

## Simulerer framtidens datamaskin

11.jun 2007 05:00

Av: [Arnfinn Christensen](#) , Journalist

Eirik Ovrum har laget et dataprogram som simulerer en ny type datamaskiner - kvantedatamaskiner. Disse vil lynraskt kunne søke i enorme databaser, og brukes til å overføre hemmelige koder ved hjelp av såkalt kvante-sammenfiltrering over enorme avstander uten fysisk kontakt.

Ovrums dataprogram simulerer en kvantedatamaskin, og basert på andres forskning har han laget et dataprogram som trolig kan kjøres på en slik kvantedatamaskin - når den er ferdig utviklet.

Ennå er nemlig kvantedatamaskiner bare på forsøksstadiet. Når de blir virkelighet, vil de muligens kunne erstatte vanlige datamaskiner helt eller delvis og være mye mindre og mer effektive, i hvert fall til enkelte oppgaver.

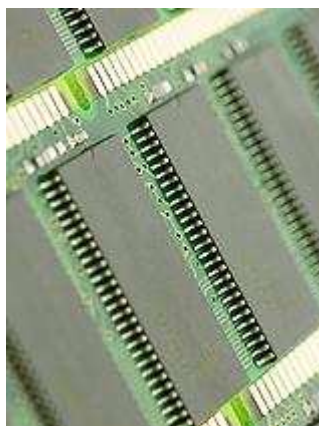
Det amerikanske militærvesenet er interessert i kvantedatamaskiner fordi de kan knuse fiendens hemmelige militære koder, og brukes til å lage nye og uknuselige koder.

Ovrums doktorgrad er en stein i det store internasjonale forskningsbyggverket som tar sikte på å utvikle denne typen datamaskiner. Det er få norske steiner i dette byggverket, så Ovrum er i en liten og eksklusiv faggruppe her i landet.

### Datateknologien møter veggen

En tradisjonell datamaskin består veldig forenklet av mange små elektriske brytere, kalt transistorer. Millioner av slike transistorer er montert sammen på databrikker og danner mikroprosessen som er hjernen i en PC.

Nå begynner Intel, Motorola og de andre produsentene av mikroprosessorer å nærme seg fysiske grenser for hva de kan få til. Problemet er at mikroprosessorene utvikler varme, som alt annet hvor det går elektrisk strøm. Jo mindre og raskere prosessorene blir, desto mer varme utvikles på mindre område, og det blir vanskelig å få god nok kjøling.



Tradisjonell datateknologi begynner å nærme seg en grense for hvor små og raske komponentene kan bli.

## En dimensjon mindre

En transistor i en tradisjonell mikroprosessor består av mange atomer og molekyler. I en kvantedatamaskin består hver minste del bare av ett elektron, et ladet atom eller en lyspartikkel - et foton.

Da blir hele datamaskinen en dimensjon mindre. Energiforbruket blir mye lavere, og de små avstandene gjør at hastigheten på beregningene kan økes.

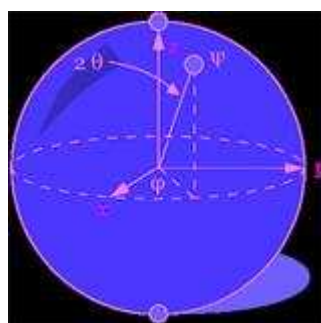
Den nye teknologien er mulig fordi elektroner og andre elementærpartikler - såkalte kvanter - oppfører seg annerledes enn transistorer. Dette er den store fordelen med kvantedatamaskiner, men også en stor utfordring.

Kvantedatamaskiner må nemlig konstrueres etter helt nye teoretiske prinsipper som gir store muligheter.

## En Qubit

- I en vanlig datamaskin består data av enere og nuller - såkalte "bits". I en kvantedatamaskin er bits erstattet av såkalte kvantebits eller "qubits", forteller Ovrum.

Et qubit kan for eksempel være et elektron, der tallet "en" betyr at elektronet spinner i en retning, mens tallet "null" betyr at elektronet spinner i en annen retning.



En teoretisk modell av en qubit.

Et lyskvant eller foton kan på sin side ha ulike polarisasjoner, for eksempel vannrett for en og loddrett for null. Polarisering av lys utnyttes blant annet i solbriller som fjerner ubehagelige reflekser av sollys med en bestemt polarisering.

Problemet er at qubits ikke lar seg avlese uten videre. Skal du bestemme spinnretningen på ett bestemt elektron, så mister du informasjonen. Den eneste måten du kan finne ut av spinnretningen på, er ved å ha mange like kopier og så finne gjennomsnittet av mange målinger.

Slik sett er kvantedatamaskiner basert på sannsynlighetsberegninger.

## Teleportering

Drømmen om å kunne trylle seg fra ett sted til et annet med øyeblikkelig virkning har sitt gjensvar i kvantepartiklenes underlige verden. Riktignok kan ikke en og samme partikkel forflytte seg, men to partikler på vidt forskjellige steder kan ha felles egenskaper. Dette kalles kvante-sammenfiltring.

For milliarder av år siden ble universet skapt og all materie var samlet på et lite område. Hvis to partikler oppstod på samme sted den gangen som et sammenfiltret par, men seinere ble spredd til hvert sitt hjørne av universet, beholder de likevel sammenfiltreringen.



Partikler som en gang har blitt sammenfiltret, vil speile hverandres egenskaper momentant over store avstander.  
(Foto:CERN)

Det betyr at hvis spinnet forandres på ett elektron i en annen galakse mange millioner lysår unna, vil et sammenfiltret elektron på jorda forandre spinnet momentant og tilsvarende, enda lyset bruker millioner av år fra galaksen til oss.

- Men dette betyr ikke at informasjon kan overføres raskere enn lyshastigheten, understreker Ovrum.

### Parallell overføring

For å kunne dekode informasjonen i qubitene, må vi nemlig sende nødvendig tilleggsinformasjon på den vanlige måten, for eksempel som radiobølger. Og de går med lysets hastighet.

- Likevel kan kvante-teleportering brukes til å overføre informasjon som er særegen for kvantesystemer, for eksempel hemmelige kodede meldinger som ikke kan avlyttes underveis, forteller Ovrum.

Det er allerede gjort eksperimenter med slik kvantekryptering hvor man bruker sammenfiltrede fotoner over en strekning på 144 kilometer på Kanariøyene, og snart skal det forsøkes teleportering til og fra en satellitt.

### Nytt verktøy for partikkelfysikere

- Kvantedatamaskiner er bedre på noen oppgaver enn andre, forteller Ovrum.

Det de er aller best til, er å simulere hva som skjer inne i og mellom atomene - kvantemekanikk. Forskerne på det europeiske senteret for partikkelfysikk CERN i Geneve i dag har rom fulle av datamaskiner for å få regnekraft nok til å analysere data som kommer fra partikkelakselleratorene.



Kvantedatamaskiner søker raskt gjennom mange tallkombinasjoner.

I framtida kan kanskje et slikt rom fullt av tradisjonelle datamaskiner erstattes med en kvantedatamaskin. Kvantedatamaskinen kan gjøre beregningene mye enklere fordi den ligner på systemene den skal simulere.

### Analoge systemer

Det blir som når rillen i en gammeldags LP-plate får stiftet til å vibrere i takt med lydsvingningene og lager lyden direkte. Det trengs ingen utregninger. Det

som skjer i rillen og i høyttalerne er analoge eller tilsvarende fenomener.

Slik vil kvantedatamaskinen være analog eller tilsvarende kvantepartiklene den skal simulere. Den slipper å "oversette" fra kvantespråk til vanlig datamaskinkode.

### Kodeknekker

- Kvantedatamaskinen vil også kunne brukes til å knekke koder og den typen elektroniske sikkerhetsnøkler som er mest utbredt i dag, for eksempel i nettbanker, forteller Ovrum.

Slike nøkler er basert på at både avsender og mottaker kjenner ett hemmelig primtall - et tall som bare er delelig med seg selv og en.

Når de så utveksler et annet primtall, ganges dette med nøkkel-primtallet, og mottakeren kan enkelt forklart dividere seg tilbake til det primtallet som oversendes.

Kvantedatamaskiner kan mye raskere enn vanlige datamaskiner finne fram til den hemmelige tallnøkkelen og knekke koden. Er det snakk om store tall, kan forbedringsfaktoren være tusen eller millioner ganger.

Men Ovrum tror ikke dette betyr slutten for datasikkerhet for de fleste av oss.

- Kvantedatamaskinene vil muliggjøre kvantekryptografi, en helt ny form for kryptering eller sikker koding av data. Kvantekryptografi kan overføre hemmelige kodenøkler i form av lyspartikler i optiske fibere, sier Eirik Ovrum.

### Framtidas datamaskiner?

De første spinkle prototypene på kvantedatamaskiner er i ferd med å se dagens lys, forteller Ovrum.

Ved å bruke en magnetresonans-maskin av samme type som legene undersøker pasienter med på sykehus, har forskerne klart å simulere et lite kvantesystem på fem atomer i et molekyl.

Men det er ennå lenge igjen til vi kan få kjøpt et innstikkskort til PC-en med en kvantedatamaskin.

- I dag kan ikke en kvantedatamaskin erstatte en vanlig datamaskin til generell databehandling, sier Ovrum.

Kvantedatamaskinen vil ha sine spesielle bruksområder, men Ovrum utelukker ikke at bruksområdene i framtida kan bli utvidet.

- Uansett må kvantedatamaskinen ha hjelp av en tradisjonell datamaskin for å virke, sier Ovrum. Dermed vil vi neppe noensinne gjøre kvantespranget fullt ut til neste generasjon datamaskiner. Det er mer snakk om en samkjøring av tradisjonell og ny datateknologi, understreker Ovrum.



Kvantedatamaskiner vil trolig samkjøres med tradisjonell datateknologi

**Referanse:**

Entanglement and Quantum Simulators (Eirik Ovrum,  
University of Oslo, 2007)