

A 2-CATEGORICAL ANALYSIS OF COMPLEMENTARY FAMILIES AND QUANTUM KEY DISTRIBUTION

Krzysztof Bar¹ Jamie Vicary²

¹Department of Computer Science, University of Oxford

²Centre for Quantum Technologies, National University of Singapore
and Department of Computer Science, University of Oxford

QPL Kyoto, 6th June 2014

INTRODUCTION

2-categories allow us to reason about quantum measurements in a more elegant way and with fewer equations

INTRODUCTION

2-categories allow us to reason about quantum measurements in a more elegant way and with fewer equations

Graphical calculus:

0-cells Regions Classical information



INTRODUCTION

2-categories allow us to reason about quantum measurements in a more elegant way and with fewer equations

Graphical calculus:

<i>0-cells</i>	Regions	Classical information
<i>1-cells</i>	Lines	Quantum systems

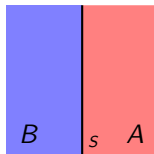
$$B \xrightarrow{s} A$$

INTRODUCTION

2-categories allow us to reason about quantum measurements in a more elegant way and with fewer equations

Graphical calculus:

<i>0-cells</i>	Regions	Classical information
<i>1-cells</i>	Lines	Quantum systems

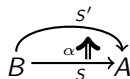


INTRODUCTION

2-categories allow us to reason about quantum measurements in a more elegant way and with fewer equations

Graphical calculus:

<i>0-cells</i>	Regions	Classical information
<i>1-cells</i>	Lines	Quantum systems
<i>2-cells</i>	Vertices	Quantum dynamics

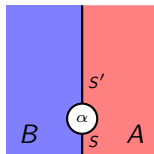


INTRODUCTION

2-categories allow us to reason about quantum measurements in a more elegant way and with fewer equations

Graphical calculus:

<i>0-cells</i>	Regions	Classical information
<i>1-cells</i>	Lines	Quantum systems
<i>2-cells</i>	Vertices	Quantum dynamics



INTRODUCTION

2-categories allow us to reason about quantum measurements in a more elegant way and with fewer equations

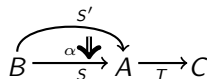
Graphical calculus:

0-cells Regions Classical information

1-cells Lines Quantum systems

2-cells Vertices Quantum dynamics

Horizontal composition



INTRODUCTION

2-categories allow us to reason about quantum measurements in a more elegant way and with fewer equations

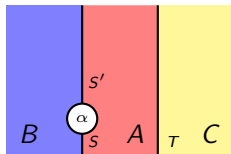
Graphical calculus:

0-cells Regions Classical information

1-cells Lines Quantum systems

2-cells Vertices Quantum dynamics

Horizontal composition



INTRODUCTION

2-categories allow us to reason about quantum measurements in a more elegant way and with fewer equations

Graphical calculus:

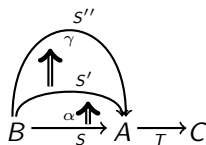
0-cells Regions Classical information

1-cells Lines Quantum systems

2-cells Vertices Quantum dynamics

Horizontal composition

Vertical composition



INTRODUCTION

2-categories allow us to reason about quantum measurements in a more elegant way and with fewer equations

Graphical calculus:

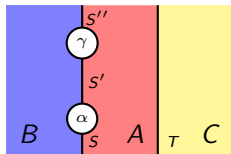
0-cells Regions Classical information

1-cells Lines Quantum systems

2-cells Vertices Quantum dynamics

Horizontal composition

Vertical composition



INTRODUCTION

2-categories allow us to reason about quantum measurements in a more elegant way and with fewer equations

Graphical calculus:

0-cells Regions Classical information

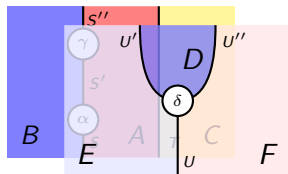
1-cells Lines Quantum systems

2-cells Vertices Quantum dynamics

Horizontal composition

Vertical composition

Tensor product



INTRODUCTION

2-categories allow us to reason about quantum measurements in a more elegant way and with fewer equations

Graphical calculus:

0-cells Regions Classical information

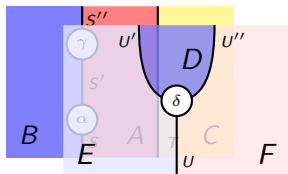
1-cells Lines Quantum systems

2-cells Vertices Quantum dynamics

Horizontal composition

Vertical composition

Tensor product



Semantics given by the symmetric monoidal 2-category **2Hilb** that has:

- *0-cells* given by natural numbers
- *1-cells* - matrices whose entries are finite-dimensional Hilbert spaces
- *2-cells* given by matrices whose entries are linear maps

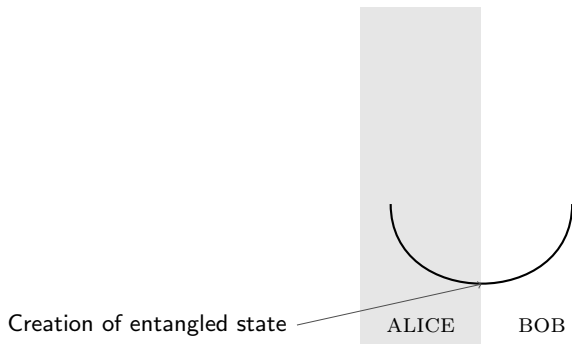
QUANTUM KEY DISTRIBUTION VIA E91



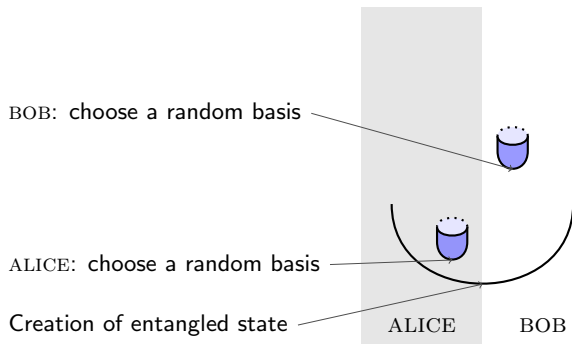
ALICE

BOB

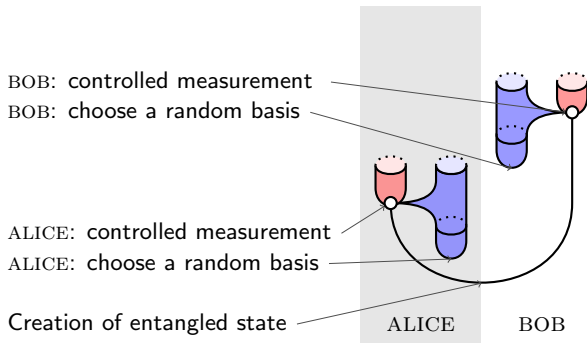
QUANTUM KEY DISTRIBUTION VIA E91



QUANTUM KEY DISTRIBUTION VIA E91

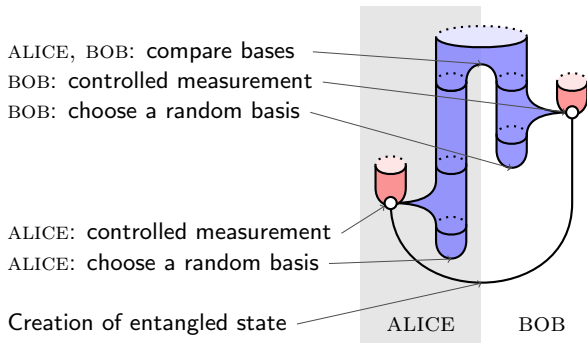


QUANTUM KEY DISTRIBUTION VIA E91



basis information
key information

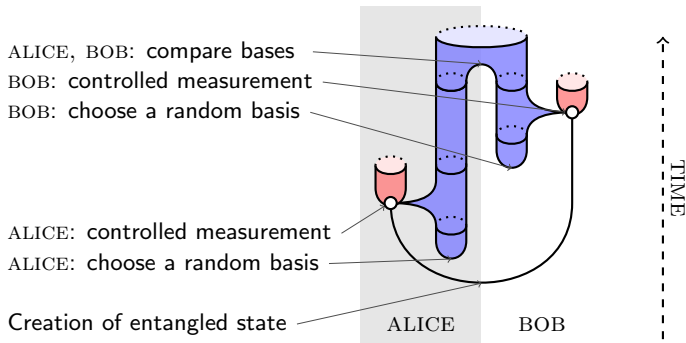
QUANTUM KEY DISTRIBUTION VIA E91



basis information
key information

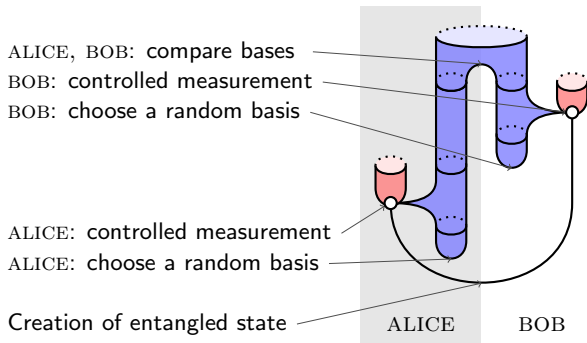
QUANTUM KEY DISTRIBUTION VIA E91

Vertical 2-cell composition corresponds to temporal composition.
Horizontal 2-cell composition corresponds to spatial composition



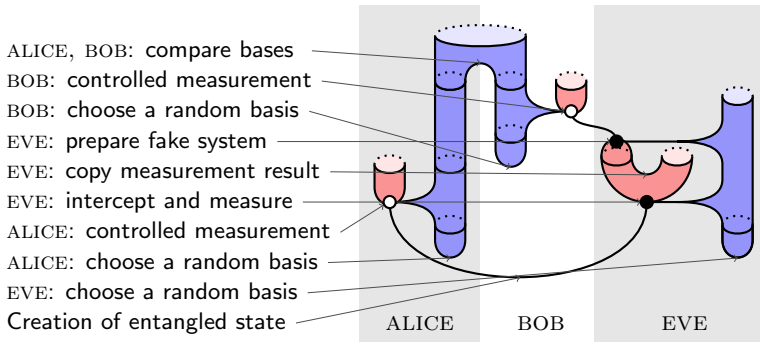
By choosing a 2-category these diagrams are interpreted in, we choose the theory of Physics to work in. Quantum theory is modelled by **2Hilb**.

QUANTUM KEY DISTRIBUTION VIA E91



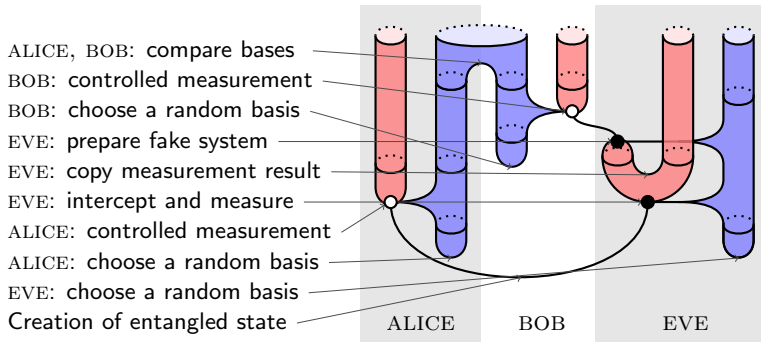
basis information
key information

QUANTUM KEY DISTRIBUTION VIA E91



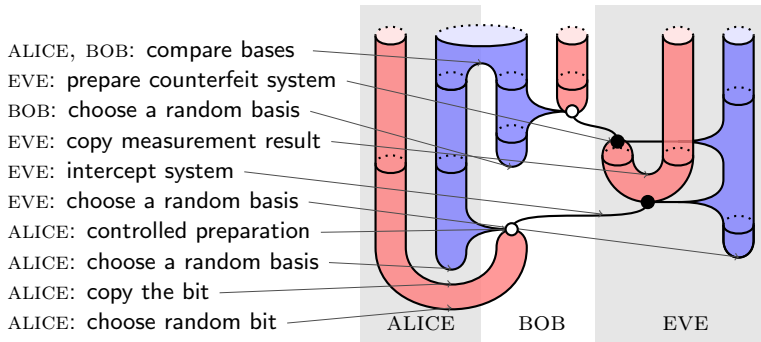
basis information
key information

QUANTUM KEY DISTRIBUTION VIA E91



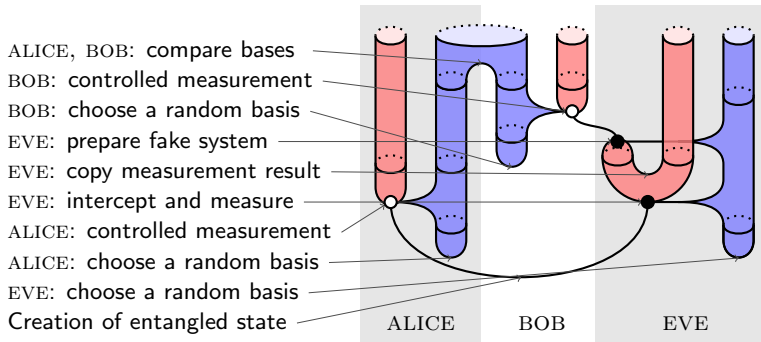
basis information
key information

QUANTUM KEY DISTRIBUTION VIA E91



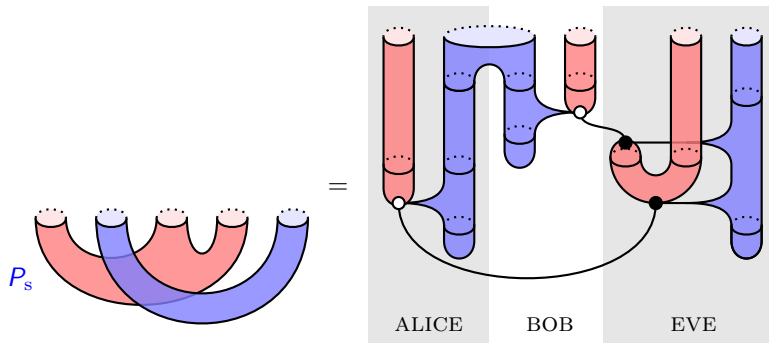
basis information
key information

QUANTUM KEY DISTRIBUTION VIA E91



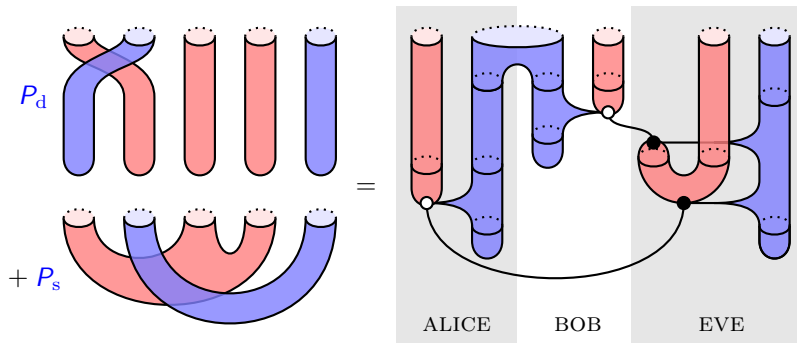
basis information
key information

QUANTUM KEY DISTRIBUTION VIA E91



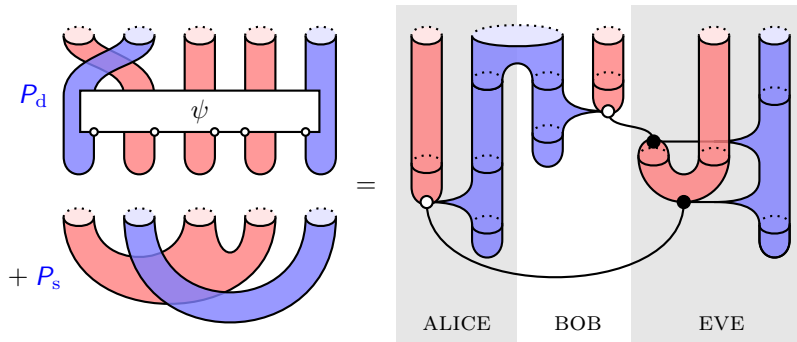
basis information
key information

QUANTUM KEY DISTRIBUTION VIA E91

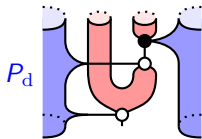


basis information
key information

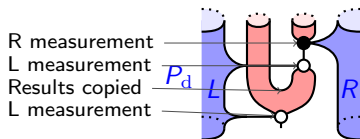
QUANTUM KEY DISTRIBUTION VIA E91



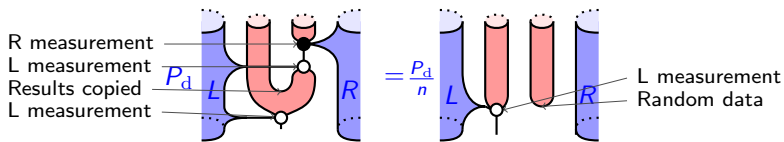
COMPLEMENTARITY OF FAMILIES OF CONTROLLED OPERATIONS



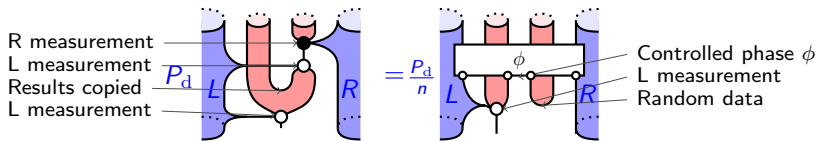
COMPLEMENTARITY OF FAMILIES OF CONTROLLED OPERATIONS



COMPLEMENTARITY OF FAMILIES OF CONTROLLED OPERATIONS

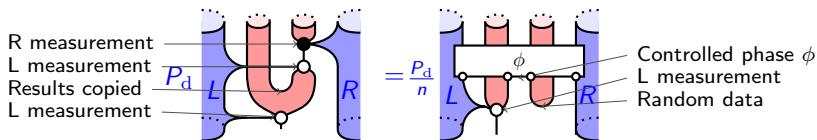


COMPLEMENTARITY OF FAMILIES OF CONTROLLED OPERATIONS



COMPLEMENTARITY OF FAMILIES OF CONTROLLED OPERATIONS

Controlled complementarity A family of controlled operations is *complementary*, if there exists a phase ψ such that:

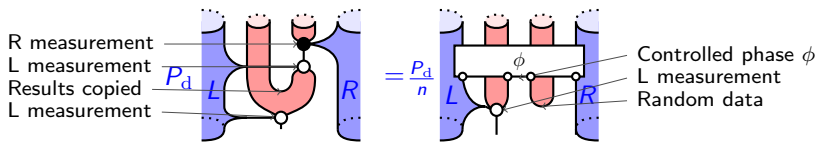


THEOREM

Solutions to the controlled complementarity equation in 2Hilb correspond to families of mutually unbiased bases

COMPLEMENTARITY OF FAMILIES OF CONTROLLED OPERATIONS

Controlled complementarity A family of controlled operations is *complementary*, if there exists a phase ψ such that:



THEOREM

Solutions to the controlled complementarity equation in 2Hilb correspond to families of mutually unbiased bases

THEOREM

The QKD equation and the Controlled complementarity equation are topologically equivalent

SUMMARY

What is the significance of this work?

SUMMARY

What is the significance of this work?

- Completely syntactic proof of $\text{QKD} \Leftrightarrow \text{MUB}$ equivalence that uses only the logical structure

SUMMARY

What is the significance of this work?

- Completely syntactic proof of $\text{QKD} \Leftrightarrow \text{MUB}$ equivalence that uses only the logical structure

Also in the paper:

- Logical correctness proof of Klappenecker and Roettler's construction of a solution to the Mean King's problem from a family of mutually unbiased bases

SUMMARY

What is the significance of this work?

- Completely syntactic proof of $\text{QKD} \Leftrightarrow \text{MUB}$ equivalence that uses only the logical structure

Also in the paper:

- Logical correctness proof of Klappenecker and Roettler's construction of a solution to the Mean King's problem from a family of mutually unbiased bases

Future directions:

- Application to other quantum protocols
- Nonstandard, 'classical' models

SUMMARY

What is the significance of this work?

- Completely syntactic proof of $\text{QKD} \Leftrightarrow \text{MUB}$ equivalence that uses only the logical structure

Also in the paper:

- Logical correctness proof of Klappenecker and Roettler's construction of a solution to the Mean King's problem from a family of mutually unbiased bases

Future directions:

- Application to other quantum protocols
- Nonstandard, 'classical' models

Thank you!