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

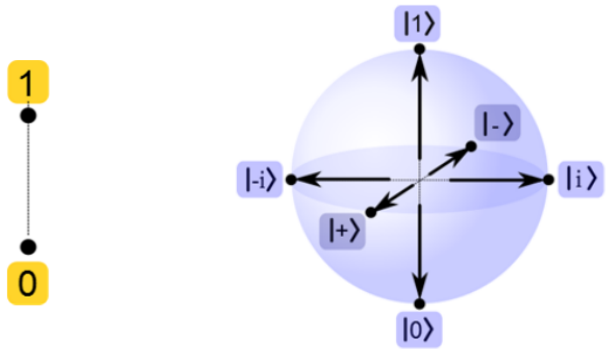
January 11, 2020

Outline

Introduction

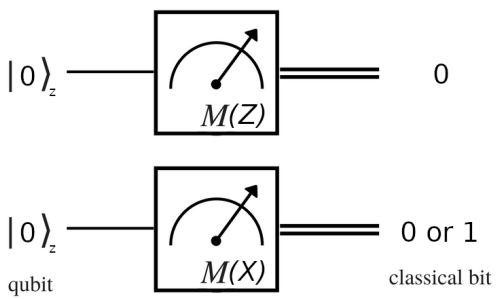
Quantum Information

- The classical bit vs. the qubit



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

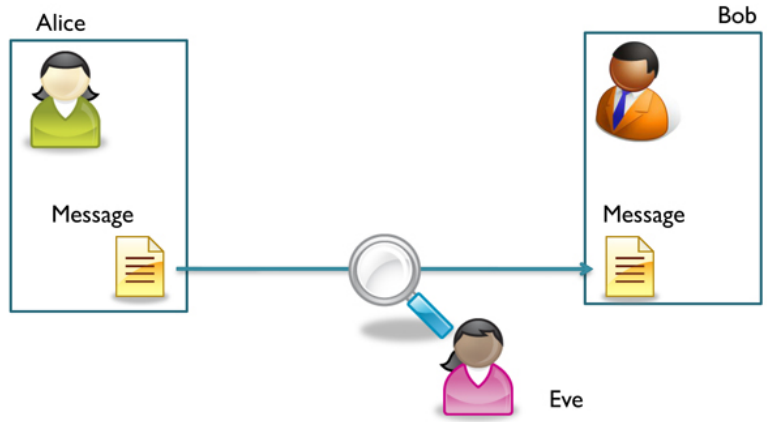
- Mutual unbiasedness



Measuring $|0\rangle_z$ in the Z and X bases [4].

Quantum Cryptography

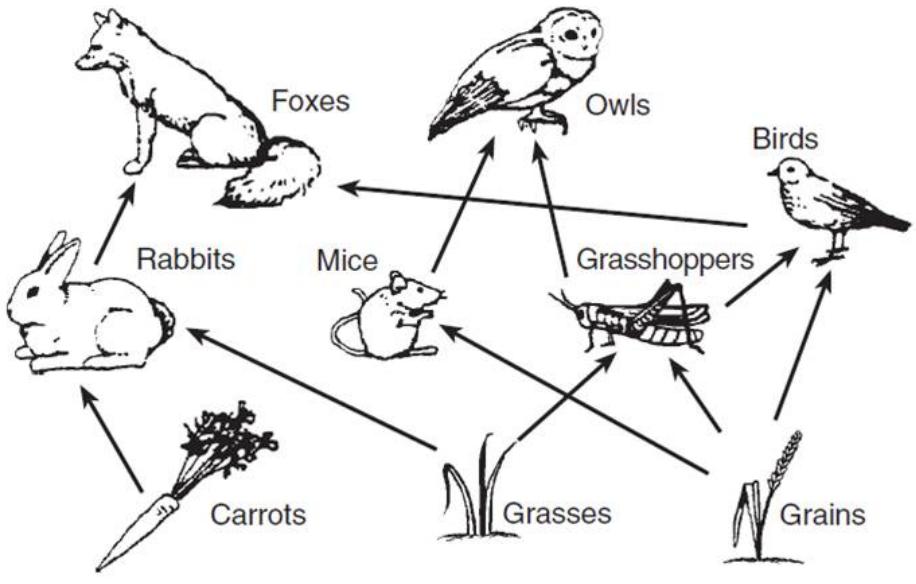
- Quantum cryptographic protocols: Sending a message securely using quantum mechanics



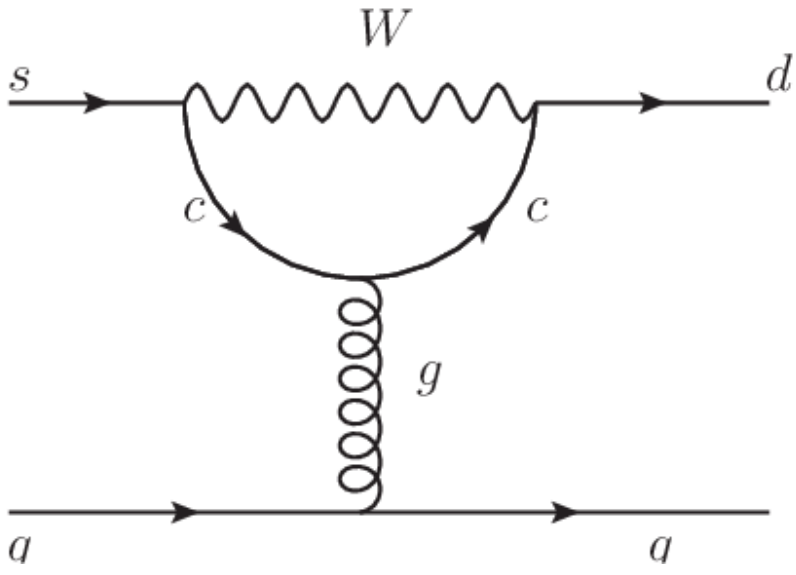
Alice, Bob, and Eve's roles in (quantum) cryptographic protocols [2].

- Dirac notation is not very intuitive

The Diagrammatic Notation



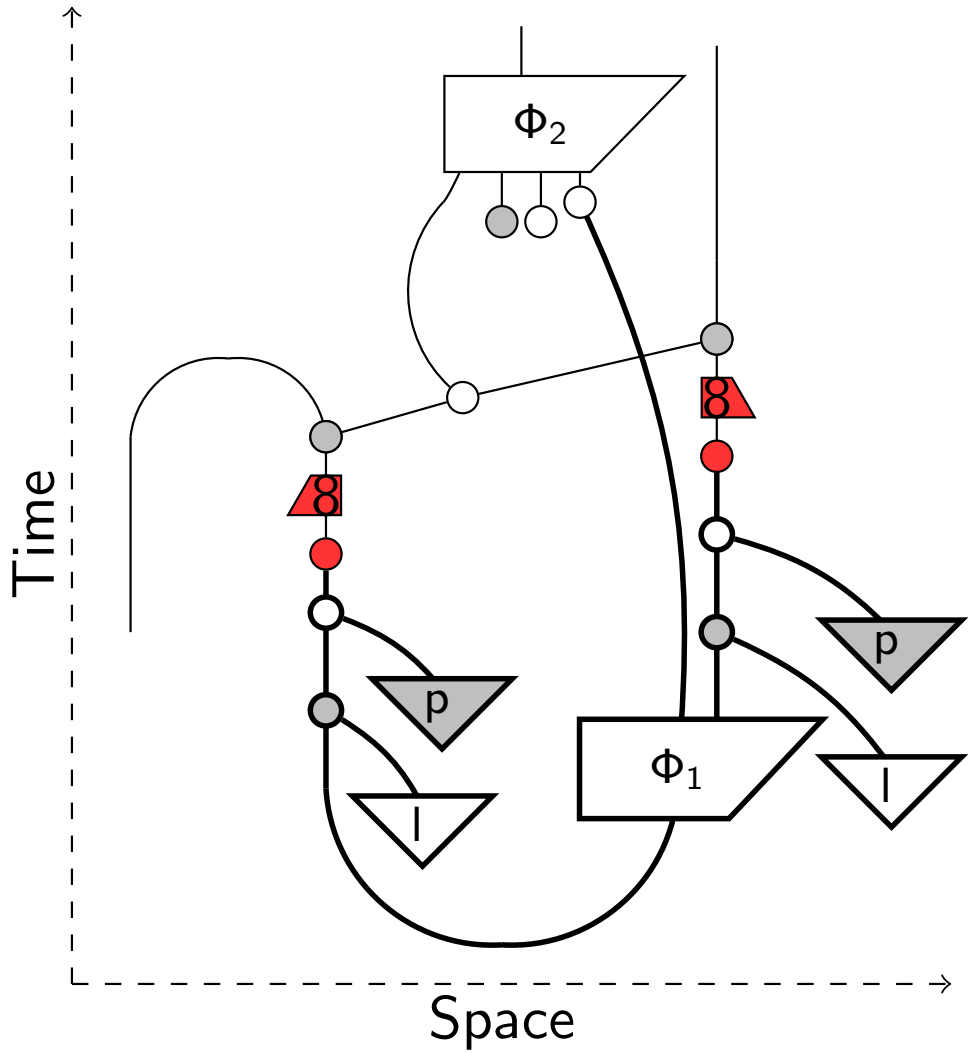
Diagrams in ecology: food webs [3].



Diagrams in particle physics: Feynman diagrams [6].

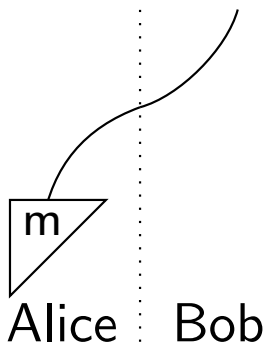
The Dagrammatic Notation

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

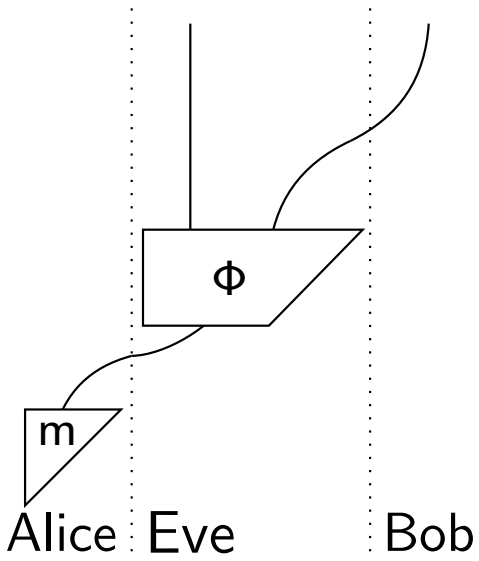


The Classical One Time Pad

Ideal situation:



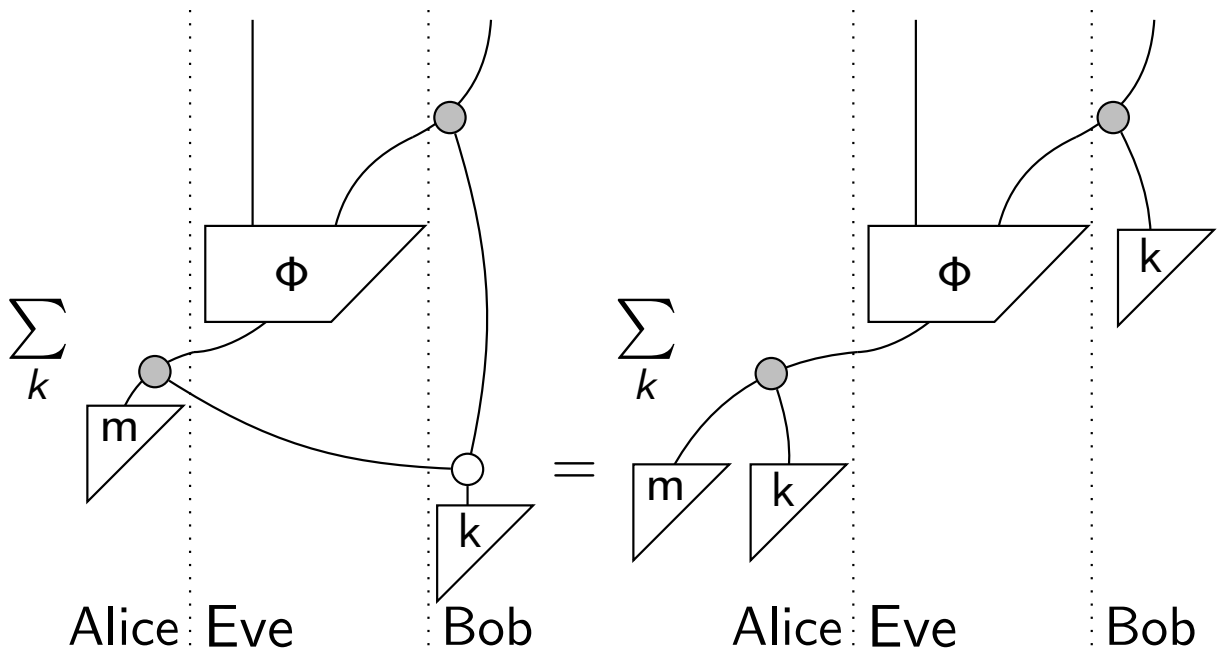
Real situation:



(1)

The Classical One Time Pad

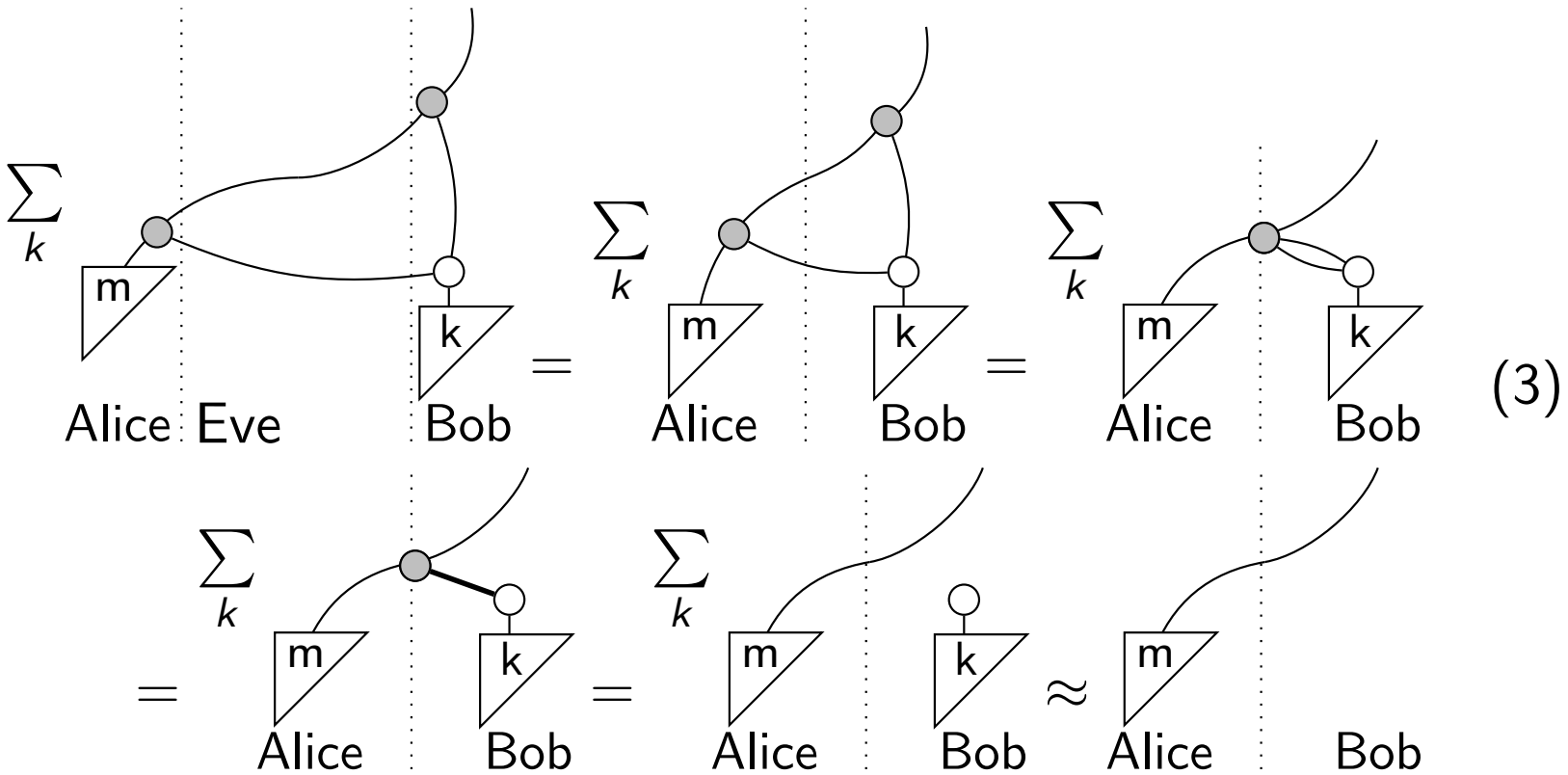
- The OTP solution: xor with secret random variable k



(2)

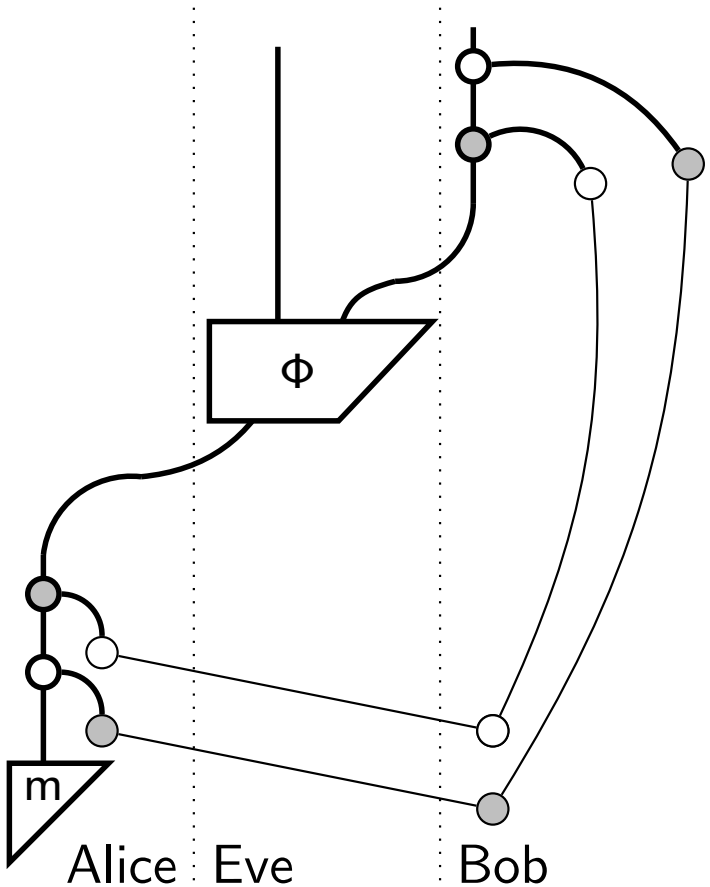
The Classical One Time Pad

- If Eve does not interfere, can Alice and Bob still communicate?

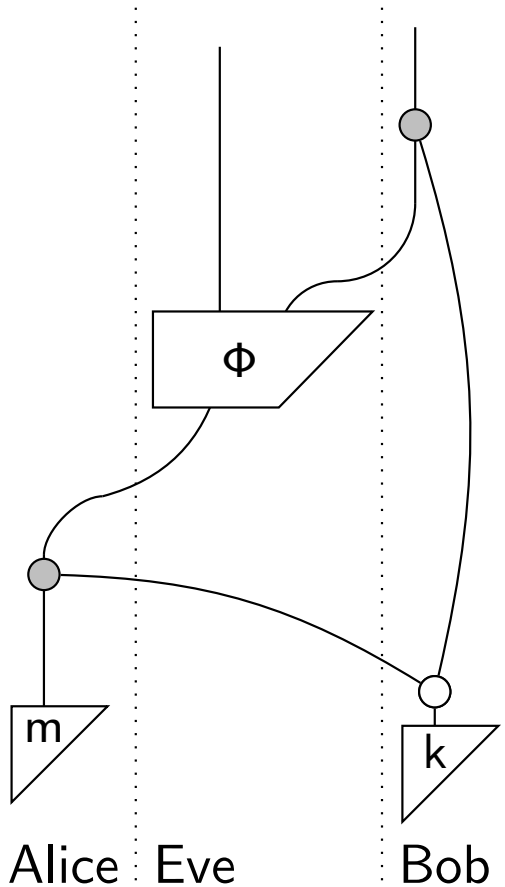


The Quantum One Time Pad

The Quantum One Time Pad



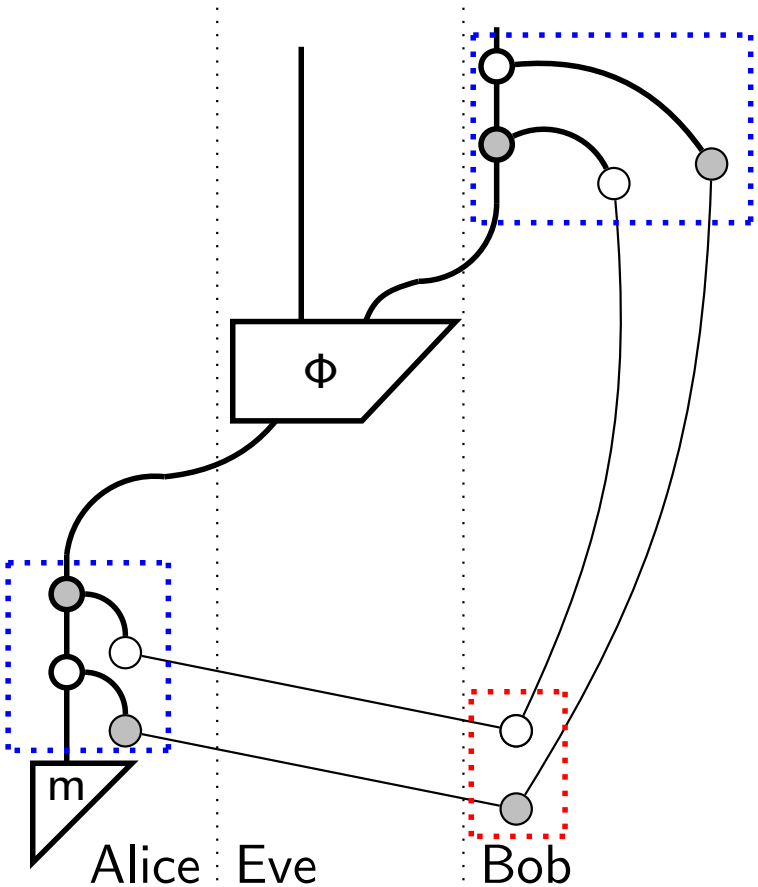
The Classical One Time Pad



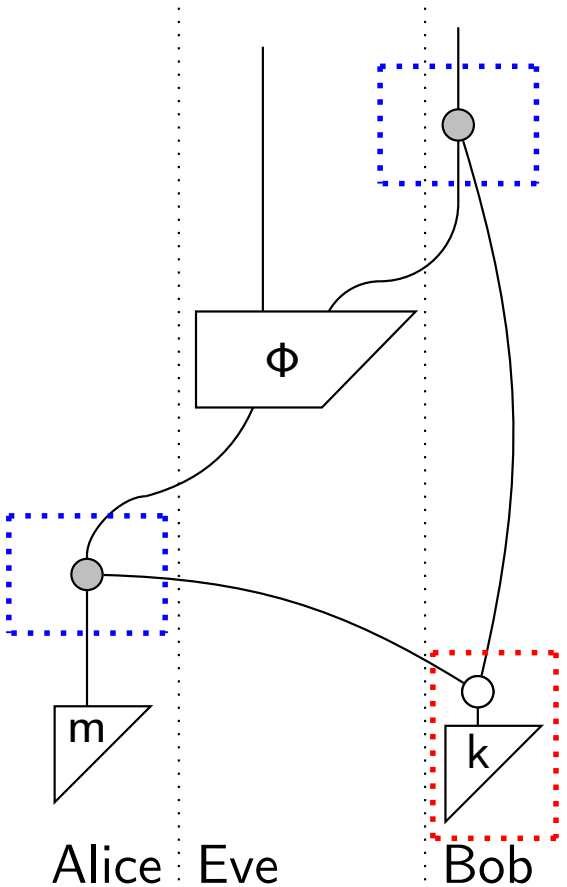
(4)

The Quantum One Time Pad

The Quantum One Time Pad

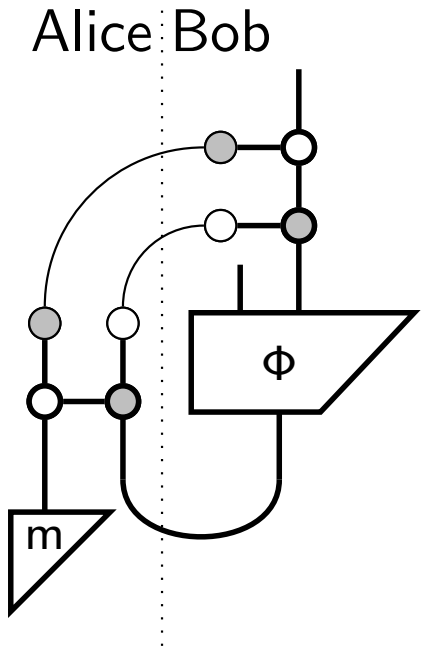


The Classical One Time Pad



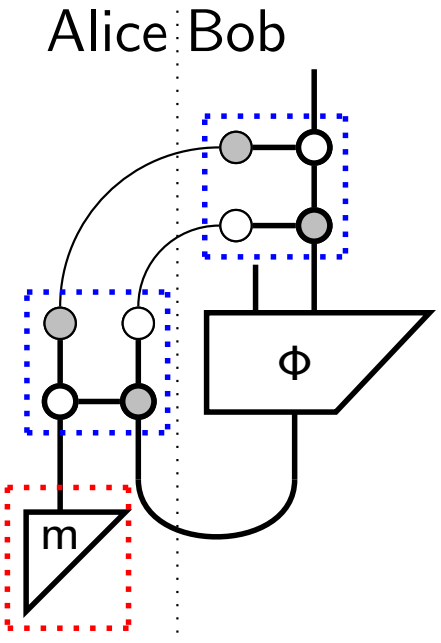
(5)

Equivalence: Quantum Teleportation



(6)

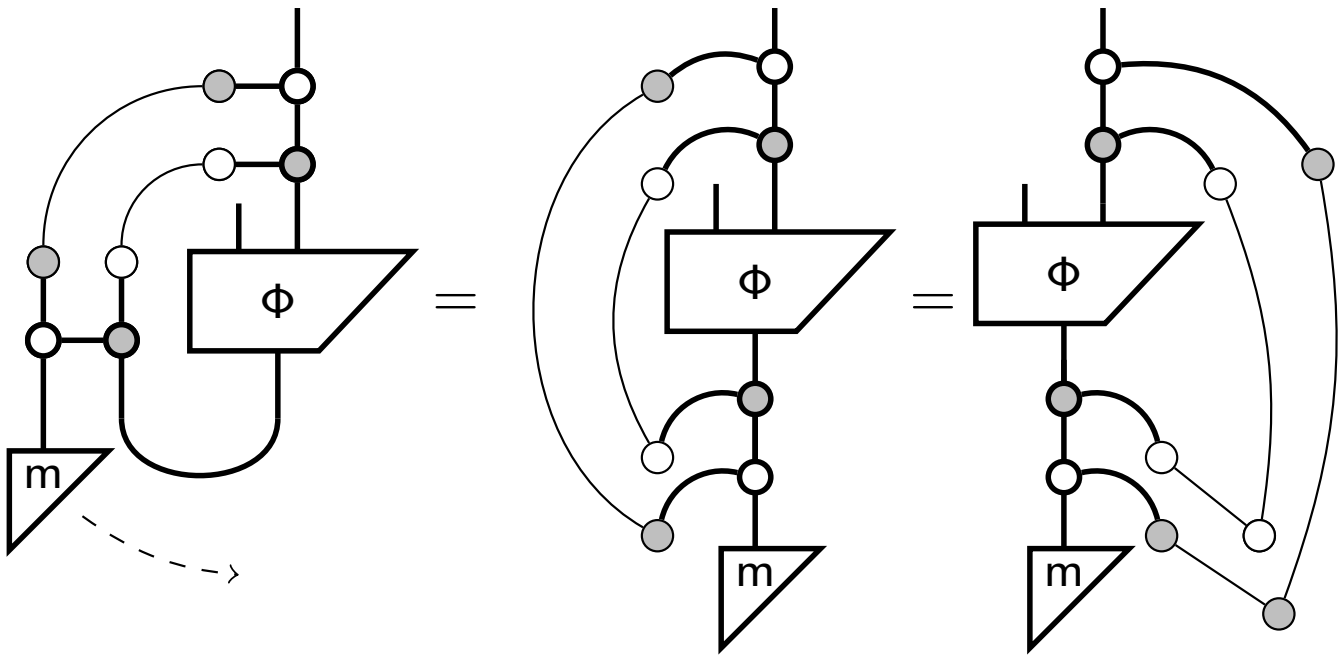
Equivalence: Quantum Teleportation



(7)

Equivalence: Quantum Teleportation

Quantum Teleportation = The Quantum One Time Pad = (8)



Quantum Key Recycling

Discussion

References


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


Mathieu Cunche.
À l'attaque des codes secrets.
Interstices, 2011.


Randi Glaser.
Food Web Examples.
Blendspace.


Nimish Mishra.
Understanding the Basics of Quantum Computation.
Towards Data Science, 2019.


Krysztof Pomorski, Panagiotis Giounanlis, Elena Blokhina, and Robert Staszewski.