Unspeakable cryptography

Jamie Vicary (joint with Dominic Verdon)
Department of Computer Science, University of Oxford

Oxford Cryptography Day
Mathematical Institute, University of Oxford
17 March 2016

Speakable information

Communication channels are a useful and common abstraction.

Speakable information

Communication channels are a useful and common abstraction.

We usually assume they transmit arbitrary quantum or classical information.

Speakable information

Communication channels are a useful and common abstraction.

We usually assume they transmit arbitrary quantum or classical information.

Such information is *speakable*.

Speakable information

Communication channels are a useful and common abstraction.

We usually assume they transmit arbitrary quantum or classical information.

Such information is *speakable*.

But there is a hidden assumption: parties share a reference frame.

Speakable information

Communication channels are a useful and common abstraction.

We usually assume they transmit arbitrary quantum or classical information.

Such information is *speakable*.

But there is a hidden assumption: parties share a reference frame.

More generally, you cannot transmit *resources*, like charge.

Unspeakable information

Unspeakable information can't be transmitted through a channel.

Unspeakable information

Unspeakable information can't be transmitted through a channel.

Information can *become* unspeakable when there is no shared reference frame.

Unspeakable information

Unspeakable information can't be transmitted through a channel.

Information can *become* unspeakable when there is no shared reference frame.

Unspeakable information can be transmitted by *material objects*.

Unspeakable information

Unspeakable information can't be transmitted through a channel.

Information can *become* unspeakable when there is no shared reference frame.

Unspeakable information can be transmitted by *material objects*.

To an aviator lost in fog, without instruments—how do you transmit the *direction* of home?

Unspeakable information

Unspeakable information can't be transmitted through a channel.

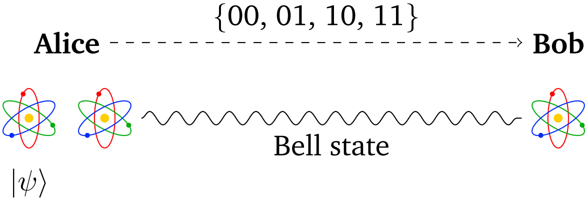
Information can *become* unspeakable when there is no shared reference frame.

Unspeakable information can be transmitted by *material objects*.

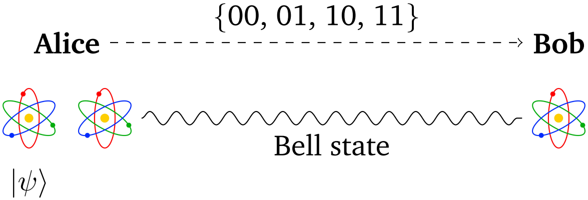
To an aviator lost in fog, without instruments—how do you transmit the *direction* of home?

Given a classical channel to an alien species, how do you *define* 'left' and 'right'?

Unspeakable quantum teleportation

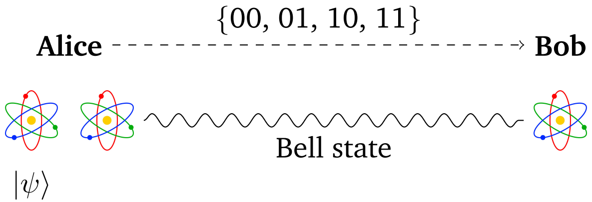


Unspeakable quantum teleportation



Qubit teleportation involves the following steps:

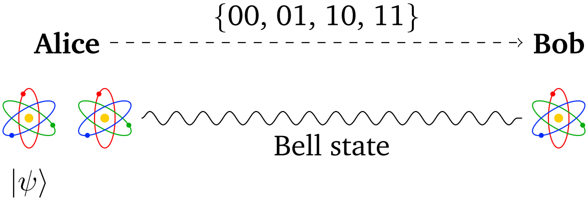
Unspeakable quantum teleportation



Qubit teleportation involves the following steps:

- Alice has a qubit state $|\psi\rangle$ to be transmitted.

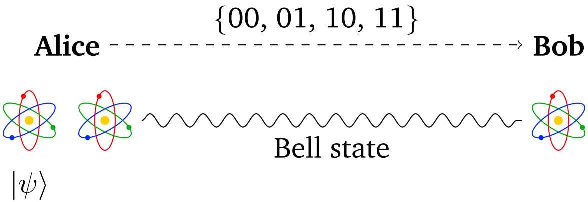
Unspeakable quantum teleportation



Qubit teleportation involves the following steps:

- Alice has a qubit state $|\psi\rangle$ to be transmitted.
- Alice and Bob share a Bell state.

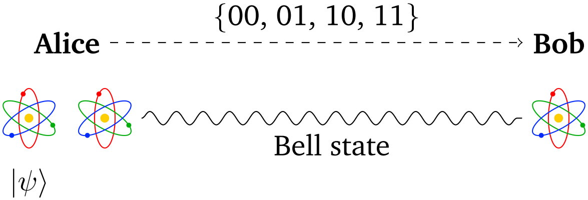
Unspeakable quantum teleportation



Qubit teleportation involves the following steps:

- Alice has a qubit state $|\psi\rangle$ to be transmitted.
- Alice and Bob share a Bell state.
- Alice performs a bipartite measurement, receiving result $i \in \{00, 01, 10, 11\}$, which is sent to Bob by a *classical channel*.

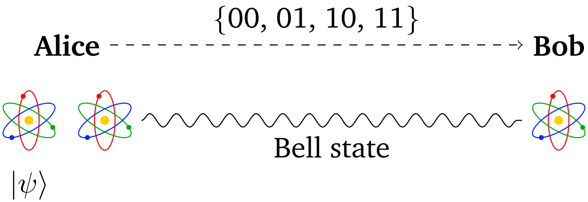
Unspeakable quantum teleportation



Qubit teleportation involves the following steps:

- Alice has a qubit state $|\psi\rangle$ to be transmitted.
- Alice and Bob share a Bell state.
- Alice performs a bipartite measurement, receiving result $i \in \{00, 01, 10, 11\}$, which is sent to Bob by a *classical channel*.
- Bob then performs a unitary operator U_i to his system.

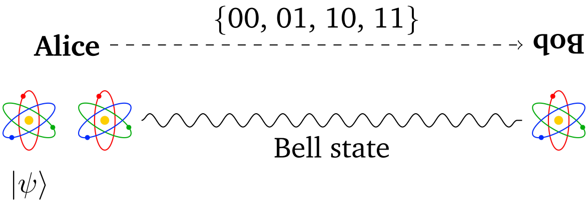
Unspeakable quantum teleportation



Qubit teleportation involves the following steps:

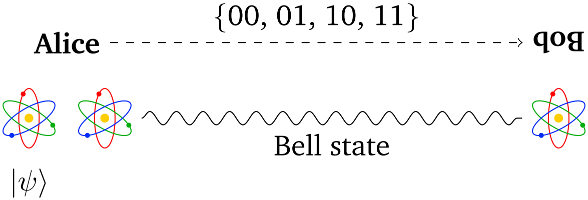
- Alice has a qubit state $|\psi\rangle$ to be transmitted.
- Alice and Bob share a Bell state.
- Alice performs a bipartite measurement, receiving result $i \in \{00, 01, 10, 11\}$, which is sent to Bob by a *classical channel*.
- Bob then performs a unitary operator U_i to his system.
- Success means that Bob's system is now in state $|\psi\rangle$.

Unspeakable quantum teleportation



If Alice and Bob don't share a reference frame, then $|\psi\rangle$ becomes *unspeakable*, since nothing Alice says can help Bob construct it.

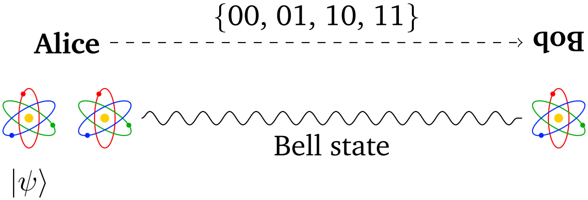
Unspeakable quantum teleportation



If Alice and Bob don't share a reference frame, then $|\psi\rangle$ becomes *unspeakable*, since nothing Alice says can help Bob construct it.

Can $|\phi\rangle$ still be teleported?

Unspeakable quantum teleportation

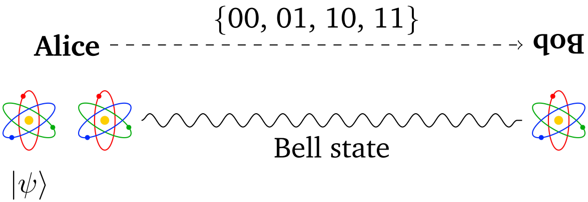


If Alice and Bob don't share a reference frame, then $|\psi\rangle$ becomes *unspeakable*, since nothing Alice says can help Bob construct it.

Can $|\phi\rangle$ still be teleported?

If Bob is rotated by 180°, his system exhibits a representation of $\mathbb{Z}_2$, defined by some unitary V such that $V^2 = \mathrm{id}$.

Unspeakable quantum teleportation



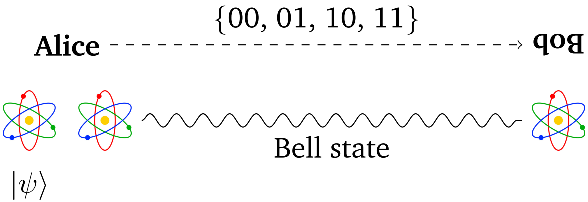
If Alice and Bob don't share a reference frame, then $|\psi\rangle$ becomes *unspeakable*, since nothing Alice says can help Bob construct it.

Can $|\phi\rangle$ still be teleported?

If Bob is rotated by 180°, his system exhibits a representation of $\mathbb{Z}_2$, defined by some unitary V such that $V^2 = \mathrm{id}$.

When Bob applies a unitary U_i, it appears *in Alice's frame* that he is performing $V^\dagger U_i V$.

Unspeakable quantum teleportation



If Alice and Bob don't share a reference frame, then $|\psi\rangle$ becomes *unspeakable*, since nothing Alice says can help Bob construct it.

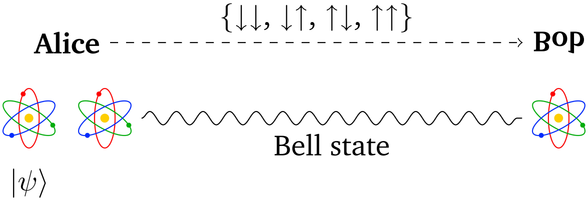
Can $|\phi\rangle$ still be teleported?

If Bob is rotated by $180°$, his system exhibits a representation of $\mathbb{Z}_2$, defined by some unitary V such that $V^2 = \text{id}$.

When Bob applies a unitary U_i, it appears *in Alice's frame* that he is performing $V^\dagger U_i V$.

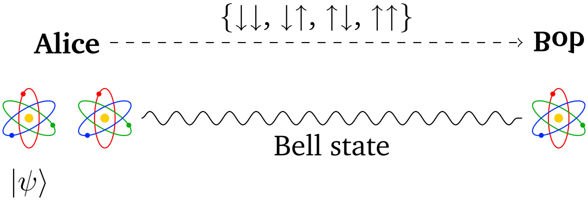
This *breaks* quantum teleportation: "unspeakable information cannot be teleported".

Unspeakable quantum teleportation



New idea: Alice encodes her 2 bits *unspeakably*, as physical arrows.

Unspeakable quantum teleportation

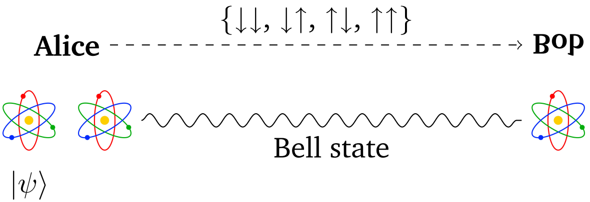


New idea: Alice encodes her 2 bits *unspeakably*, as physical arrows.

Let's track the possibilities:

Alice' result	**Bob's action**	**Bop's action**
$\uparrow\uparrow$	$U_{\uparrow\uparrow}$	$V^\dagger\, U_{\downarrow\downarrow}\, V$

Unspeakable quantum teleportation

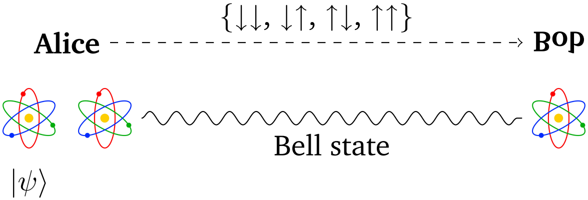


New idea: Alice encodes her 2 bits *unspeakably*, as physical arrows.

Let's track the possibilities:

Alice' result	**Bob's action**	**Bop's action**
$\uparrow\uparrow$	$U_{\uparrow\uparrow}$	$V^\dagger\, U_{\downarrow\downarrow}\, V$
$\uparrow\downarrow$	$U_{\uparrow\downarrow}$	$V^\dagger\, U_{\downarrow\uparrow}\, V$

Unspeakable quantum teleportation

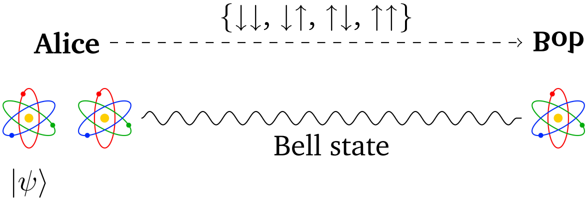


New idea: Alice encodes her 2 bits *unspeakably*, as physical arrows.

Let's track the possibilities:

Alice' result	Bob's action	Bop's action
$\uparrow\uparrow$	$U_{\uparrow\uparrow}$	$V^\dagger\, U_{\downarrow\downarrow}\, V$
$\uparrow\downarrow$	$U_{\uparrow\downarrow}$	$V^\dagger\, U_{\downarrow\uparrow}\, V$
$\downarrow\uparrow$	$U_{\downarrow\uparrow}$	$V^\dagger\, U_{\uparrow\downarrow}\, V$

Unspeakable quantum teleportation

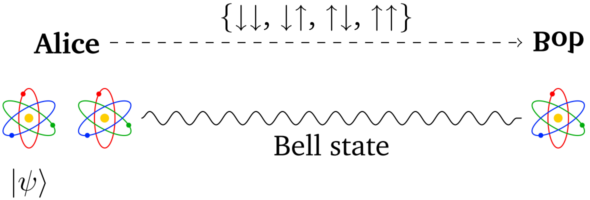


New idea: Alice encodes her 2 bits *unspeakably*, as physical arrows.

Let's track the possibilities:

Alice' result	Bob's action	Bop's action
$\uparrow\uparrow$	$U_{\uparrow\uparrow}$	$V^\dagger U_{\downarrow\downarrow} V$
$\uparrow\downarrow$	$U_{\uparrow\downarrow}$	$V^\dagger U_{\downarrow\uparrow} V$
$\downarrow\uparrow$	$U_{\downarrow\uparrow}$	$V^\dagger U_{\uparrow\downarrow} V$
$\downarrow\downarrow$	$U_{\downarrow\downarrow}$	$V^\dagger U_{\uparrow\uparrow} V$

Unspeakable quantum teleportation



New idea: Alice encodes her 2 bits *unspeakably*, as physical arrows.

Let's track the possibilities:

Alice' result	**Bob's action**	**Bop's action**
$\uparrow\uparrow$	$U_{\uparrow\uparrow}$	$V^\dagger\, U_{\downarrow\downarrow}\, V$
$\uparrow\downarrow$	$U_{\uparrow\downarrow}$	$V^\dagger\, U_{\downarrow\uparrow}\, V$
$\downarrow\uparrow$	$U_{\downarrow\uparrow}$	$V^\dagger\, U_{\uparrow\downarrow}\, V$
$\downarrow\downarrow$	$U_{\downarrow\downarrow}$	$V^\dagger\, U_{\uparrow\uparrow}\, V$

If columns 2 and 3 are identical, teleportation always succeeds.

Unspeakable quantum teleportation

Here is a solution:

$$U_{\downarrow\downarrow} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \qquad U_{\downarrow\uparrow} = \frac{1}{4}\begin{pmatrix} -\sqrt{2}-\sqrt{6} & -\sqrt{2}+\sqrt{6} \\ -\sqrt{2}+\sqrt{6} & \sqrt{2}+\sqrt{6} \end{pmatrix}$$

$$U_{\uparrow\uparrow} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \qquad U_{\uparrow\downarrow} = \frac{1}{4}\begin{pmatrix} \sqrt{2}-\sqrt{6} & -\sqrt{2}-\sqrt{6} \\ -\sqrt{2}-\sqrt{6} & -\sqrt{2}+\sqrt{6} \end{pmatrix}$$

$$V = \begin{pmatrix} \sqrt{3}/2 & 1/2 \\ 1/2 & -\sqrt{3}/2 \end{pmatrix}$$

Unspeakable quantum teleportation

Here is a solution:

$$U_{\downarrow\downarrow} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \qquad U_{\downarrow\uparrow} = \frac{1}{4}\begin{pmatrix} -\sqrt{2}-\sqrt{6} & -\sqrt{2}+\sqrt{6} \\ -\sqrt{2}+\sqrt{6} & \sqrt{2}+\sqrt{6} \end{pmatrix}$$

$$U_{\uparrow\uparrow} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \qquad U_{\uparrow\downarrow} = \frac{1}{4}\begin{pmatrix} \sqrt{2}-\sqrt{6} & -\sqrt{2}-\sqrt{6} \\ -\sqrt{2}-\sqrt{6} & -\sqrt{2}+\sqrt{6} \end{pmatrix}$$

$$V = \begin{pmatrix} \sqrt{3}/2 & 1/2 \\ 1/2 & -\sqrt{3}/2 \end{pmatrix}$$

So unspeakable quantum teleportation *is* possible in this situation.

Unspeakable quantum teleportation

Here is a solution:

$$U_{\downarrow\downarrow} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \qquad U_{\downarrow\uparrow} = \frac{1}{4}\begin{pmatrix} -\sqrt{2}-\sqrt{6} & -\sqrt{2}+\sqrt{6} \\ -\sqrt{2}+\sqrt{6} & \sqrt{2}+\sqrt{6} \end{pmatrix}$$

$$U_{\uparrow\uparrow} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \qquad U_{\uparrow\downarrow} = \frac{1}{4}\begin{pmatrix} \sqrt{2}-\sqrt{6} & -\sqrt{2}-\sqrt{6} \\ -\sqrt{2}-\sqrt{6} & -\sqrt{2}+\sqrt{6} \end{pmatrix}$$

$$V = \begin{pmatrix} \sqrt{3}/2 & 1/2 \\ 1/2 & -\sqrt{3}/2 \end{pmatrix}$$

So unspeakable quantum teleportation *is* possible in this situation.

Previous approaches have been more complex, involving:

Unspeakable quantum teleportation

Here is a solution:

$$U_{\downarrow\downarrow} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \qquad U_{\downarrow\uparrow} = \frac{1}{4}\begin{pmatrix} -\sqrt{2}-\sqrt{6} & -\sqrt{2}+\sqrt{6} \\ -\sqrt{2}+\sqrt{6} & \sqrt{2}+\sqrt{6} \end{pmatrix}$$

$$U_{\uparrow\uparrow} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \qquad U_{\uparrow\downarrow} = \frac{1}{4}\begin{pmatrix} \sqrt{2}-\sqrt{6} & -\sqrt{2}-\sqrt{6} \\ -\sqrt{2}-\sqrt{6} & -\sqrt{2}+\sqrt{6} \end{pmatrix}$$

$$V = \begin{pmatrix} \sqrt{3}/2 & 1/2 \\ 1/2 & -\sqrt{3}/2 \end{pmatrix}$$

So unspeakable quantum teleportation *is* possible in this situation.

Previous approaches have been more complex, involving:

- extra steps, like synchronizing the reference frames;

Unspeakable quantum teleportation

Here is a solution:

$$U_{\downarrow\downarrow} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \qquad U_{\downarrow\uparrow} = \frac{1}{4}\begin{pmatrix} -\sqrt{2}-\sqrt{6} & -\sqrt{2}+\sqrt{6} \\ -\sqrt{2}+\sqrt{6} & \sqrt{2}+\sqrt{6} \end{pmatrix}$$

$$U_{\uparrow\uparrow} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \qquad U_{\uparrow\downarrow} = \frac{1}{4}\begin{pmatrix} \sqrt{2}-\sqrt{6} & -\sqrt{2}-\sqrt{6} \\ -\sqrt{2}-\sqrt{6} & -\sqrt{2}+\sqrt{6} \end{pmatrix}$$

$$V = \begin{pmatrix} \sqrt{3}/2 & 1/2 \\ 1/2 & -\sqrt{3}/2 \end{pmatrix}$$

So unspeakable quantum teleportation *is* possible in this situation.

Previous approaches have been more complex, involving:

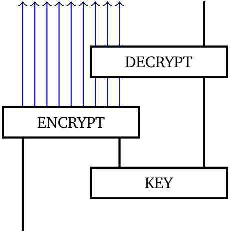
- extra steps, like synchronizing the reference frames;
- extra resources, like more shared entanglement.

Encryption and teleportation

There is a deep analogy between classical encryption and quantum teleportation.

Encryption and teleportation

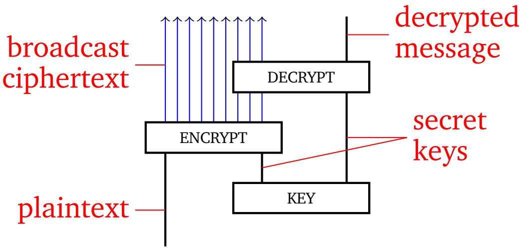
There is a deep analogy between classical encryption and quantum teleportation.



Encrypted communication

Encryption and teleportation

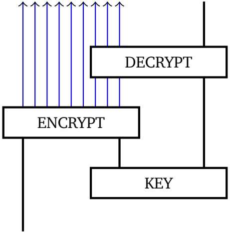
There is a deep analogy between classical encryption and quantum teleportation.



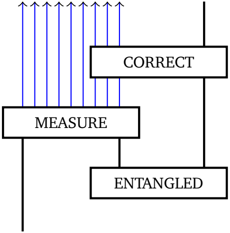
Encrypted communication

Encryption and teleportation

There is a deep analogy between classical encryption and quantum teleportation.



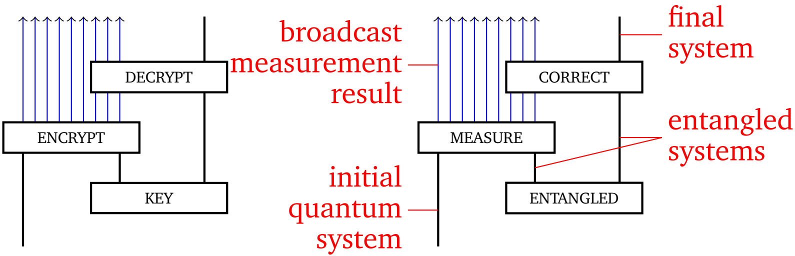
Encrypted communication



Quantum teleportation

Encryption and teleportation

There is a deep analogy between classical encryption and quantum teleportation.

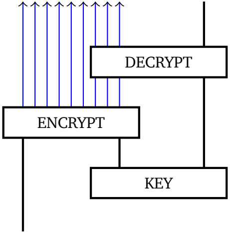


Encrypted communication

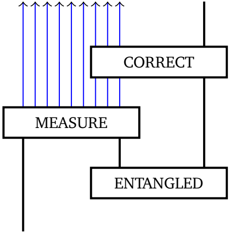
Quantum teleportation

Encryption and teleportation

There is a deep analogy between classical encryption and quantum teleportation.



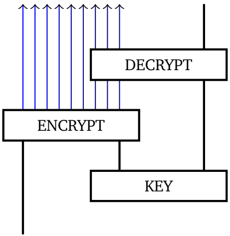
Encrypted communication



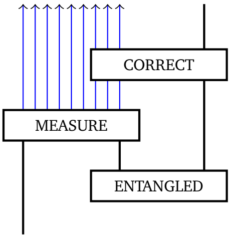
Quantum teleportation

Encryption and teleportation

There is a deep analogy between classical encryption and quantum teleportation.



Encrypted communication



Quantum teleportation

This lets us translate ideas between the two settings.

Unspeakable cryptography

Here is a simple model for ‘unspeakable’ one-time-pad encryption.

Unspeakable cryptography

Here is a simple model for ‘unspeakable’ one-time-pad encryption.

Suppose Alice and Bob share a secret key, but lack a shared reference frame.

Unspeakable cryptography

Here is a simple model for ‘unspeakable’ one-time-pad encryption.

Suppose Alice and Bob share a secret key, but lack a shared reference frame.

Alice can still securely transmit directional information to Bob with the following scheme:

Plaintext	**Key**	**Ciphertext**
$\uparrow$	1	$\downarrow$
$\uparrow$	0	$\uparrow$
$\downarrow$	1	$\uparrow$
$\downarrow$	0	$\downarrow$

Unspeakable cryptography

Here is a simple model for ‘unspeakable’ one-time-pad encryption.

Suppose Alice and Bob share a secret key, but lack a shared reference frame.

Alice can still securely transmit directional information to Bob with the following scheme:

Plaintext	**Key**	**Ciphertext**
$\uparrow$	1	$\downarrow$
$\uparrow$	0	$\uparrow$
$\downarrow$	1	$\uparrow$
$\downarrow$	0	$\downarrow$

Key and ciphertext can’t *both* be speakable or unspeakable.

Category theory!

Research process:

Category theory!

Research process:

- Identifying the abstract structure of teleportation internal to **Hilb**, the category of Hilbert spaces.

Category theory!

Research process:

- Identifying the abstract structure of teleportation internal to **Hilb**, the category of Hilbert spaces.
- Looking for the same structure in **Rep**(G), the category of unitary representations of a finite group.

Category theory!

Research process:

- Identifying the abstract structure of teleportation internal to **Hilb**, the category of Hilbert spaces.
- Looking for the same structure in **Rep**(G), the category of unitary representations of a finite group.
- Realizing this is nontrivial.

Category theory!

Research process:

- Identifying the abstract structure of teleportation internal to **Hilb**, the category of Hilbert spaces.
- Looking for the same structure in **Rep**(G), the category of unitary representations of a finite group.
- Realizing this is nontrivial.
- Working out what on earth it's supposed to mean.

Category theory!

Research process:

- Identifying the abstract structure of teleportation internal to **Hilb**, the category of Hilbert spaces.
- Looking for the same structure in **Rep**(G), the category of unitary representations of a finite group.
- Realizing this is nontrivial.
- Working out what on earth it's supposed to mean.

Information is *unspeakable* when it is encoded in a nontrivial representation of a group.

Category theory!

Research process:

- Identifying the abstract structure of teleportation internal to **Hilb**, the category of Hilbert spaces.
- Looking for the same structure in **Rep**(G), the category of unitary representations of a finite group.
- Realizing this is nontrivial.
- Working out what on earth it's supposed to mean.

Information is *unspeakable* when it is encoded in a nontrivial representation of a group.

Spatial degree of freedom: $G \subset SO(3)$

Category theory!

Research process:

- Identifying the abstract structure of teleportation internal to **Hilb**, the category of Hilbert spaces.
- Looking for the same structure in **Rep**(G), the category of unitary representations of a finite group.
- Realizing this is nontrivial.
- Working out what on earth it's supposed to mean.

Information is *unspeakable* when it is encoded in a nontrivial representation of a group.

Spatial degree of freedom: $G \subset SO(3)$

Charge degree of freedom: $G \subset SU(3) \times SU(2) \times U(1)$

Category theory!

Research process:

- Identifying the abstract structure of teleportation internal to **Hilb**, the category of Hilbert spaces.
- Looking for the same structure in **Rep**(G), the category of unitary representations of a finite group.
- Realizing this is nontrivial.
- Working out what on earth it's supposed to mean.

Information is *unspeakable* when it is encoded in a nontrivial representation of a group.

Spatial degree of freedom: $G \subset SO(3)$

Charge degree of freedom: $G \subset SU(3) \times SU(2) \times U(1)$

Thanks for listening!