A novel notation for quantum cryptography

Applications to some recent quantum cryptographic protocols and their equivalences

Zef Wolffs
External Research Supervisor: Boris Škorić
Internal Thesis Advisor: Jacco de Vries

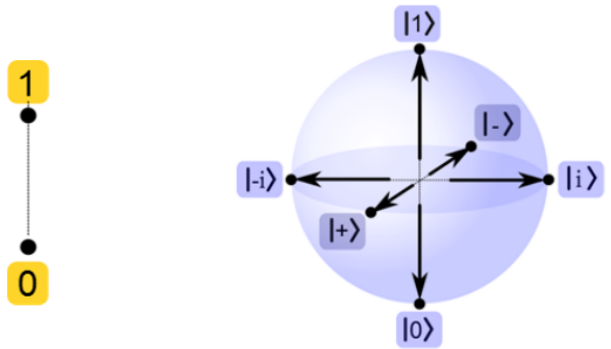
January 12, 2020

Outline

Introduction

Quantum Information

- The classical bit vs. the qubit

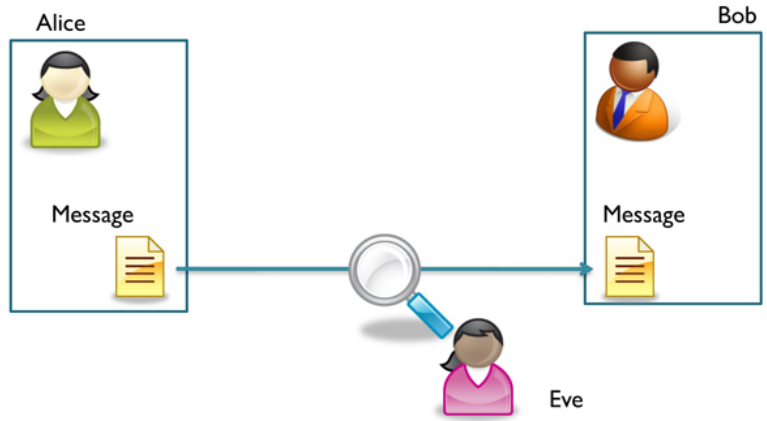


Representation of a classical bit (Left) and a qubit (right) [5].

- Encoding and decoding

Quantum Cryptography

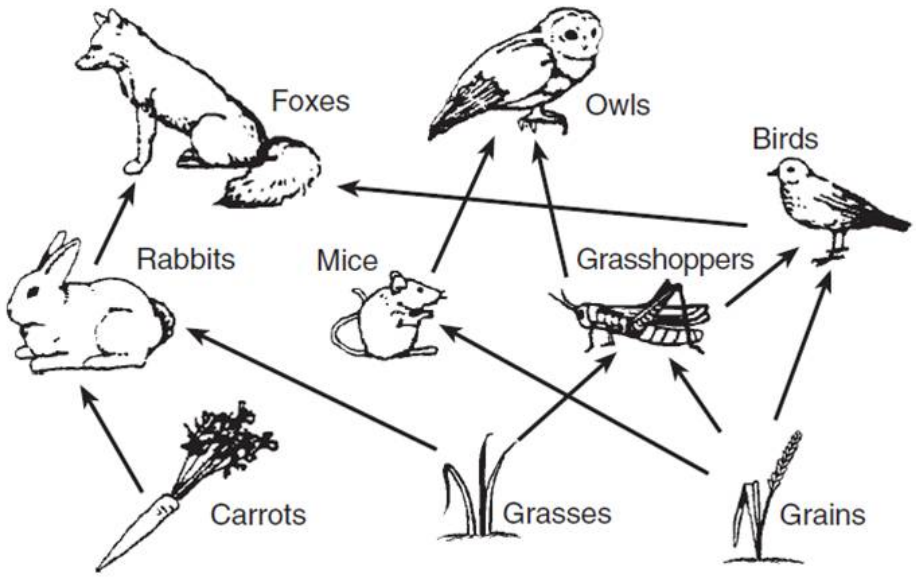
- Quantum cryptographic protocols: Sending a message securely using quantum mechanics



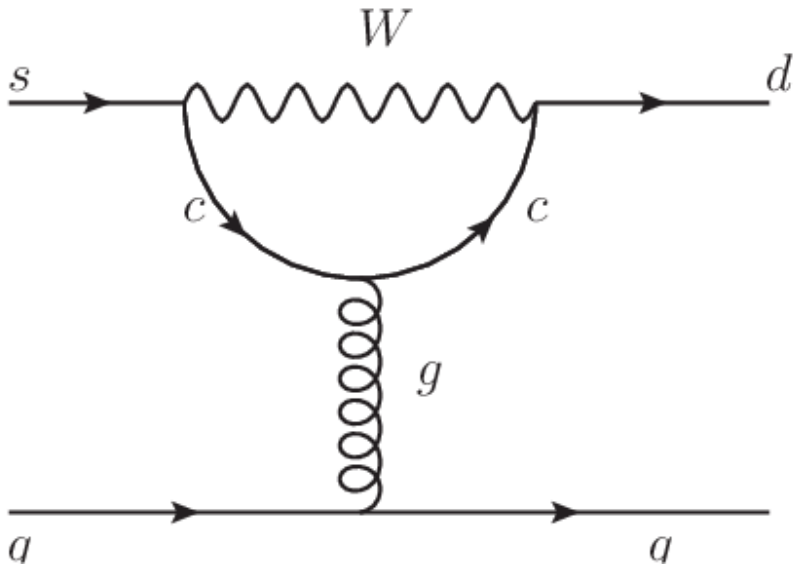
Alice, Bob, and Eve's roles in (quantum) cryptographic protocols [2].

- Dirac notation is not very intuitive

The Diagrammatic Notation



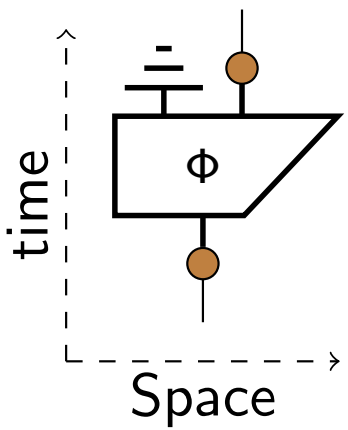
Diagrams in ecology: food webs [3].



Diagrams in particle physics: Feynman diagrams [6].

The Dagrammatic Notation

- Proposed by Coecke and Kissinger in 2017, in *Picturing Quantum Processes* [1].



The Aim

- Taking into account the rising popularity of quantum cryptography and the fact that its current notation is insufficient for describing it intuitively we want to give the diagrammatic method a place in the field of quantum cryptography by...

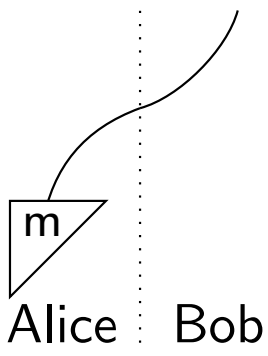
  1. Writing a short handbook-style introduction to this notation for physicists reluctant to read the entire book *Picturing Quantum Processes [1].*

  2. Constructing some recent quantum cryptographic developments and protocols in this new notation.

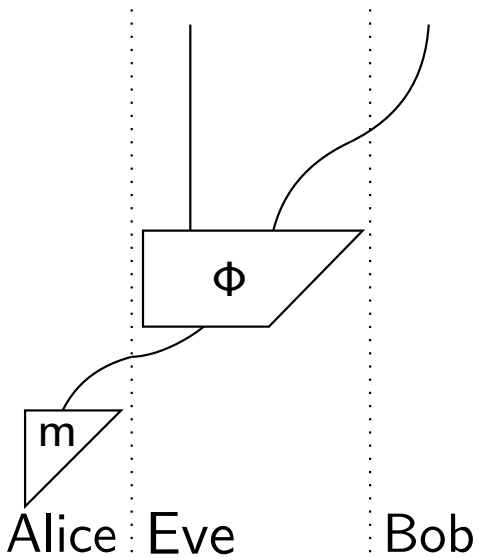
The Classical One Time Pad

The Classical One Time Pad

Ideal situation:



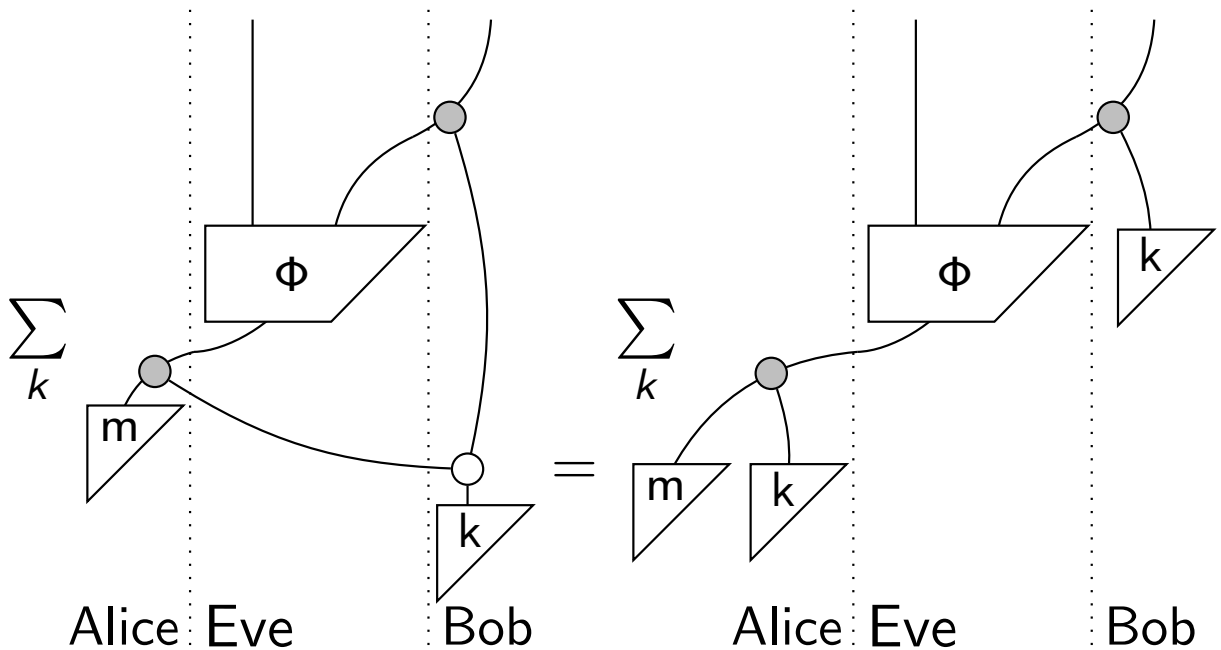
Real situation:



(1)

The Classical One Time Pad

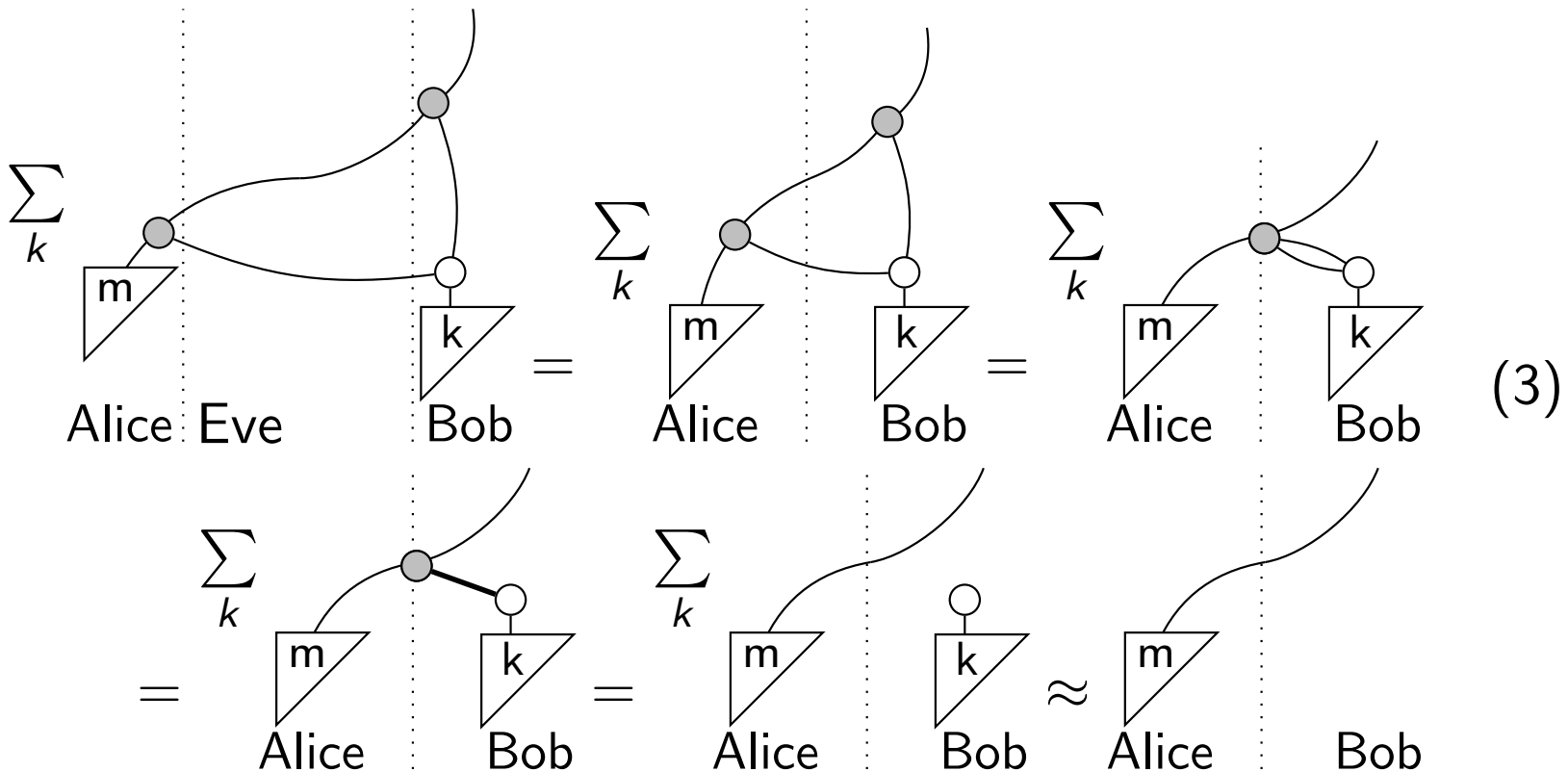
- The One Time Pad solution: xor with secret random variable k



(2)

The Classical One Time Pad

- If Eve does not interfere, communication should be provably correct.

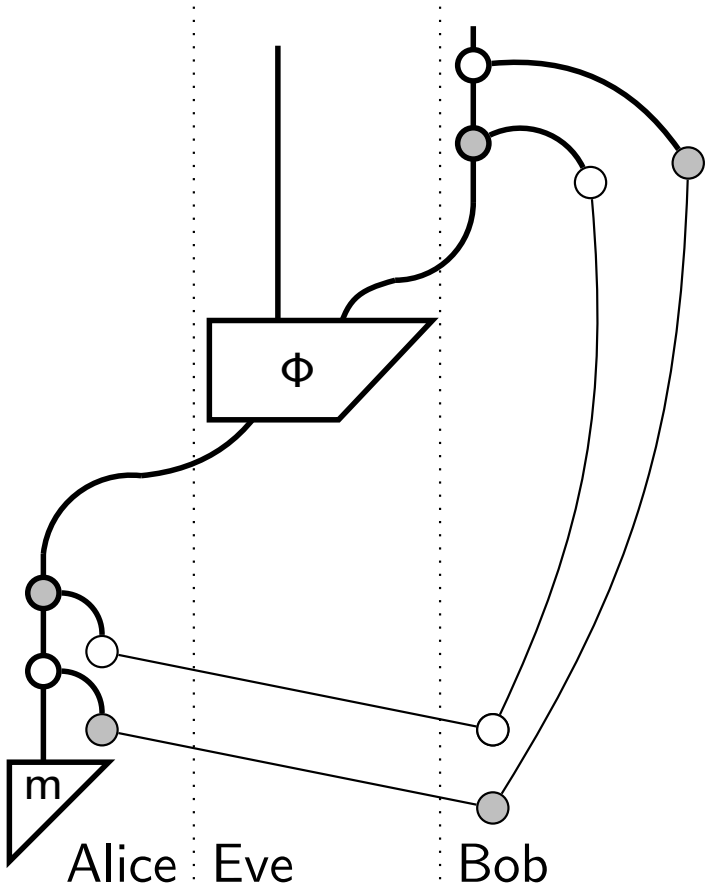


The Quantum One Time Pad

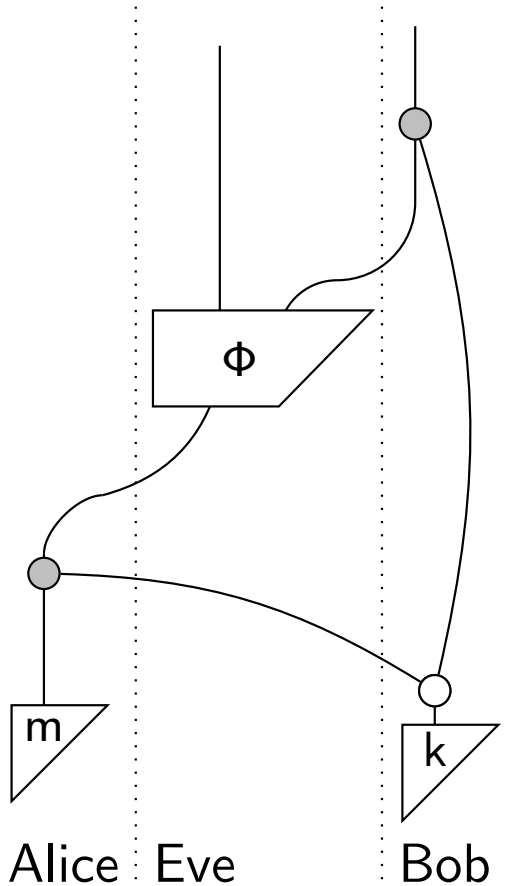
The Quantum One Time Pad

The Quantum One Time Pad

The Quantum One Time Pad



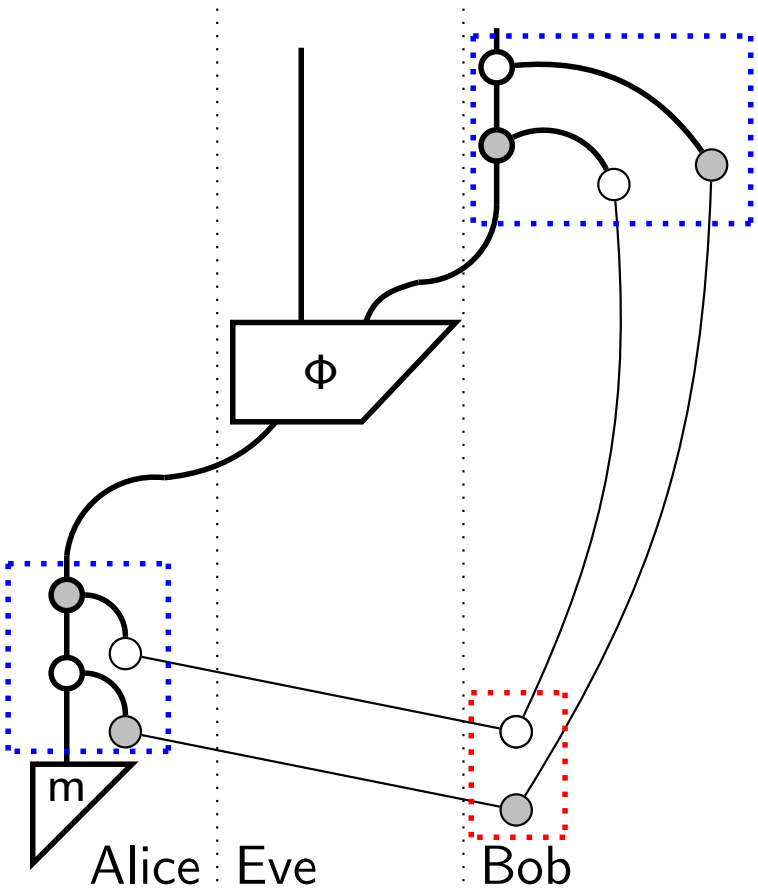
The Classical One Time Pad



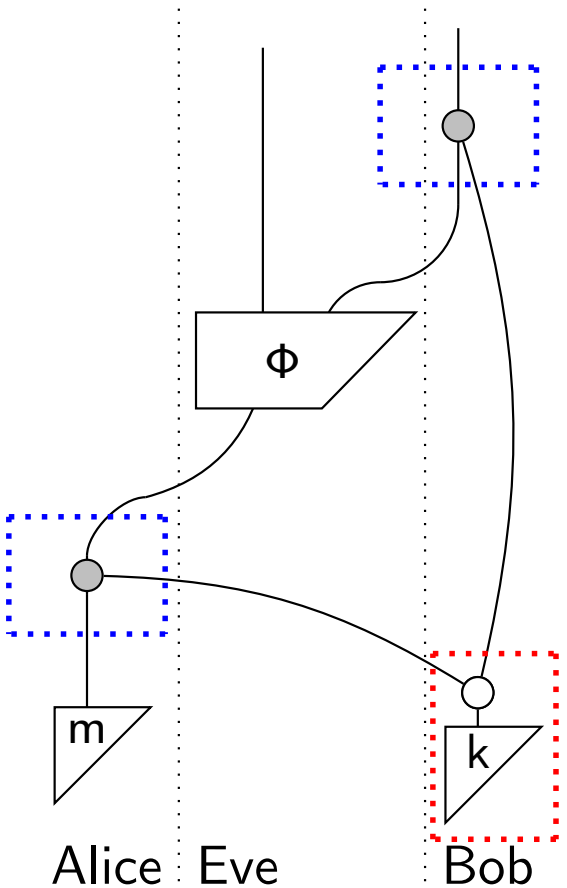
(4)

The Quantum One Time Pad

The Quantum One Time Pad



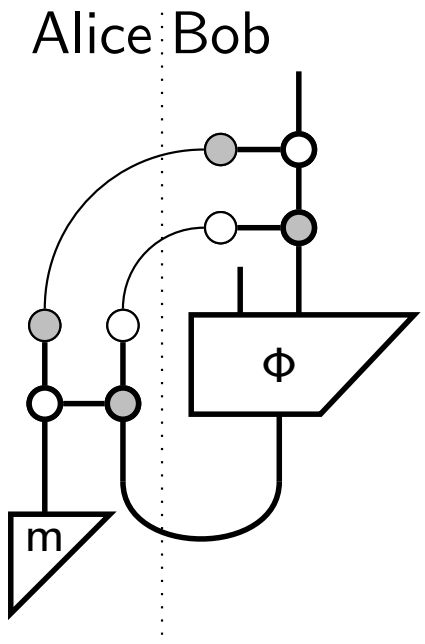
The Classical One Time Pad



(5)

Quantum Teleportation and Quantum One Time Pad Equivalence

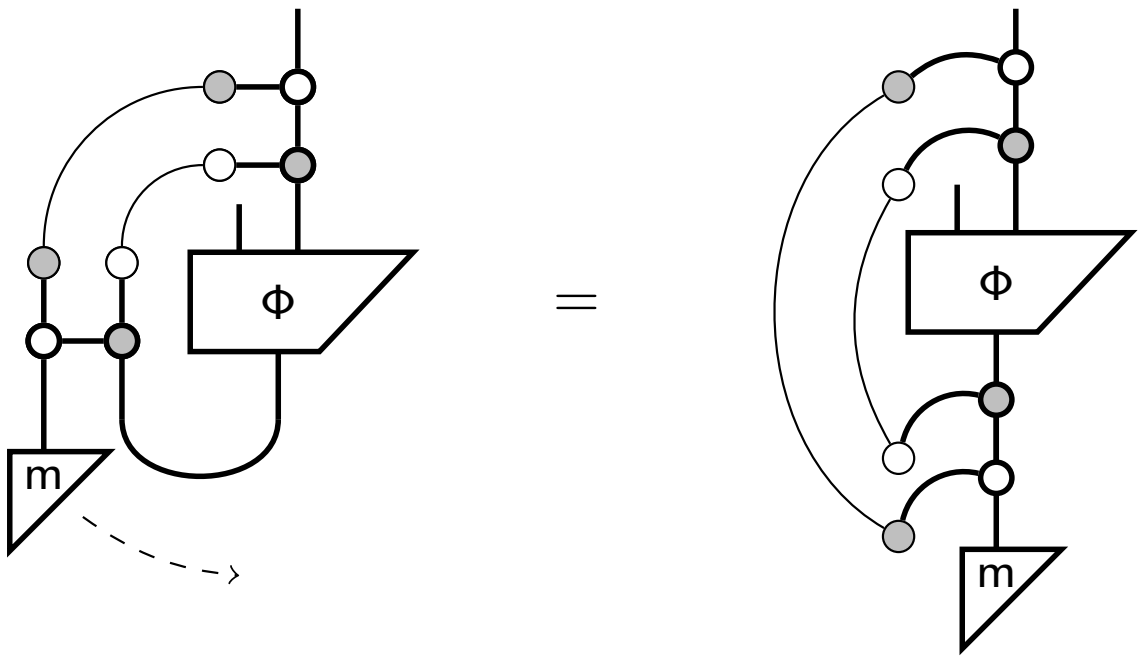
Quantum Teleportation



(6)

Quantum Teleportation and Quantum One Time Pad Equivalence

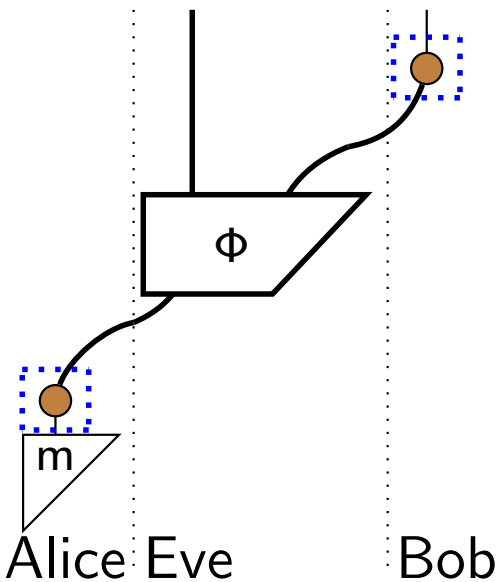
Quantum Teleportation = The Quantum One Time Pad



(7)

Quantum Key Recycling

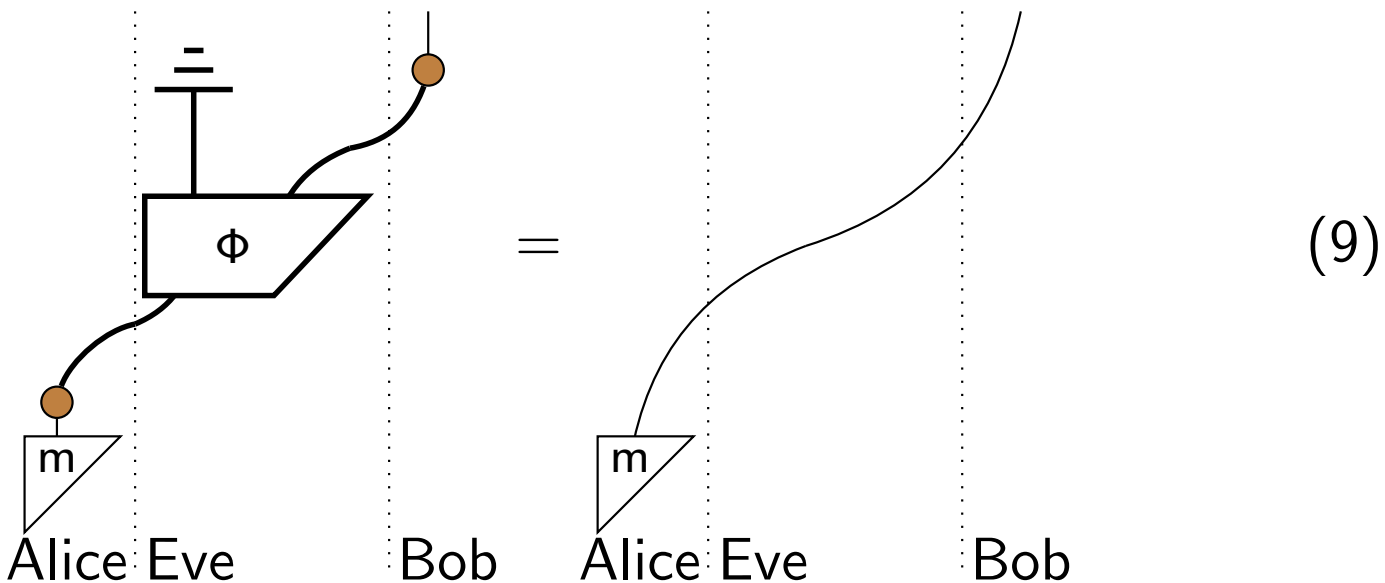
Quantum Key Recycling



(8)

Quantum Key Recycling

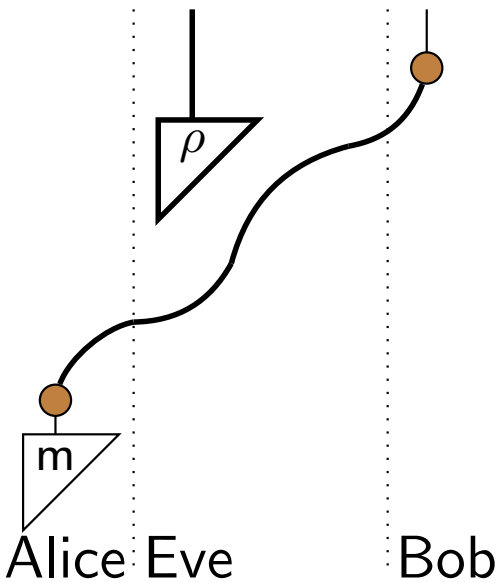
- Security proof for quantum key recycling in the noiseless case, the starting point:



(9)

Quantum Key Recycling

- With a lot of steps in between, the end result becomes:



(10)

- In words: Eve's part of the diagram separates entirely from Alice and Bob's communication channel!

Discussion and Conclusions

Discussion and Conclusions

- What novel things did we achieve in this thesis?

Discussion and Conclusions

- What novel things did we achieve in this thesis?
  - Wrote the first short **handbook-style introduction** to the diagrammatic notation

Discussion and Conclusions

- What novel things did we achieve in this thesis?
  - Wrote the first short **handbook-style introduction** to the diagrammatic notation
  - Developed the **classical One Time Pad** diagrammatically and showed that it both works and is secure

Discussion and Conclusions

- What novel things did we achieve in this thesis?
  - Wrote the first short **handbook-style introduction** to the diagrammatic notation
  - Developed the **classical One Time Pad** diagrammatically and showed that it both works and is secure
  - Developed the **quantum One Time Pad** diagrammatically and showed that it both works and is secure

Discussion and Conclusions

- What novel things did we achieve in this thesis?
  - Wrote the first short **handbook-style introduction** to the diagrammatic notation
  - Developed the **classical One Time Pad** diagrammatically and showed that it both works and is secure
  - Developed the **quantum One Time Pad** diagrammatically and showed that it both works and is secure
  - Showed that **Quantum Teleportation** is equivalent to the quantum One Time Pad, and therefore also works and is secure

Discussion and Conclusions

- What novel things did we achieve in this thesis?
  - Wrote the first short **handbook-style introduction** to the diagrammatic notation
  - Developed the **classical One Time Pad** diagrammatically and showed that it both works and is secure
  - Developed the **quantum One Time Pad** diagrammatically and showed that it both works and is secure
  - Showed that **Quantum Teleportation** is equivalent to the quantum One Time Pad, and therefore also works and is secure
  - Developed **Quantum Key Recycling** diagrammatically, included a fully fledged security proof and worked out equivalences from a recent paper [4]

Discussion and Conclusions

- Did this achieve the aims?

Discussion and Conclusions

- Did this achieve the aims?
  1. Writing a short handbook-style introduction to this notation for physicists hesitant to read the entire book *Picturing Quantum Processes [1].*

Discussion and Conclusions

- Did this achieve the aims?
  1. Writing a short handbook-style introduction to this notation for physicists hesitant to read the entire book *Picturing Quantum Processes [1].*
     Maybe, up to the reader to decide.

Discussion and Conclusions

- Did this achieve the aims?
  1. Writing a short handbook-style introduction to this notation for physicists hesitant to read the entire book *Picturing Quantum Processes [1].*
     Maybe, up to the reader to decide.

  2. Constructing some recent quantum cryptographic developments and protocols in this new notation.

Discussion and Conclusions

- Did this achieve the aims?
  1. Writing a short handbook-style introduction to this notation for physicists hesitant to read the entire book *Picturing Quantum Processes [1].*
     Maybe, up to the reader to decide.

  2. Constructing some recent quantum cryptographic developments and protocols in this new notation.
     Yes!

Discussion and Conclusions

- Role of diagrammatic notation?
- More technical: classical channels have a basis?

(11)

Discussion and Conclusions

- In future research it would be interesting to...
  - Develop a full security proof for Quantum Key Recycling with noise
  - Generally work out more protocols and equivalences in this notation

Questions?

References

[1] Bob Coecke and Aleks Kissinger.
Picturing Quantum Processes.
Cambridge University Press, Cambridge, 2017.

[2] Mathieu Cunche.
À l'attaque des codes secrets.
Interstices.info, 2011.

[3] Randi Glaser.
Food Web Examples.
Blendspace.com, n.d.

[4] Daan Leermakers and Boris Škorić.
Quantum Alice and Silent Bob.
https://eprint.iacr.org/2019/875, 2019.

[5] Krysztof Pomorski, Panagiotis Giounanlis, Elena Blokhina, and Robert Staszewski.
From Quantum Hardware to Quantum AI.
University College Dublin, Dublin, 2018.

[6] Kimberley Vos, H. Wilschut, and R. Timmermans.
Limits on lorentz violation in neutral-kaon decay.
Proceedings of the Sixth Meeting on CPT and Lorentz Symmetry, 2013.