Kvantecomputeren er stadig en drøm

Kvantecomputeren er stadig en drøm, men der sker hele tiden teknologiske fremskridt som bringer drømmen tættere på at blive realiseret.
Anvendelsen af kvantemekanik til beregning åbner nogle ret fantastiske perspektiver, men på grund af kvantemekanikkens sandsynligheds teoretiske karakter er der brug for helt ny algoritmer.
En af de algoritmer der for alvor satte gang i forskningen omkring kvanteteoretiske algoritmer var Peter Schorr's opdagelse af en kvanteteoretisk algoritme til at finde primfaktorer.
Problemet med at finde primfaktorerne i et tal har længe været betragtet som et problem hvor beregningstiden vokser eksponentielt med størrelsen af tallet og det er derfor i praksis umuligt at finde en algoritme der på en almindelig komputer kan løse problemet indenfor en rimelig tid.
Schorr's algoritme viser at på en kvantecomputer kan dette problem løses i det der hedder polynomial tid hvilket vil sige at på en kvantecomputer kan man faktisk faktorisere tal i primfaktorer indenfor rimelig tid, et par år i stedet for flere milliarder år.
Da vanskeligheden ved at faktorisere store tal er en af grundstenene i moderne krypteringsmetoder vil kvantecomputeren have en stor effekt på problemerne omkring data sikkerhed.
I foredraget vil jeg beskrive strukturen af en kvantecomputer som man i dag forestiller sig den og beskrive de matematiske aspekter af Schorr's algoritme.

Niels O. Nygaard