $\mathcal{E}$ if there exists a channel $\mathcal{R}$, a fixed state σ_A, and a state τ_A such that

$$\mathcal{R} \circ \mathcal{E}(\sigma_A \otimes \sigma_B) = \tau_A \otimes \sigma_B, \ \forall \ \sigma_B$$

- There is no added benefit to the generalized notion of operator quantum error correction
- Given a GenOQEC channel Φ for a subsystem B with a fixed ancilla state $\sigma_A = \sum p_i |\psi_i\rangle\langle\psi_i|$ and output ancilla τ_A. Then, the channel is OQEC for any $|\psi_i\rangle\langle\psi_i|$[4]:

$$\implies B \text{ is OQEC for } \Phi$$

[4] TJ, Kribs, Laflamme, Plosker (2014)

Summary

- Private quantum channels provide a quantum analog to the classical one-time pad
- Random commuting unitary channels cannot yield operator private subsystems
- Encoding information into fixed subsystems provide additional freedom
- Duality between general private subsystems and error correction only recovered when extending the Hilbert space beyond standard complementarity

Thank you for your attention!

Fonds de recherche Nature et technologies Québec

NSERC CRSNG

Ontario

CIFAR
CANADIAN INSTITUTE for ADVANCED RESEARCH

Industry Canada Industrie Canada