Quantum Information Protocols with Gaussian States of Light

Quantum Information Protocols with Gaussian States of Light eller på dansk, Kvanteinformationsprotokoller med Gaussiske lystilstande er den mundrette titel på min afhandling skrevet på Institut for Fysik ved Danmarks Tekniske Universitet. Titlen giver et praj om hvad afhandlingen handler om, hvis man kan afkode hvad den betyder, så det virker som et naturligt sted at starte. Ordet kvant kommer af kvantum, som igen kommer fra det latinske quantus der betyder "hvor stort". Det refererer til den berømte (og berygtede) kvantemekanik som beskæftiger sig med opførslen af universets mindste bestanddele. I min afhandling er kvantemekanik vigtigt fordi lys består af lyspartikler eller lyskvanter, og især bruger jeg Gaussiske lystilstande som er en speciel form for laserlys. En protokol er et fint ord for en samling af instrukser lidt ligesom en algoritme fra computerverdenen. Disse instrukser skal udføres i en bestemt rækkefølge for at opnå et ønsket resultat. En kvanteinformationsprotokol er derfor en samling af instrukser der overfører kvanter fra et sted til et andet og disse kvanter indeholder information. I denne afhandling siger disse instrukser derfor noget om hvad man skal gøre ved lyskvanterne inden man sender dem fra A til B.

Anvendelser

Det er selvfølgelig alt sammen meget fint, men hvad kan det bruges til? Kvanteinformatik er en lovende forskningsdisciplin der på sigt kommer til at føre til banebrydende computere og principielt ubrydelig sikkerhed. De banebrydende computere er de såkaldte kvantecomputere, som vil være i stand til at simulere kvantemekaniske systemer hurtigere og bedre end før. Det vil blandt andet gøre det muligt at simulere effekten af nye former for medicin helt ned på det molekylære niveau. Den ubrydelige sikkerhed vil kunne bruges til at sikre bankoverførsler og anden følsom information meget bedre end vi er i stand til i dag. Min forskning har primært beskæftiget sig med at udvikle protokoller der bruger de kvantemekaniske egenskaber af laserlys til at kryptere information. Vi har udført et eksperiment der viser hvordan man i princippet kan opsætte en sikker netværksstruktur i en storby, og et mere kompliceret eksperiment der viser at man kan kryptere trafik mellem en klient og en kvantecomputer. Det næste skridt er at implementere disse teknikker i et større netværk, f.eks. Københavnsområdet, hvor der i en vis udstrækning allerede er adgang til optiske ledninger, som er nødvendige siden teknologien er lysbaseret.

EU er i øjeblikket i gang med at lancere en større forskningspulje på 1 milliard Euro netop inden for kvanteinformatik, og satser stort på at disse teknologier skal blive klar til kommerciel brug indenfor de næste to årtier til gavn for samfundet. Den eksperimentelle del af kvanteinformatikken er teknologisk meget udfordrende, og benytter sig af teknikker fra konventionel optisk kommunikation, signalbehandling og elektronik. Ligeledes er der også behov for teknikker fra den klassiske fysik i den forstand at det er meget vigtigt at de eksperimentielle opstillinger holdes under konstante temperaturer og dæmpning af mekaniske vibrationer fra omverdenen. At sikre stabiliteten af opstillingerne så de virker hver gang man tænder dem er i øjeblikket den største udfordring i forhold til at bringe disse teknologier til markedet.

Det historiske perspektiv

Grundstenen i moderne kryptering, RSA algoritmen, blev opfundet i midt 70'erne, af Rivest, Shamir og Adleman. Den var en revolutionerende opdagelse, der fik en stor flok matematikere interesserede i kryptering og dermed bidrog til feltets udvidelse, samtidig med at den gjor-

de det muligt at udnytte computere, som på det tidspunkt var i hastig udvikling, til effektiv kryptering. 40 år senere er algoritmen stadig i brug, blandt andet til Dankort-overførsler. RSA algoritmen og dens afarter er så dybt integrerede i det moderne informationssamfund at et brud på sikkerheden af den ville have katastrofale konsekvenser, ikke bare for finanssektoren, men også for alt fra regeringer til privatpersoner. Det kan derfor godt give lidt sved på panden når man bliver klar over at det ikke kan bevises at RSA rent faktisk virker. Det eneste der kan siges er, at hvis der er en måde at bryde den på, så er det ikke almen viden. Uden at virke alt for paranoid kunne man godt forestille sig at USA's National Security Agency havde en metode til at bryde RSA algoritmens sikkerhed som de ikke vil dele med offentligheden. Kvantekryptering som beskrevet i min afhandling løser dette problem endegyldigt.

I 1984 opdagede Charles Bennett og Gilles Brassard en metode til at udveksle hemmelige nøgler med beviselig sikkerhed. De forestillede sig to personer der ønskede at kommunikere. For at dele en hemmelig nøgle mellem hinanden brugte de 4 forskellige slags lyspartikler. Lyspartiklerne opfører sig som kvantemekaniske objekter og er derfor meget skrøbelige overfor påvirkninger udefra. Hvis en aflytter skulle forsøge at opsnappe lyspartiklerne mens de er på vej fra en person A, kaldet Alice, til en person B, kaldet Bob, ville aflytteren være nødt til at kopiere dem så der stadig ankommer kopier af partiklerne til B. Det er dog en meget fundamental egenskab ved kvantemekaniske objekter at de ikke kan kopieres, og på den måde sikrer kvantemekanikken sikkerheden af systemet.

Kvantekryptering er dog ikke uden sine problemer, og der har siden den første opdagelse været intens forskning på området. Der har blandt andet været såkaldte feltdemonstrationer i både Tokyo og Schweiz, hvor teknologien blev brugt til at sikre et kommunalvalg. Kina har i øjeblikket ambitioner om at sammensætte et krypteret netværk mellem Beijing og Shanghai. Det største problem er i øjeblikket en meget skrap begrænsing af den afstand systemet fungerer over. Den indbyggede følsomhed de kvantemekaniske tilstande har, som netop giver sikkerheden, gør også at der opstår problemer omkring afstande på 100 km hvor hastigheden af dataoverførslen falder drastisk. Dette tab er en konsekvens af de optiske ledninger man bruger til at transportere lyset og det er også et problem for almindelig fiber kommunikation, som det der bruges til at levere hurtigt internet. I nutidens optiske kommunikation har man dog forstærkere, der øger lysstyrken og dermed signalet. En sådan forstærker ville fuldstændig destruere de følsomme kvantesignaler og kan derfor ikke bruges til at overkomme afstandsbegrænsingen af kvantekrypteringen.

Senere forskning har afsløret at det ikke er nødvendigt at bruge enkelte lyspartikler for at udnytte lysets indbyggede kvantemekaniske egenskaber. Det er tilstrækkeligt at måle den støj en laserstråle altid udviser, nærmere bestemt den støj der opstår fordi laserstrålen består af individuelle lyspartikler. Man kan derfor lave kvantekrypteringen ved at give Alice en laser og lade hende indsætte informationen om den hemmelige nøgle i lyset ved at variere lysstyrken. Det lys kan Bob måle så han får at vide hvad nøglen er, og han vil samtidig kunne opdage hvis der er en aflytter. Den sikkerhed som Alice og Bob opnår er stærkere end hvad vi hidtil har haft adgang til i den forstand at den er baseret på fysiske love. De metoder der bruges i dag udnytter matematiske strukturer i talsystemer, men de virker som tidligere beskrevet kun hvis det antages at aflytterens computer ikke er hurtig nok. Disse bekymringer behøver Alice og Bob ikke gøre sig hvis de bruger kvantekryptering.

Et nyt bidrag til kvantemekanisk kryptering

Min forskning viser at man kan gøre krypteringen endnu bedre, ved at give det måleudstyr der normalt er hos Bob til aflytteren. Det lyder måske som en dårlig ide, men mine forsøg har vist

at det virker i praksis. Metoden fungerer ved at både Alice og Bob får en lyskilde hvor de begge to indsætter signaler i laserstrålen ved at variere deres lysstyrker. Disse signaler skal bruges til at bygge deres fælles hemmelige nøgle. De sender så disse signaler til en fælles modtager, som aflytteren i princippet kan kontrollere. Modtageren er bygget på en bestemt måde så den ikke måler lyset fra Alice og Bob hver for sig, men i stedet måler det sammenlagte eller interfererede lys. Fordi signalerne er interfererede kan aflytteren ikke adskille dem, men Alice og Bob kan hver for sig regne ud hvad deres modpart kodede ind i lyset, fordi de kender den del af signalet de selv kodede ind.

Det er umiddelbart let at se at denne type kvantekryptering er velegnet til en netværksstruktur. Svagheden ved den er at Alice er nødt til at være meget tæt på modtageren før det virker, ellers bliver dataoverførslen af den hemmelige nøgle alt for langsom, og tæt på betyder i denne sammenhæng ganske få kilometer. Til gengæld kan Bob så være op til 50 km væk. Heldigvis er denne afstandsbegrænsing ikke et større problem i en storby, hvor man kunne forestille sig at det ville være muligt at sætte modtagerstationer op med jævne mellemrum. Brugerne kunne så koble på afhængigt af hvor de selv befinder sig for at kommunikere sikkert med hinanden, og det er ikke nødvendigt for dem at stole på at modtagerstationen er sikker, fordi den ikke behøver være det. I denne sammenhæng ville København være et oplagt sted at afprøve denne teknologi fordi byområdets størrelse passer godt til hvad er teknologisk muligt i øjeblikket.

Andre former for kryptering

En stor del af min forskning handlede om den ovenfor beskrevne kvantekryptering med to parter, Alice og Bob, som gerne vil etablere sikkerhed mellem sig. I slutningen af mit PhD forløb flyttede fokus sig imidlertid til hvad vi kalder ensidig kvantesikkerhed. Vi forestiller os et scenarie hvor en klient ønsker at behandle noget data på en kvantecomputer. Hun har ikke selv en kvantecomputer til rådighed, men vi befinder os i en, mere eller mindre fjern, fremtid hvor centraliserede kvantecomputere kan tilgås på kvanteinternettet lidt på samme måde som man kan leje lagerplads hos Dropbox i dag. IBM har for nylig gjort en simpel udgave af dette koncept tilgængelig via internettet under navnet IBM Quantum Experience. Klienten forbinder sig til en centraliseret kvantecomputer, en server, hvor hun beder serveren om at køre et bestemt program på hendes data. Hun stoler dog ikke på de personer eller det selskab der vedligeholder denne kvanteserver, så hun vil gerne kryptere sine data. Her opstår der et problem, for hvordan kan kvantecomputeren regne på data der er krypteret? Det svarer til at skrive en søgetekst til Google der bliver krypteret inden man trykker på søg.

Det viser sig at det kan lade sig gøre for kvantecomputeren at regne på krypteret data, hvis man krypterer det på den rigtige måde. I samarbejde med to teoretiske fysikere fra Toronto, Canada viste vi hvordan man kan kryptere et input til et program i en kvantecomputer, køre programmet, returnere outputtet af programmet til klienten og lade hende dekryptere outputtet. Hvis det gøres rigtigt bliver det dekrypterede output det samme som hvis klienten havde sendt det ukrypterede input til serveren. Det betyder at klienten kan køre programmet og få det output hun har brug for uden at afsløre det rigtige input til kvantecomputeren. Et muligt scenarie hvor dette overraskende resultat kunne finde anvendelse er indenfor fremtidens bioteknologi. Man kunne forestille sig at et biotek firma i al hemmelighed har en formodning om at et bestemt molekyle kan bruges til at lave effektiv medicin mod en sygdom, og en måde for dem at afprøve det er at simulere molekylets reaktion på forskellige påvirkninger. Sådanne simulationer er meget tidskrævende for almindelige computere, men for en fremtidig kvantecomputer ville det være barnemad. Det føromtalte biotek firma beslutter sig for at købe adgang til en server med en kvantecomputer og køre et program der simulerer disse påvirkninger, men de ønsker

ikke at afsløre deres input, molekylet. Med den krypteringsteknik vi har udviklet gennem min forskning kan molekylet holdes hemmeligt samtidig med at biotek firmaet får resultatet af deres simulation.

Håbet er at forskningen og mine eksperimentielle resultater bidrager til at bringe disse teknologier tættere på at revolutionere informationsteknologien, til gavn for hele samfundet via hurtigere og bedre computere og stærkere informationssikkerhed til alle der må have brug for det.