Logical Foundations for Classical Encryption and Quantum Teleportation

Jamie Vicary
Centre for Quantum Technologies, University of Singapore
and Department of Computer Science, University of Oxford

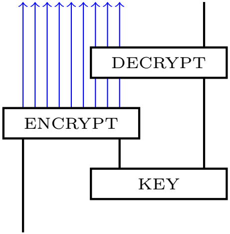
Post-Quantum Research: Identifying Future Challenges and Directions
Isaac Newton Institute, University of Cambridge
9 May 2014

Introduction

There is a deep analogy between encryption and teleportation:

Introduction

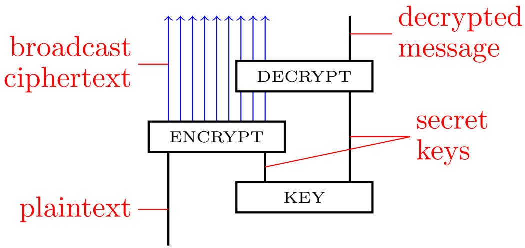
There is a deep analogy between encryption and teleportation:



Encrypted communication

Introduction

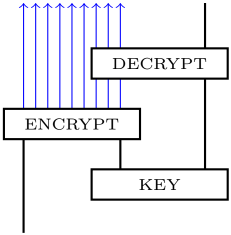
There is a deep analogy between encryption and teleportation:



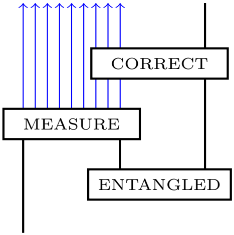
Encrypted communication

Introduction

There is a deep analogy between encryption and teleportation:



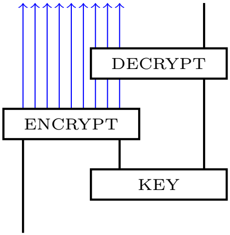
Encrypted communication



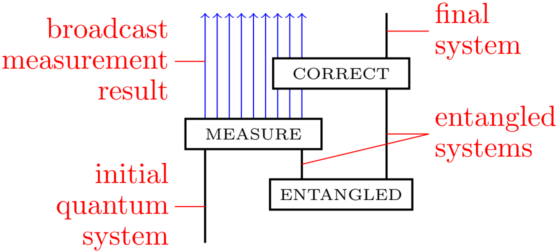
Quantum teleportation

Introduction

There is a deep analogy between encryption and teleportation:



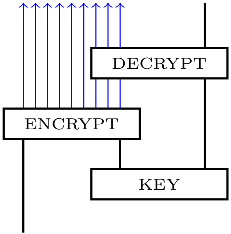
Encrypted communication



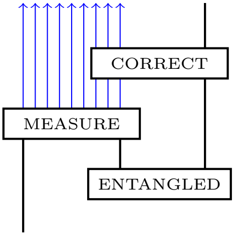
Quantum teleportation

Introduction

There is a deep analogy between encryption and teleportation:



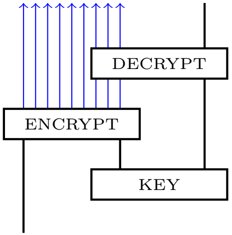
Encrypted communication



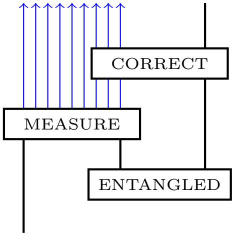
Quantum teleportation

Introduction

There is a deep analogy between encryption and teleportation:



Encrypted communication

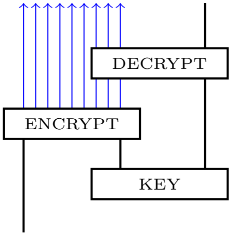


Quantum teleportation

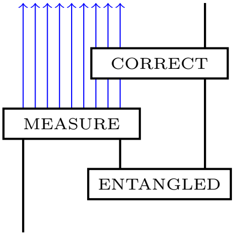
New idea. We can make this precise using *geometrical* mathematics.

Introduction

There is a deep analogy between encryption and teleportation:



$\mapsto$



Encrypted communication

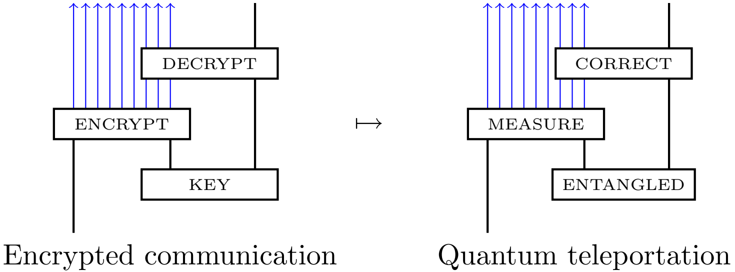
Quantum teleportation

New idea. We can make this precise using *geometrical* mathematics.

Nice result. There is a general classical-to-quantum construction.

Introduction

There is a deep analogy between encryption and teleportation:



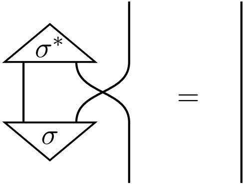
New idea. We can make this precise using *geometrical* mathematics.

Nice result. There is a general classical-to-quantum construction.

Part of the *categorical quantum computing* programme launched by Abramsky and Coecke in 2004.

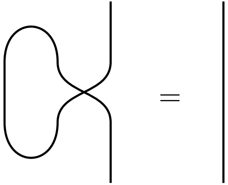
Strings and correlation

Consider the following equation, where σ is a bipartite state preparation and σ^* is the corresponding bipartite postselection:



Strings and correlation

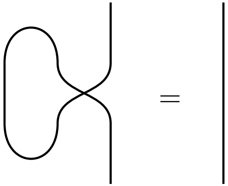
Consider the following equation, where σ is a bipartite state preparation and σ^* is the corresponding bipartite postselection:



We change notation and use **topological strings**.

Strings and correlation

Consider the following equation, where σ is a bipartite state preparation and σ^* is the corresponding bipartite postselection:



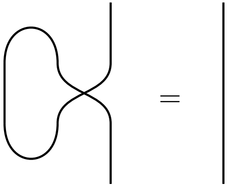
We change notation and use **topological strings**.

We can investigate consequences of this equation in different settings.

- **Quantum theory.**
  The state σ is *maximally entangled*: $|\sigma\rangle = |00\rangle + |11\rangle$

Strings and correlation

Consider the following equation, where σ is a bipartite state preparation and σ^* is the corresponding bipartite postselection:



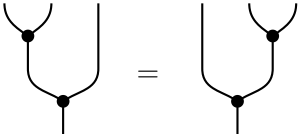
We change notation and use **topological strings**.

We can investigate consequences of this equation in different settings.

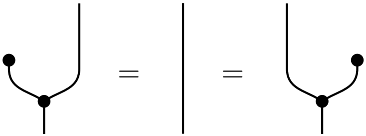
- **Quantum theory.**
  The state σ is *maximally entangled*: $|\sigma\rangle = |00\rangle + |11\rangle$
- **Classical computation.**
  The state σ is *perfectly correlated*: $\sigma = \{00\} \cup \{11\}$.

Surfaces and logic

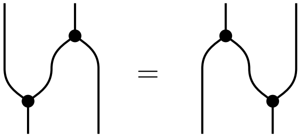
We now think about basic properties of copying, comparing and deleting classical information:



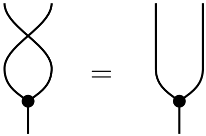
Associativity



Unit



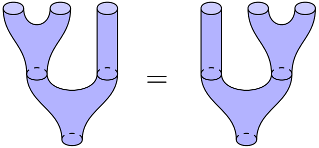
Frobenius law



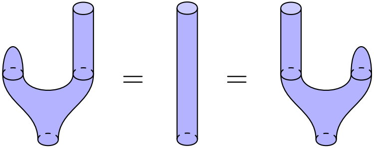
Commutativity

Surfaces and logic

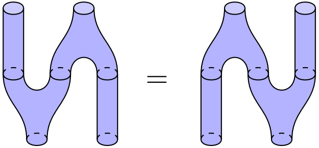
We now think about basic properties of copying, comparing and deleting classical information:



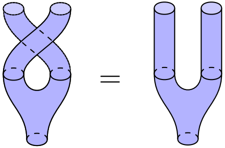
Associativity



Unit



Frobenius law

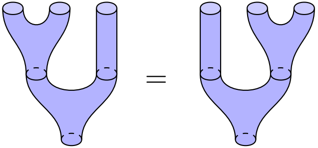


Commutativity

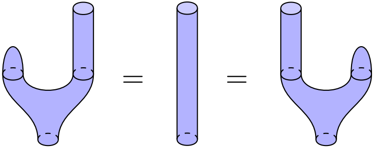
These are the laws obeyed by surfaces up to deformation!

Surfaces and logic

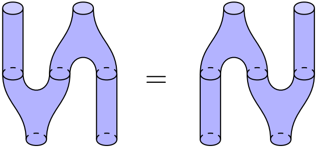
We now think about basic properties of copying, comparing and deleting classical information:



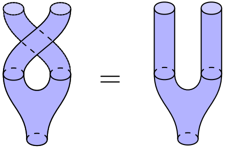
Associativity



Unit



Frobenius law

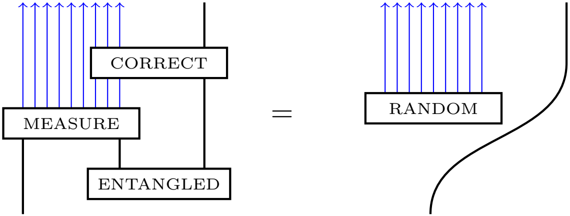


Commutativity

These are the laws obeyed by surfaces up to deformation!
So we change notation and use **topological surfaces**.

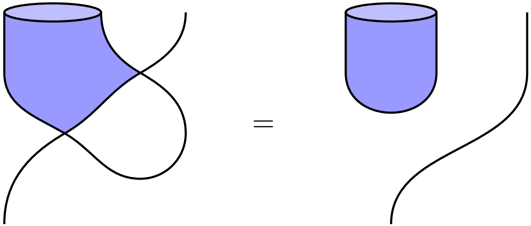
Geometrical structure

Here is ordinary teleportation:



Geometrical structure

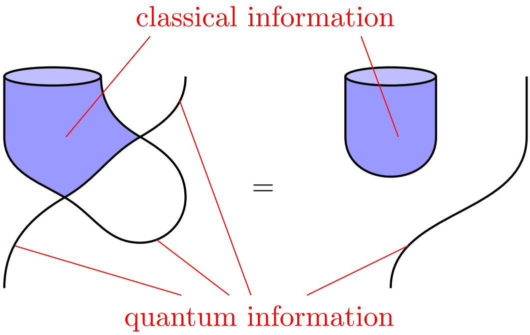
Here is ordinary teleportation:



We make it rigorous with this geometrical equation.

Geometrical structure

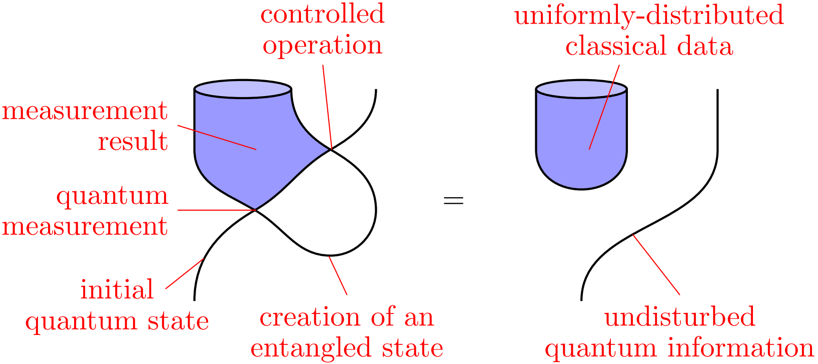
Here is ordinary teleportation:



We make it rigorous with this geometrical equation.

Geometrical structure

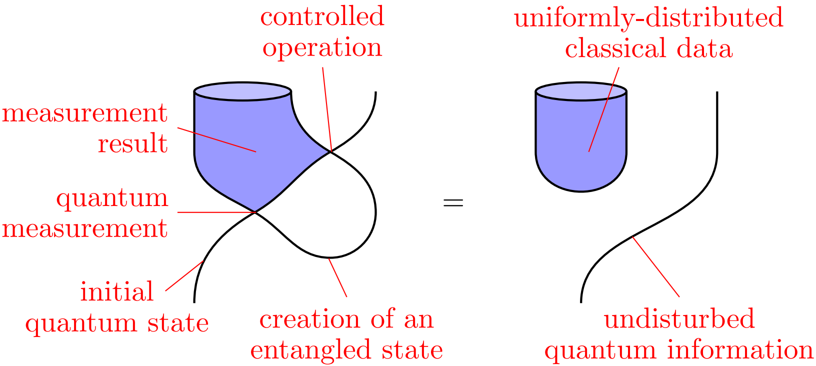
Here is ordinary teleportation:



We make it rigorous with this geometrical equation.

Geometrical structure

Here is ordinary teleportation:

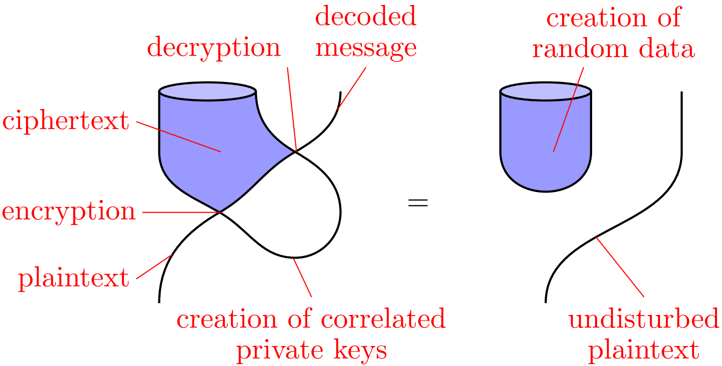


We make it rigorous with this geometrical equation.

Theorem. Quantum solutions correspond exactly to implementations of quantum teleportation.

Geometrical structure

Here is ordinary teleportation:

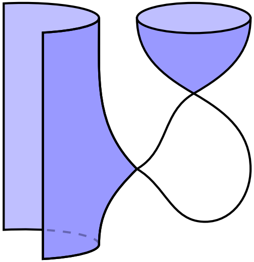


We make it rigorous with this geometrical equation.

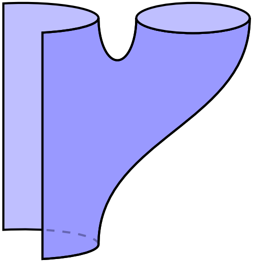
Theorem. Classical solutions correspond exactly to implementations of classical one-time-pad encryption.

Dense coding

This equation describes *dense coding*:

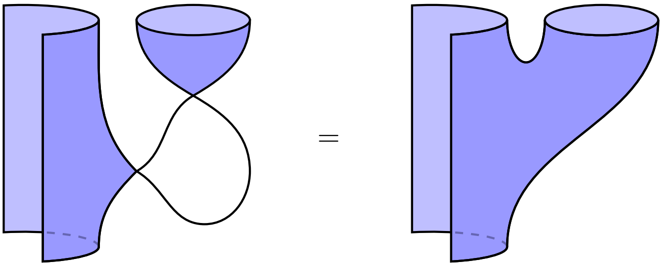


$$=$$



Dense coding

This equation describes *dense coding*:



It describes the transmission of data through a channel with only *half* the apparent required capacity!

This is *topologically equivalent* to the teleportation equation.

So what?

So what?

- Allows us to reason *logically* about cryptographic primitives in both quantum and classical computation.

So what?

- Allows us to reason *logically* about cryptographic primitives in both quantum and classical computation.
- Provides a formal foundation for *computational support* tools.

So what?

- Allows us to reason *logically* about cryptographic primitives in both quantum and classical computation.
- Provides a formal foundation for *computational support* tools.
- Gives a unified setting to consider *integrated* classical and quantum phenomena—for example, QKD+OTP.

So what?

- Allows us to reason *logically* about cryptographic primitives in both quantum and classical computation.
- Provides a formal foundation for *computational support* tools.
- Gives a unified setting to consider *integrated* classical and quantum phenomena—for example, QKD+OTP.
- Addresses fascinating *conceptual* questions:

So what?

- Allows us to reason *logically* about cryptographic primitives in both quantum and classical computation.
- Provides a formal foundation for *computational support* tools.
- Gives a unified setting to consider *integrated* classical and quantum phenomena—for example, QKD+OTP.
- Addresses fascinating *conceptual* questions:
  - What is the fundamental relationship between classical and quantum computation?

So what?

- Allows us to reason *logically* about cryptographic primitives in both quantum and classical computation.

- Provides a formal foundation for *computational support* tools.

- Gives a unified setting to consider *integrated* classical and quantum phenomena—for example, QKD+OTP.

- Addresses fascinating *conceptual* questions:
  - What is the fundamental relationship between classical and quantum computation?
  - What is the mathematical structure of quantum information flow?

So what?

- Allows us to reason *logically* about cryptographic primitives in both quantum and classical computation.
- Provides a formal foundation for *computational support* tools.
- Gives a unified setting to consider *integrated* classical and quantum phenomena—for example, QKD+OTP.
- Addresses fascinating *conceptual* questions:
  - What is the fundamental relationship between classical and quantum computation?
  - What is the mathematical structure of quantum information flow?

Thank you!