

Kvantedatamaskiner og kvantekommunikasjon

- Kvantedatamaskiner
- Kvantekryptering
- Teleportasjon

Nytt felt ~1990- med rask utvikling
Teori og eksperimentelle realiseringer

1

Kvantedatamaskiner - bakgrunn

Klassisk datamaskin

- Utvikling basert på stadig mindre kretselementer
- Må ha et stort antall atomer per kretselement for at maskinen skal være deterministisk og følge Maxwells lover

På enkeltatom-nivå gjelder Kvantemekanikk istedenfor Maxwell!

Derfor lager vi heller en

Kvantedatamaskin!

2

Representasjon av data

Klassisk datamaskin

Informasjon representert med *bits*: 1 og 0

Spenning / ikke-spenning

Lys / ikke-lys

Kvantedatamaskin

Informasjon representert med *qubits*: $|1\rangle$ og $|0\rangle$

Eks: Spinn opp / spinn ned for elektron

Vertikalt / horisontalt polarisert foton

Energitilstander for atom

Frekvens for foton

...

Død / levende katt

3

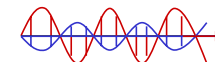
Kvantebit - qubit

En qubit $|\psi\rangle$ kan være i tilstandene $|0\rangle$ eller $|1\rangle$,
men også en *superposisjon* av $|0\rangle$ og $|1\rangle$:

$$|\psi\rangle = a |0\rangle + b |1\rangle, \text{ hvor } |a|^2 + |b|^2 = 1$$

Eks: Et fotons polarisasjon:

$$\begin{aligned} \mathbf{E} &= a E_x + b E_y \\ &= a \cdot \text{horisontal pol} + b \cdot \text{vertikal pol} \end{aligned}$$



4

Kvantemekaniske målinger

En qubit $|\psi\rangle$ er i tilstanden:

$$|\psi\rangle = a |0\rangle + b |1\rangle, \text{ hvor } |a|^2 + |b|^2 = 1$$

Vi måler $|\psi\rangle$ i basisene $|0\rangle$ og $|1\rangle$:

Resultat: $|0\rangle$ med sannsynlighet $|a|^2$

$|1\rangle$ med sannsynlighet $|b|^2$

Eks: Mål et foton's polarisasjon vha polarisator langs horisontalen og detektor



5

Multiple qubits

To qubit'er:

$$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle, \\ \text{ hvor } |a_{00}|^2 + |a_{01}|^2 + |a_{10}|^2 + |a_{11}|^2 = 1$$

Eks: Bell-tilstander:


$$|\psi\rangle = a |00\rangle + b |11\rangle$$

Fysisk:

To fotoner som er "sammenbundet" (entanglement):
Måler du den ene så kjenner du den andre

6

Logiske operasjoner

Klassisk: NOT: $0 \rightarrow 1$ og $1 \rightarrow 0$ 
AND, NAND, OR, NOR, XOR osv

Kvanteoperasjoner på en qubit:

$$|\psi\rangle = a |0\rangle + b |1\rangle \rightarrow |\psi\rangle = a' |0\rangle + b' |1\rangle$$

Beskrives av en unitær matrise \mathbf{U} :

$$\begin{bmatrix} a' \\ b' \end{bmatrix} = \begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \mathbf{U} \begin{bmatrix} a \\ b \end{bmatrix}$$

7

Eksempler på logiske operasjoner

X, "qu-not":

$$|\psi\rangle = a |0\rangle + b |1\rangle \rightarrow |\psi\rangle = a |1\rangle + b |0\rangle$$

Z:

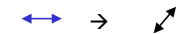
$$|\psi\rangle = a |0\rangle + b |1\rangle \rightarrow |\psi\rangle = a |0\rangle - b |1\rangle$$

H, "Hadamard", " $\sqrt{\text{not}}$ ":

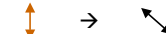
$$\begin{bmatrix} a' \\ b' \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}$$

Eks polarisasjonrotator:

$$|0\rangle \rightarrow (|0\rangle + |1\rangle)/\sqrt{2}$$



$$|1\rangle \rightarrow (|0\rangle - |1\rangle)/\sqrt{2}$$

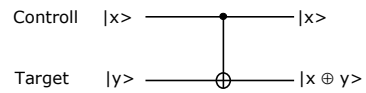


8

Multiple qubit-operasjoner

CNOT "controlled-not":

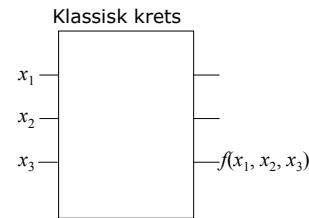
$|00\rangle \rightarrow |00\rangle$
 $|01\rangle \rightarrow |01\rangle$
 $|10\rangle \rightarrow |11\rangle$
 $|11\rangle \rightarrow |10\rangle$



Vanskelig å realisere med fotoner
fordi fotoner vekselvirker lite

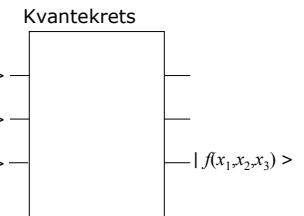
9

Hvorfor er kvantedatamaskiner så effektive?



Inngangene kan bare ha verdiene 0 eller 1:

Vi får bare informasjon om en funksjonsverdi av gangen



Inngangene kan være i en superposisjon av $|0\rangle$ og $|1\rangle$:

Kan få informasjon om en global egenskap av f ved kun en evaluering

10

Effektive algoritmer for kvantedatamaskiner

- Faktorisere store tall, knekke kryptering
- Søke i store datamengder
- Simulere kvantemekaniske systemer
- ...

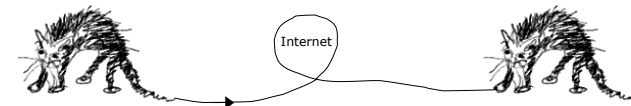
11

Teleportasjon

Er det mulig å overføre qubits fra A til B?

Alice's katt

Bob:

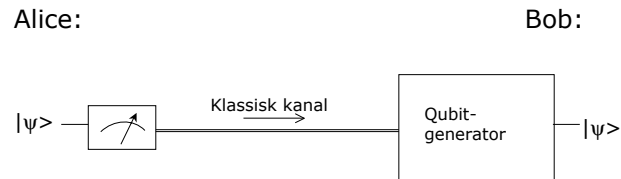


12

Teleportasjon

Problem: Overfør $|\psi\rangle = a|0\rangle + b|1\rangle$ fra Alice til Bob via en klassisk kanal.

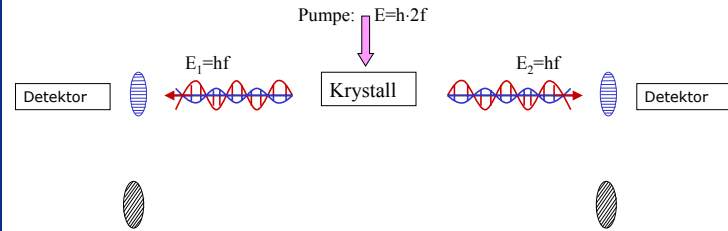
En metode som ikke fungerer:



13

Bell-tilstander (entangled states)

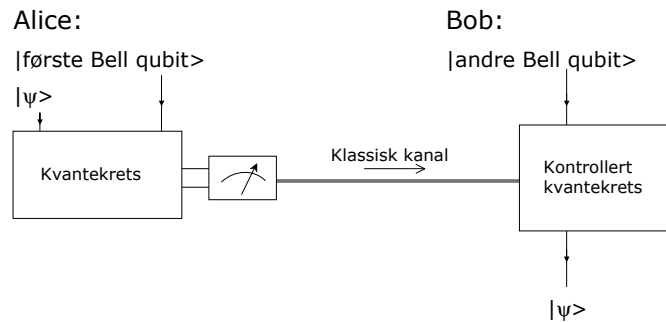
$$|\psi\rangle = 1/\sqrt{2} |00\rangle + 1/\sqrt{2} |11\rangle$$



14

Teleportasjon - metode

Må ha tilgjengelig: $|\text{Bell}\rangle = 1/\sqrt{2} |00\rangle + 1/\sqrt{2} |11\rangle$



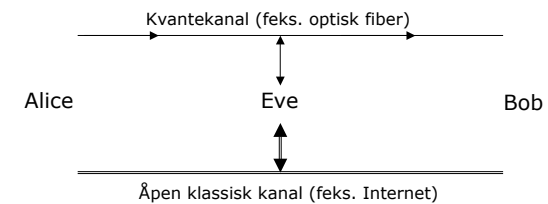
15

Kvantekryptering – sikker kommunikasjon

Sikker kommunikasjon forutsetter at Alice og Bob deler en hemmelig nøkkel (bitstreng)

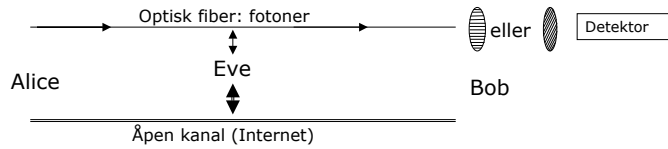
Hvordan overføre nøkkelen uten at noen kan fange den opp?

Overfør qubits som representerer nøkkelen



16

Kvantekryptering – prinsipp



1. Alice sender en sekvens av fotoner med 4 forskjellige polarisasjoner:
 $0^\circ, 45^\circ, 90^\circ, 135^\circ$ Eks: $0^\circ, 90^\circ, 135^\circ, 0^\circ, 45^\circ, 135^\circ, 45^\circ, 45^\circ$
0 1
2. Bob orienterer polarisatoren sin i en vilkårlig sekvens.
Eks:
Resultat: $45^\circ, 90^\circ, 0^\circ, 135^\circ, 45^\circ, 135^\circ, 90^\circ, 45^\circ$
3. Alice og Bob forteller hverandre åpent hvilke basis-sekvens de brukte
4. Der hvor basisene stemte overens bevarer Bob resultatet som deretter brukes som nøkkel: 1 0 1 0

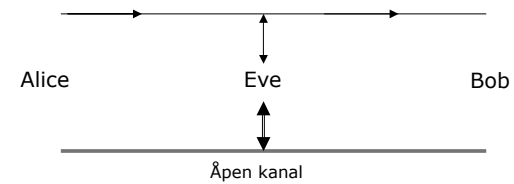
17

Kvantekryptering: Hva med avlytting?

Prinsipper fra kvantemekanikk:

- Måling forstyrrer!
- Kloning av kvantetilstander er generelt umulig!

Hvis Eve lytter, vil fotonene bli forstyrret, og Alice og Bob skjønner at de blir avlyttet



18