Fondamenti della computazione quantistica e una sua applicazione nel campo della crittografia

Tesi di Laurea in

Ingegneria Informatica

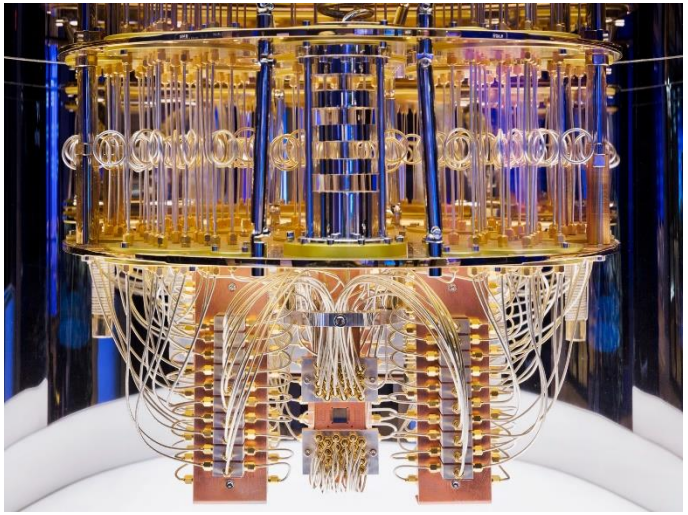
Candidato
Ilaria Salvetti

Relatori
Prof. Giuseppe Anastasi
Prof. Enzo Mingozzi
Prof. Luciano Lenzini

UNIVERSITÀ DI PISA

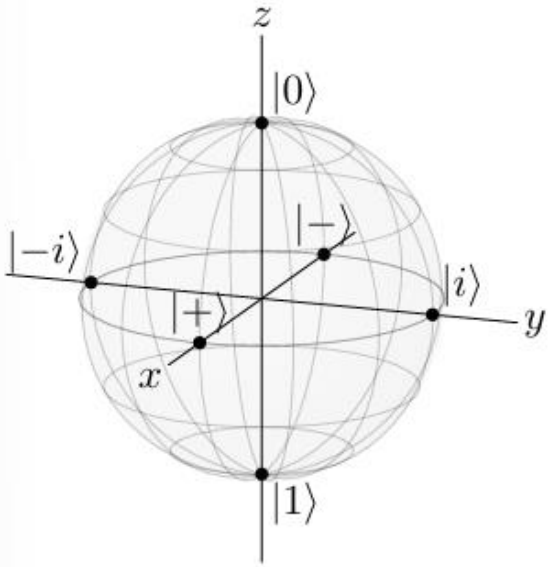
Introduzione

- La computazione quantistica è un paradigma computazionale basato sui principi della meccanica quantistica.
- La potenza dell'informatica quantistica risiede nella sua capacità di risolvere problemi considerati irrisolvibili con l'informatica classica.
- Tuttavia, sul piano pratico siamo ancora indietro con l'implementazione a causa della fragilità dei quibits che causa difficoltà nel mantenere il loro il loro stato quantistico.



Qubit

- I *qubits* stanno ai computer quantistici come i bit stanno ai computer classici.
- Sono la più piccola unità di calcolo elementare della computazione quantistica.
- Sono una combinazione di $|0\rangle$ e $|1\rangle$, chiamata *superposition*.
- Lo stato di un singolo qubit può essere visualizzato geometricamente come un punto della sfera di Bloch.

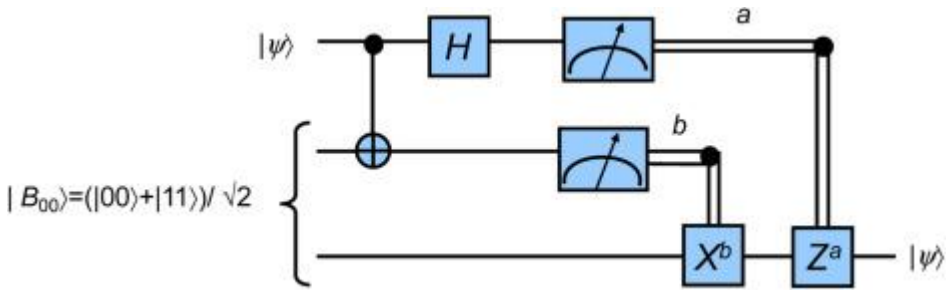


Entanglement

- Indica la caratteristica correlazione tra parti di un sistema quantistico.
- Secondo questo principio è possibile conoscere lo stato di un qubit misurando l'altro qubit, con il quale ha un vincolo.
- Nell'informatica la conseguenza è un'accelerazione dei processi di calcolo.
- Entangled qubits posso influenzarsi a vicenda più velocemente della velocità della luce.

Quantum Teleportation

- Tecnica per trasferire informazioni quantistiche da un punto A, a un punto B.
- Stati entangled vengono utilizzati per teletrasportare uno stato quantistico arbitrario.



- Questa tecnica è coerente con il Teorema di non-clonazione che afferma che non è possibile clonare uno stato quantistico sconosciuto.

BB84

- Metodo quantistico per stabilire una chiave segreta condivisa.
- *Alice* sceglie una sequenza casuale di 0 e 1 e per ognuno sceglie una base di misurazione, Z o X, non ortogonali tra loro. *Bob* riceve la sequenza e sceglie le basi in cui fare le misurazioni, a sua volta.
- Eve non può copiare perfettamente gli stati senza essere scoperta. La sicurezza del protocollo è garantita dalle leggi della fisica.
- La probabilità che Eve venga scoperta tende a 1 per un numero di bit che tende a infinito.