CRIPTOGRAFIA CUANTICA

Iván Martínez
Daniel Alzate

INTRODUCCIÓN

La criptografía cuántica es un tipo de criptografía que utiliza los principios de la física cuántica para crear un mensaje indescifrable para todos menos para el receptor previsto.

La criptografía cuántica se conoce también por su distribución de claves cuánticas o QKD (por sus siglas en inglés).

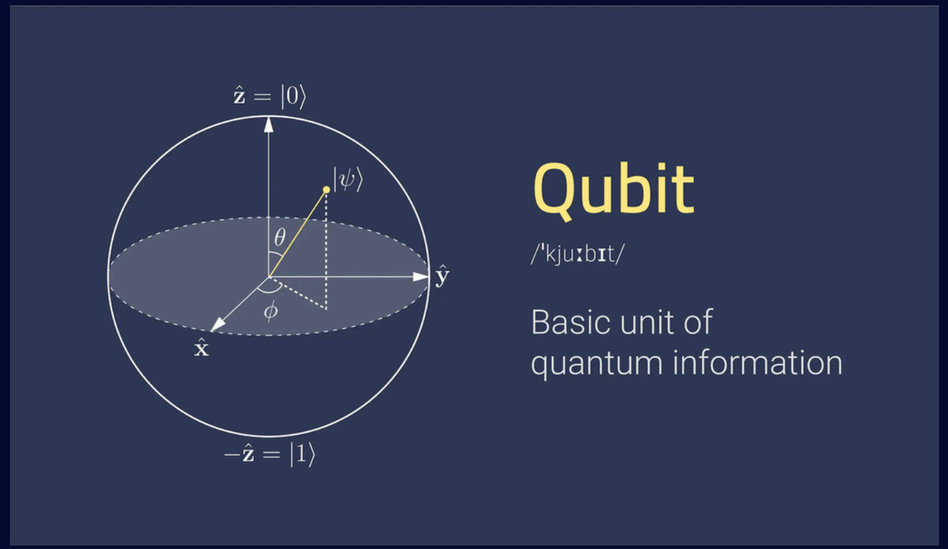
FUNDAMENTOS

- Superposición
- Entrelazamiento
- Qubits

QUBITS Y SUPERPOSICIÓN

La computación cuántica opera con qubits. El qubit es la unidad básica de la computación cuántica. Un qubit es un sistema mecánico-cuántico de dos estados.

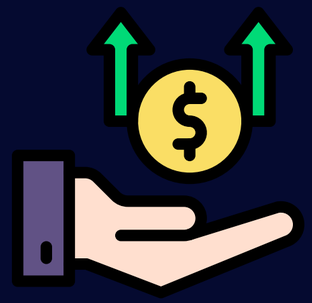
Las partículas cuánticas como los fotones pueden existir en múltiples estados a la vez, un principio conocido como superposición.



ENTRELAZAMIENTO CUÁNTICO

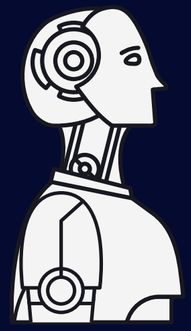
Fenómeno donde dos partículas se conectan de tal manera que el estado de una partícula instantáneamente afecta el estado de la otra, sin importar qué tan lejos estén una de la otra.

DESAFÍOS ACTUALES Y FUTUROS



Costo

Experiencia técnica



Infancia tecnológica

Intrusos

PROTOCOLO BB84

El protocolo BB84 fue propuesto por Charles Bennett y Gilles Brassard en 1984 y es uno de los primeros y más conocidos protocolos de criptografía cuántica. Su funcionamiento se basa en los principios de la mecánica cuántica, en particular en la incertidumbre cuántica y el entrelazamiento.

Bits Alice	0	1	0	1	1	0	0	0	1	1	0	1
Bases Alice	↕	⤨	⤨	↕	⤨	↕	⤨	↕	↕	⤨	↕	↕
Bases Bob	↕	↕	⤨	⤨	⤨	↕	↕	⤨	↕	↕	↕	⤨
Bits Bob	0	*1	0	*0	1	0	*1	*0	1	*1	0	*0
Chave secreta	0		0		1	0			1		0	

GRACIAS

REFERENCIAS

- Jozef Gruska. “Quantum Computing”. Mc Grawl-Hill, UK, 1999. 439 páginas. ISBN: 0077095030
- https://www.gta.ufrj.br/grad/13_1/quantica/protocolos.html