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

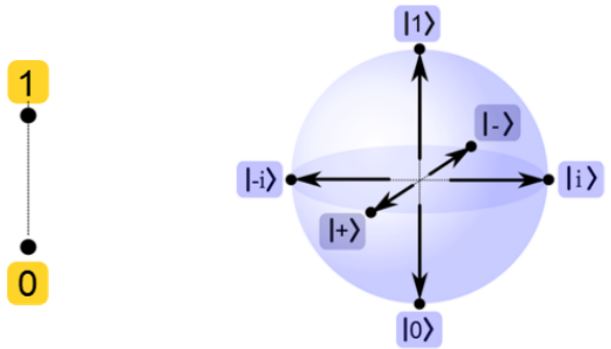
January 9, 2020

Outline

Introduction

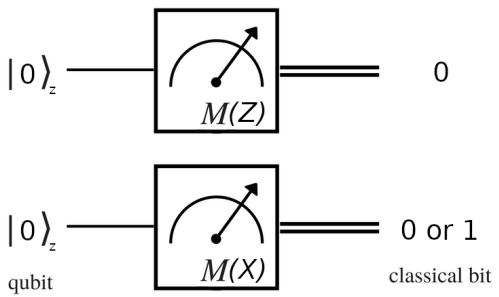
Quantum Information

- The classical bit vs. the qubit



Representation of a classical bit (Left) and a qubit (right) [4].

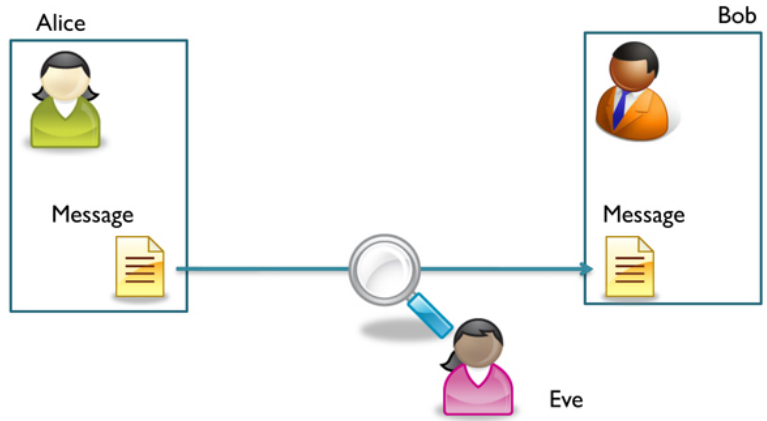
- Mutual unbiasedness



Measuring $|0\rangle_z$ in the Z and X bases [3].

Quantum Cryptography

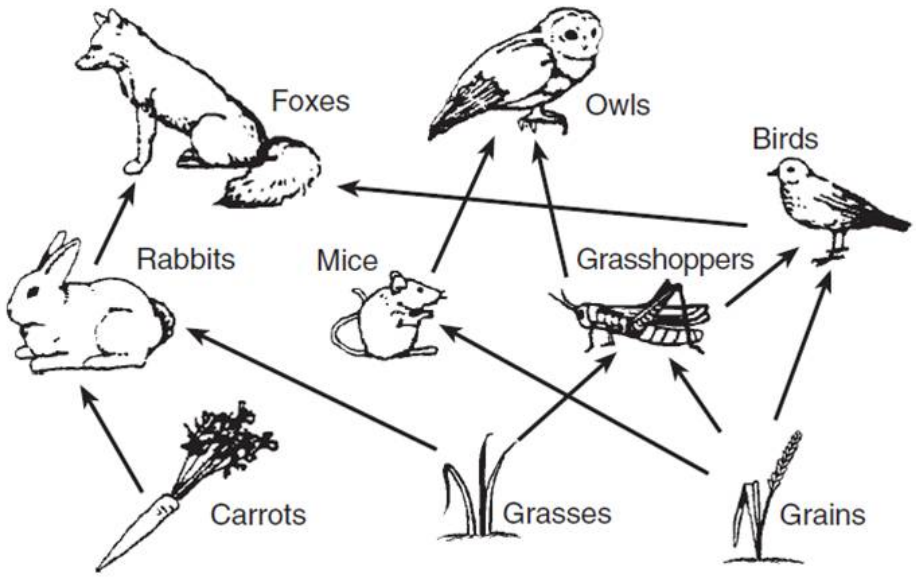
- Quantum cryptographic protocols: Sending a message securely using quantum mechanics



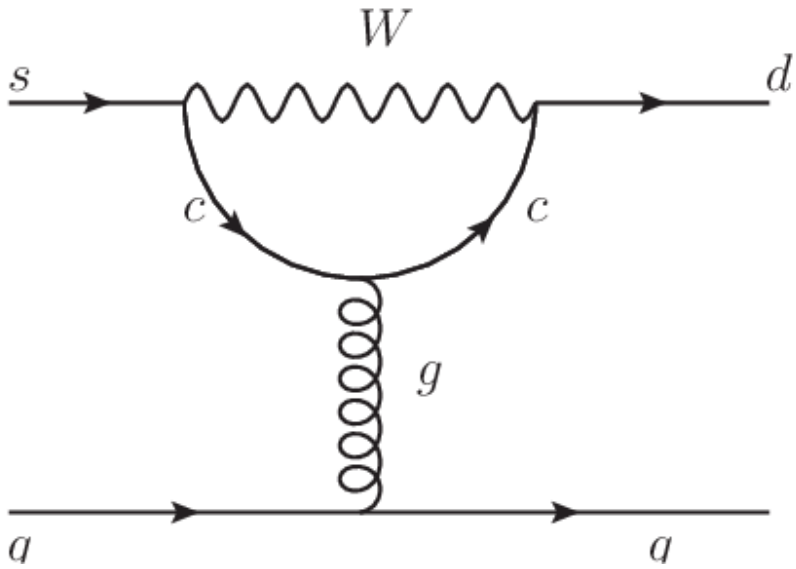
Alice, Bob, and Eve's roles in (quantum) cryptographic protocols [1].

- Dirac notation is not very intuitive

The Diagrammatic Notation



Diagrams in ecology: food webs [2].



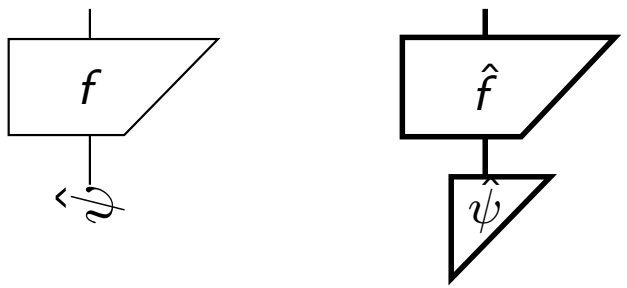
Diagrams in particle physics: Feynman diagrams [5].

The Diagrammatic Notation

- Preparing a **classical bit** ψ and **qubit** $\hat{\psi}$:

(1)

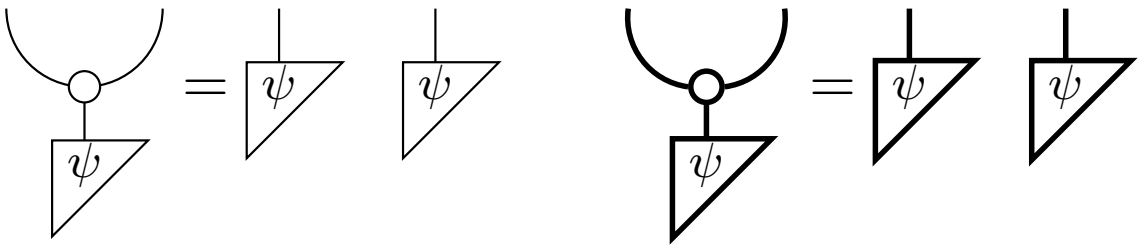
- Applying a **classical map** f and **quantum map** $\hat{f}$ to these states respectively:



(2)

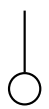
The Diagrammatic Notation

- **Spiders** copy states.



(3)

- Whenever they have no input they create a random bit.



(4)

The Classical One Time Pad

References


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.
From Quantum Hardware to Quantum AI.
University College Dublin, 2018.


Kimberley Vos, H. Wilschut, and R. Timmermans.