Kvantenøgledistribution

Foråret 2025

Anna Liv Paludan Bjerregaard

Niels Bohr Institutet, Københavns Universitet

NQCP

NIELS BOHR INSTITUTE

Indhold

Afsnit 1

Formål med teksten

Denne tekst er supplerende materiale til afsnittet om kvantenøgledistribution i LIFE Fondens undervisningsforløb om kvantekommunikation, *Unbreakable*. Målet med teksten er at give en grundigere introduktion til det matematiske og kvantefysiske grundlag for kvantenøgledistribution.

Afsnit 2

Krypteringsnøgler

Krypteringsnøgler er grundlaget for, at kommunikation i den moderne verden kan foregå sikkert. Man kan tænke på dem som en slags ordbog, som kan oversætte et sæt af symboler til et andet – hvis man ikke har ordbogen, er det meget svært at oversætte krypterede beskeder. Et eksempel kunne være, hvis man kun sendte beskeder i morsekode. Det er nemt at forstå beskederne, hvis man kender morsealfabetet, men hvis ikke, er det meget svært. Hvis kun afsender og modtager har krypteringsnøglen, kan de kommunikerer sikkert, men hvordan kan de sørge for, at *kun* de ved, hvad nøglen er? Man kan dele nøglen fysisk på et stykke papir, men det kræver fysisk kontakt. Man kunne sende nøglen krypteret med en ny krypteringsnøgle, men så har man samme problem med den nye nøgle, som krypterer den originale nøgle. Kvantenøgledistribution er en metode, som udnytter kvantemekanikkens love til at kunne sende nøgler over lange afstande gennem optiske fibre og *samtidig* bekræfte, om nøglen er blevet aflyttet af en anden eller ej.

Den samfundsmæssige interesse for kvantenøgledistribution er større end nogensinde. I 1996 viste Peter Shor, at moderne RSA-kryptering, som anvender store primtal som krypteringsnøgler, kan brydes effektivt af en kvantecomputer. Kvantecomputeren nærmer sig nu teknologisk realisering, og det bliver derfor vigtigere og vigtigere at kunne kryptere beskeder, på en måde som ikke kan brydes. Kvantenøgledistribution er med til at sikre kryptering selv i en fremtid med kvantecomputere.

Afsnit 3

Kvantemekanikkens spilleregler

I kvantenøgledistribution bruges polarisation af lys og polarisationsfiltre til at sende krypteringsnøglen mellem parter, som gerne vil kommunikere hemmeligt, men hvorfor er det smart? Enkelte fotoner er kvantemekaniske partikler og følger derfor kvantemekanikkens love – et faktum, som kan udnyttes til at skabe en krypteringsnøgle, som man ved er hemmelig. For at forstå, hvordan kvantenøgledistribution fungerer, skal vi først forstå klassisk polarisation og dernæst, hvad der sker, når en foton med kvantemekanisk polarisation passerer igennem et polarisationsfilter.

Underafsnit 3.1

Klassisk polarisation

Figur 1. Udsvingsretning for en lysbølge illustreret i 2D og i 3D. Symbolet ⊙ betyder, at udbredelsesretningen er ud af papiret, altså direkte mod dig!

I den klassiske (altså *ikke* kvantemekaniske) teori om elektromagnetisme er lys beskrevet som elektromagnetiske bølger og har derfor følgende egenskaber:

- Bølgelængde
- Udsvingsamplitude
- Udbredelsesretning
- Udsvingsretning

Udsvingsretningen skal være vinkelret på udbredelsesretningen, f.eks. svinger bølger i vand op og ned, mens de bevæger sig langs vandets overflade. Da en lysbølge altid har én bestemt udbredelsesretning, vil udsvingsretningen af de elektromagnetiske felter altid være defineret i en todimensionel plan, som ses i den første illustration i figur 1. Lysbølgens udsvingsretning kalder vi for bølgens *polarisation*. Hvis vi indsætter en x-akse og en y-akse, kan vi opskrive polarisationen som en vektor $\vec{P}$:

$$\vec{P} = \begin{pmatrix} a \\ b \end{pmatrix} , \tag{3.1}$$

hvor komponenterne indikerer, *hvor meget* af lyset der er polariseret langs hver akse.

Et polarisations*filter* er så et stykke tyndt materiale, som kun tillader passage af den del af lyset, der har en bestemt polarisation. Hvis filteret orienteres lodret opad, vil 0% af en vandret polariseret lysbølge passere igennem – en lodret polariseret bølge vil derimod passere 100% igennem. Da filterets orientering også er en retning, kan denne også beskrives som en vektor $\vec{o}$:

$$\vec{o} = \begin{pmatrix} c \\ d \end{pmatrix} . \tag{3.2}$$

Bemærk at, da $\vec{P}$ og $\vec{o}$ begge blot er retninger, kan vi behandle dem som enhedsvektorer, og $|\vec{P}| = |\vec{o}| = 1$. Hvis vi sender lys med en polarisation $\vec{P}$ igennem et filter med orientering $\vec{o}$, vil intensiteten af lyset på den anden siden af filteret være bestemt af prikproduktet $\vec{P} \cdot \vec{o}$. Prikproduktet kan skrives som et udtryk af vinklen $\theta_{P,o}$ mellem $\vec{P}$ og $\vec{o}$

$$I_{\text{efter}} = I_{\text{før}} |\vec{P} \cdot \vec{o}|^2 = I_{\text{før}} \cos^2 \theta_{P,o} \,, \tag{3.3}$$

hvor $I_{\text{før}}$ er intensiteten af lyset (målt i W/m^2), før det har passeret filteret. Kigger vi på særtilfældet, hvor $\vec{o}$ er en enhedsvektor langs x-aksen, så vil det gælde, at $\cos^2 \theta_{P,o} = a^2$. Den klassiske fortolkning af dette er, at kun en brøkdel af lyset passerer igennem filteret. F.eks. vil 100% af lyset passerer igennem, hvis $\theta_{P,o} = 0°$, hvorimod kun 50% af lyset kommer igennem, hvis $\theta_{P,o} = 45°$. Tabel 1 viser et overblik over lysets passage for forskellige orienteringer af vinklen $\theta_{P,o}$. Polarisationen af det passerede lys vil være i samme retning som filtrets orientering.

Vinkel $\theta_{P,o}$	0°	45°	90°	135°	180°
$I_{\text{efter}}/I_{\text{før}}$ (i %)	100%	50%	0%	50%	100%

Tabel 1. Intensiteten af lys som har passeret igennem et polarisationsfilter som en procentdel af den originale intensitet. Procenterne er fundet ved brug af ligning 3.3.

Underafsnit 3.2

Er en foton polariseret?

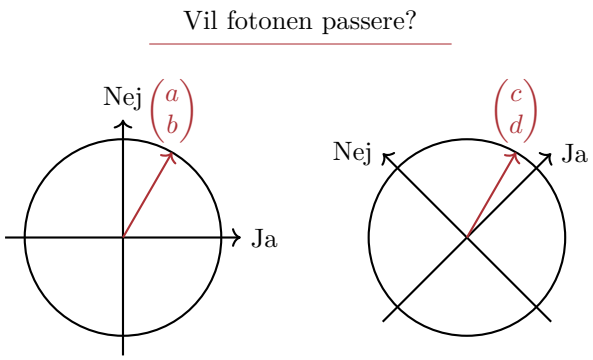
Hvis vi i stedet for at arbejde med en hel stråle af lys blot holder os til en enkel foton, bliver vores forståelse af polarisation straks udfordret: Hvis jeg sender en foton med polarisering $\vec{P}$ gennem et polarisationsfilter med orientering $\vec{o}$, hvad sker der så? Lad os sige at $\theta_{P,o} = 45°$. Her ville vi i det klassiske tilfælde sige, at *halvdelen* af lyset vil passere, men vil halvdelen af en foton gå igennem filteret, mens den anden halvdel bliver stoppet? Det viser sig, at fotonen ikke deles i halve, men at der er to mulige udfald: Enten bliver fotonen stoppet, eller også passerer den igennem. Polarisationen bestemmer, hvor *sandsynligt* hvert af disse udfald er. Sandsynligheden for, at en foton med polarisation $\vec{P}$ passerer et polarisationsfilter med orientering $\vec{o}$ er:

$$p_{\text{passage}} = |\vec{P} \cdot \vec{o}|^2 = \cos^2 \theta_{P,o} \,, \tag{3.4}$$

hvor vi bruger p til at indikere sandsynlighed (p'et står for engelsk *propability*). Polarisationen af en foton, som har passeret et polarisationsfilter, vil have samme orientering som filtrets orientering, uanset hvad polarisationen af fotonen var før passagen. Bemærk ligheden mellem ligning 3.4 for sandsynlighed og ligning 3.3 for intensitet efter passage gennem filteret. I resten af denne tekst vil vi fokusere på tilfælde, hvor fotonens polarisation og polarisationsfiltret er orienteret lodret, vandret eller $\pm 45°$ i forhold til hinanden.

Underafsnit 3.3

Er det kvanteteknologi?



Figur 2. Tilstanden af polarisationen af en enkelt foton i den vertikale-horisontale basis samt den skrå basis. Bemærk, at selvom selve vektoren er den samme, er dens komponenter basis-afhængige.

Når man hører ordet "kvantemekanik", tænker mange på Niels Bohr, som undersøgte interaktioner mellem atomer og lys. Kvantenøgledistribution er kvanteteknologi, da teknologien udnytter fotoners kvantemekaniske egenskaber. Inden for kvantemekanikkens fagsprog beskrives polarisationen af fotonen som en *tilstand*, og polarisationsfilteret foretager en *måling* af denne tilstand. Hvis en foton med polarisation $\vec{P}$ rammer et polarisationsfilter med orientering $\vec{o}$, kan vi undersøge, om fotonen passerer igennem polarisationsfiltret. Vi ved fra Tabel 1, at fotonen vil passere med 100% sandsynlighed, hvis fotonens polarisering er parallel med orienteringen af filteret. Hvis $\vec{P}$ og $\vec{o}$ er vinkelrette i forhold til hinanden, vil fotonen passerer med 0% sandsynlighed. Der er med andre ord to udfald: "*Ja*, fotonen går igennem" og "*Nej*, fotonen går ikke igennem".

Vi kan derfor beskrive polarisationsvektoren i en såkaldt *basis* af polarisationsfilterets retning (ja) og en komponent vinkelret på denne (nej). En basis er det sæt af enhedsvektorer, som vi bruger til at definere alle andre vektorers komponenter. Det mest normale valg af basis er blot enhedsvektorer langs x- og y-akserne. Ligning 3.5 og figur 2 viser, at den samme vektor skrives på forskellige måder med forskellige baser.

$$\vec{P} = a\vec{v}_{\rightarrow} + b\vec{v}_{\uparrow} \quad \text{eller} \quad \vec{P} = c\vec{v}_{\nearrow} + d\vec{v}_{\nwarrow} \tag{3.5}$$

Bemærk i denne ligning, at $\vec{v}_{\rightarrow}$, $\vec{v}_{\uparrow}$, $\vec{v}_{\nearrow}$ og $\vec{v}_{\nwarrow}$ er enhedsvektorer, og at a, b, c, og d er tal mellem 0 og 1. Hvis du spørger en kvantefysiker, vil hun med sit fagsprog sige, at fotonens polarisation er i en *superposition* af vores basis. Hun ville nok også skrive den ovenstående ligning på følgende måde:

$$|p\rangle = a\,|{\rightarrow}\rangle + b\,|{\uparrow}\rangle \quad \text{eller} \quad |p\rangle = c\,|{\nearrow}\rangle + d\,|{\nwarrow}\rangle \tag{3.6}$$

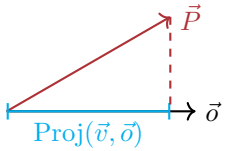
Den kantede parentes $|\ \rangle$ kaldes en "ket" og er den udbredte notation for en kvantemekanisk tilstand. I denne tekst vælger vi dog at bruge 'normale" vektorer med pile til at beskrive tilstande.

Vi kan nu bruge disse vektorer til at udregne sandsynligheden for, at en foton passerer igennem et polarisationsfilter. Denne sandsynlighed viser sig at være kvadratet af *projektionen* af polarisationen ($\vec{P}$) på filterets orientering ($\vec{o}$). Projektionen af to

vektorer beskriver, hvor meget de to vektorer overlapper, og kan findes ved:

$$\text{Proj}(\vec{P}, \vec{o}) = \frac{\vec{P} \cdot \vec{o}}{|\vec{o}|^2} \,. \tag{3.7}$$

Den geometriske fortolkning af dette overlap er vist i figur 3.



Figur 3. Projektionen af to vektorer kan fortolkes geomtetrisk som afbildningen af den ene vektor langs den anden.

Hvis vi tager eksemplet, hvor polarisationsfilteret er orienteret vandret, udtrykker a og b sandsynlighederne for, om fotonen passerer eller ej:

$$p_{\text{Ja}} = \text{Proj}(\vec{P}, \vec{v}_{\rightarrow})^2 = a^2 \,, \quad p_{\text{Nej}} = \text{Proj}(\vec{P}, \vec{v}_{\uparrow})^2 = b^2 \,. \tag{3.8}$$

Bemærk, at fotonen enten skal passere eller blive stoppet. Summen af sandsynlighederne skal derfor være 1 (svarende til 100 %: $p_{\text{Ja}} + p_{\text{Nej}} = a^2 + b^2 = 1$). Da $|\vec{P}| = a^2 + b^2 = 1$, betyder dette, at $\vec{P}$ er en enhedsvektor, som peger på et punkt på enhedscirklen, hvilket også er indikeret i figur 2.

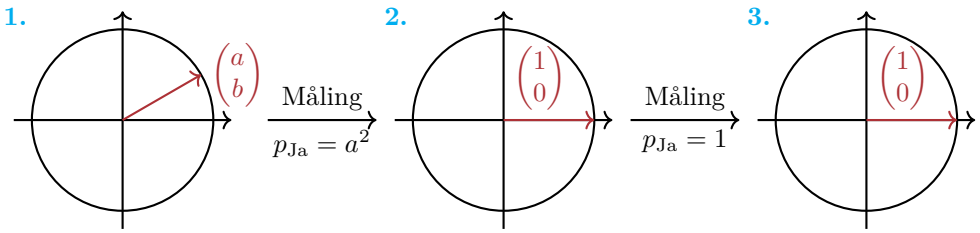
Underafsnit 3.4

Flere polarisationsfiltre i træk

Vi har indtil videre beskrevet, hvad der sker, når en enkelt foton passerer igennem et polarisationsfilter, men kvantenøgledistribution bruger to polarisationsfiltre (eller endnu flere, hvis en spion lytter med). Derfor er det nødvendigt at undersøge, hvad der sker, hvis vi måler polarisationen af den samme foton flere gange i træk. Som nævnt, har en foton, som har passeret et polarisationsfilter, samme polarisation som filterets orientering. Der sker altså følgende tre ting, når fotonen passerer de to filtre, der begge er orienteret vandret:

1. Fotonen passerer det første filter. Hvis fotonen har polarisation $\vec{P} = \begin{pmatrix} a \\ b \end{pmatrix}$, sker dette med sandsynlighed $p_{\text{Ja}} = a^2$.
2. Efter at have passeret det første filter har fotonen nu med sikkerhed polarisation $\vec{P} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Den vil med garanti passerer det andet filter, som også er orienteret vandret, $p_{\text{Ja}} = 1$.
3. Efter at have passeret det andet filter har fotonen nu polarisation $\vec{P} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

Disse tre trin er også illustreret i Figur 4. Generelt kan vi sige, at hvis to filtrer er orienteret ens, ved vi med sikkerhed, at en foton, som passerer igennem det ene, også vil passere det andet.



Figur 4. Tilstanden af polarisationen af en enkelt foton i den vertikale-horisontale basis som passerer det samme filter to gange.

Hvis vi derimod orienterer det andet polarisationsfilter, så det *ikke* er orienteret på samme måde som det første polarisationsfilter, svarer det til, at vi først måler langs én basis og dernæst en anden. Dette er vist i figur 5. Hvis det første filter er indstillet vandret, og det næste er $+45°$ roteret, vil de tre skridt for fotonen være:

1 Fotonen passerer det første filter. Hvis fotonen har polarisation $\vec{P} = \begin{pmatrix} a \\ b \end{pmatrix}$, sker dette med sandsynlighed $p_{\text{Ja}} = a^2$.

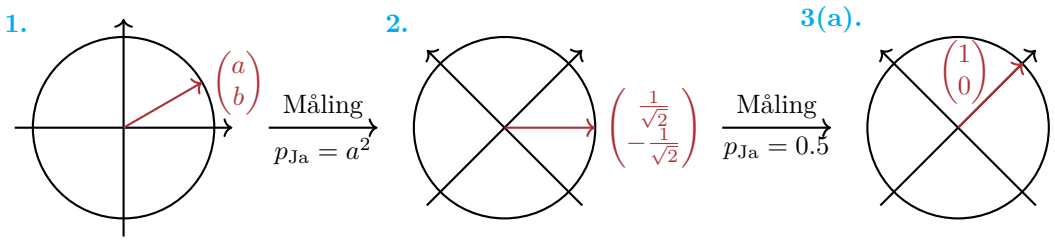
2 Efter at have passeret det første filter har fotonen nu med sikkerhed polarisation $\vec{P} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ i basisen af det første filter. I basisen af det andet filter, er samme polarisation beskrevet som $\vec{P} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$. Fotonen vil derfor passere det andet filter med sandsynligheden $p_{\text{Ja}} = \text{Proj}(\vec{P}, \vec{v}_{\nearrow}) = \frac{1}{2}$.

3 Der er nu to mulige udfald:

(a) Fotonen passerer det andet filter med 50% sandsynliged og bliver opfanget af modtageren.

(b) fotonen bliver stoppet af det andet filter med 50% sandsynlighed, og modtageren modtager ikke noget.

Vi kan derfor ikke være sikre på, at en foton, som har passeret det første filter, også vil passerer det andet. Udfaldet er derfor *uforudsigeligt*.



Figur 5. Tilstanden af polarisationen af en enkelt foton i den vertikale-horisontale basis, som passerer to forskelligt orienterede filtrer. Bemærk skiftet af basis efter den første måling, samt at $(1/\sqrt{2})^2 = \frac{1}{2}$. Der er også mulighed for, at fotonen ikke passerer det andet filter.

Afsnit 4

Kvantenøgledistribution

Beskrivelserne af polarisationer, projektioner og sandsynligheder kan bruges til at forklare grundprincipperne i kvantenøgledistribution. Kvantenøgledistribution er en teknologi til at dele krypteringsnøgler, som kan bruges til at kryptere og dekryptere en hemmelig besked. Fremgangsmåden for kvantenøgledistributioner kan beskrives i fire trin:

1. Afsender sender nogle fotoner med tilfældige polarisationer. Polarisationerne af hver foton bestemmes af, at afsender indstiller et polarisationsfilter tilfældigt i fire forskellige orienteringer: vertikal ($\uparrow$), horisontal ($\rightarrow$), $+45°$ ($\nearrow$) eller $-45°$ ($\nwarrow$). Disse fotoner sendes via en optisk fiber til modtageren.

2. Modtager lader de afsendte fotoner passere endnu et polarisationsfilter, som også er indstillet tilfældigt i de fire mulige positioner. Modtager noterer så, om fotonen passerer polarisationsfiltret eller ej.

3. Afsender og modtager deler en begrænset mængde af deres informationer om polarisationsfiltrenes positioner via almindelige usikre kanaler, men holder noget af det hemmeligt. Dette gør de ved at fortælle hinanden: "*Mit filter var enten vandret eller lodret*" eller "*Mit filter var enten* $+45°$ *eller* $-45°$". Dette svarer til at dele basis. En spion kan aflytte denne begrænsede information, men der er ikke nok information til, at en spion kan tænke sig frem til krypteringsnøglen.

4. Afsender og modtager udvælger de fotoner, hvor polarisationerne er forudsigelige. Polarisationerne af de forudsigelige fotoner er krypteringsnøglen.

Følgende er et tænkt eksempel, som illustrerer, at en krypteringsnøgle kan deles sikkert med denne fremgangsmetode. Afsender har orienteret sit polarisationsfilter således, at fotonen sendes med en $+45°$ ($\nearrow$) polarisation. Modtager kan nu orientere sit polarisationsfilter på fire forskellige måder, som bestemmer sandsynligheden for, at fotonen passerer:

$$+45° \ : P_{\text{Ja}} = \text{Proj}(\vec{v}_{\nearrow}, \vec{v}_{\nearrow})^2 = 1 \,, \tag{4.1}$$

$$-45° \ : P_{\text{Ja}} = \text{Proj}(\vec{v}_{\nearrow}, \vec{v}_{\nwarrow})^2 = 0 \,, \tag{4.2}$$

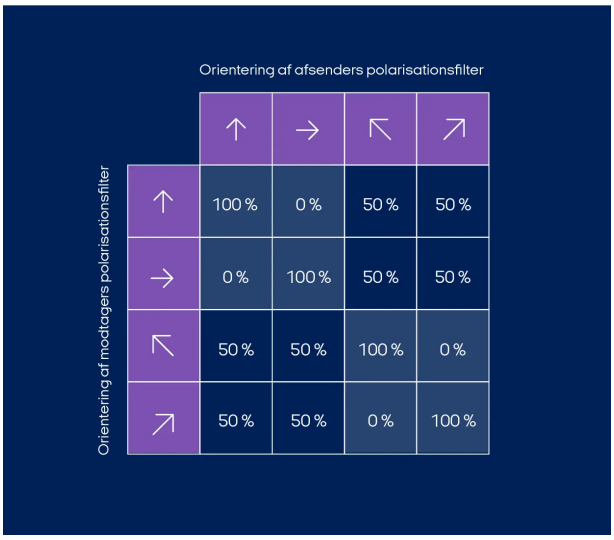
$$90° \ : P_{\text{Ja}} = \text{Proj}(\vec{v}_{\nearrow}, \vec{v}_{\rightarrow})^2 = 0.5 \,, \tag{4.3}$$

$$0° \ : P_{\text{Ja}} = \text{Proj}(\vec{v}_{\nearrow}, \vec{v}_{\uparrow})^2 = 0.5 \,. \tag{4.4}$$

I dette tilfælde siger vi, at hvis modtageren indstiller sit filter til $\pm 45°$, er udfaldet *forudsigeligt*, da der i de tilfælde kun er ét muligt udfald. Bemærk, at dette svarer til, at afsender og modtager har valgt samme basis. I kvantenøgledistributionens trin 3 & 4 udvælges de fotoner, hvor både afsender og modtager tilfældigvis har valgt samme basis. I dette eksempel svarer det til, at afsenderen har sendt en foton med enten $+45°$ eller $-45°$ polarisation. Modtagerens polarisationsfilter er som nævnt orienteret $+45°$, så modtageren kan med sikkerhed tænke sig frem til afsenderens valg af polarisation:

- Hvis de *ser* fotonen, var afsenders orientering $+45°$.
- Hvis de *ikke ser* fotonen, var afsenders orientering $-45°$.

Se et overblik over forudsigelige udfald i Figur 6.



Figur 6. Overblik over forudsigelighed af udfald for forskellige orienteringer af afsender og modtagers polarisationsfiltre. De orienteringer med forudsigelige udfalg er fremhævet med en lysere farve. Alle udfald bliver uforudsigelige, hvis en spion lytter med.

Hvis afsender og modtager vælger deres polarisationsfiltre tilfældigt, har de 50% chance for at få en foton, som er forudsigelig. Hvis der sendes nok fotoner, kan både afsender og modtager nedskrive afsenderens orientering for alle forudsigelige konfigurationer og bruge disse orienteringer som krypteringsnøgle til at kryptere en hemmelig besked. Bemærk, at dette kan gøres, helt uden at informationen om afsenderes orienteringer nogensinde er blevet sendt direkte til modtageren. Bemærk også, at der på dette tidspunkt ikke er blevet delt noget som helst hemmeligt mellem modtager og afsender, da kvantenøgledistribution skal foregå, *før* selve de hemmelige beskeder krypteres og afsendes.

Men er disse hemmelige beskeder virkelig hemmelige? Lad os prøve at tænke over, hvad der sker, hvis en spion har aflyttet de optiske fibre.

Underafsnit 4.1

Kvantenøgledistribution med aflytning

Forestil dig, at du er en spion, som vil aflytte samtalen mellem afsender og modtager. Hvis du venter, til de allerede har krypteret deres kanal, er det for sent! Du er nødt til at forsøge at aflytte kvantenøgledistributionen for at opfange krypteringsnøglen, som du skal bruge til at dekryptere beskederne mellem afsender og modtager. Du sætter derfor en fiberoptisk aflytningsenhed midt på den optiske fiber og begynder at stjæle fotoner, men nu løber du ind i et problem: Hvis du stjæler en foton fra afsenderen, vil modtageren aldrig modtage denne foton. Det ville se højst mistænkeligt ud, og det vil nok få modtageren til at mistænke, at nogen var ved at aflytte signalet. Så du bliver altså nødt til at sende en ny foton afsted, men hvilken polarisation skal du vælge? Husk på, at deling af basis (trin 3) i kvantenøgledistribution først sker, *efter* at alle fotoner er blevet afsendt. Du har derfor ingen information om, hvilken polarisation afsenderen har sendt fotonerne med. Du bliver nødt til at gætte polarisationerne. Modtager og afsender sender dog hundredevis af fotoner mellem hinanden, og hvis du som spion gætter forkert bare en enkelt gang, risikerer du at blive afsløret!

I praksis vil kvantenøgledistribution også have et skridt skridt, som ikke blev præsenteret tidligere i afsnit 4. Når alle fotoner er blevet afsendt, og afsender og modtager har delt og udvalgt de forudsigelige baser, bliver der lavet et ekstra tjek: Afsender og

modtager deler begge en lille del af deres krypteringsnøgle (f.eks. hver 5. orientering) via usikre kanaler. Hvis disse delte dele af krypteringsnøglen ikke er helt identiske for afsender og modtager, ved de, at en spion har været inde og aflytte kvantenøgledistributionen.

Underafsnit 4.2

Hvor sikkert er kvantenøgledistribution?

Kvantenøgledistribution er sikker, fordi potentielle spioner ikke med sikkerhed kan gætte polarisationen af et stort antal fotoner. Men er der en chance for, at spionen bare er heldig?

Hvis spionen selv sætter et polarisationsfilter op, som afsenderens fotoner passerer igennem, kan spionen udelukke, at afsenderens polarisationsfilter var orienteret vinkeltret med spionens filter. På samme måde kan spionen udelukke, at afsenders polarisationsfilter var orienteret parallelt med spionens filter, hvis fotonen ikke passerer. Spionen har derfor $1/3$ chance for at gætte polarisationen korrekt.

Hvis modtager og afsender sender, deler og udvælger N fotoner med forudsigelige baser og foretager deres tjek med $N/5$ af dem, er chancen for, at spionen *ikke* bliver opdaget, $(1/3)^{N/5}$. Tabel 2 viser, at spionens chance for at gætte korrekt og derved forblive uopdaget falder drastisk, når antallet af fotoner øges.

N	5	20	50	100	200
p_{Success}	33.33%	1.23%	0.002%	3×10^{-8}%	8×10^{-18}%
$p_{\text{Gæt}}$	0.4%	2.3×10^{-8}%	8.3×10^{-23}%	6.8×10^{-47}%	1.4×10^{-94}%

Tabel 2. p_{Success} angiver chancen for, at spionen ikke bliver opdaget, når afsender og modtager deler $1/5$ af krypteringsnøglen. $p_{\text{Gæt}}$ angiver chancen for blot at gætte krypteringsnøglen ud fra den delte $1/5$ af krypteringsnøglen.

Bemærk, at der her er en slags trade-off. Hvis afsender og modtager vælger at dele en større andel af krypteringsnøglen, bliver chancen også større for, at de opdager spionen. Til gengæld bliver en større andel af krypteringsnøglen delt ad en usikker kanal. Derfor bliver det nemmere at gætte resten af krypteringsnøglen for andre spioner, som *ikke* aflyttede kvantenøgledistributionen. Heldigvis er det ikke lige til at gætte denne rest af krypteringsnøglen. Hvis en spion bare gætter sig frem til krypteringsnøglen ud fra den $1/5$ af krypteringsnøglen, som deles usikkert, skal spionen gætte korrekt $4N/5$ gange. Chancen for at gætte rigtigt, er derfor $(1/4)^{4N/5}$. Som det fremgår af Tabel 2, bliver begge metoder for at udspionere meget hurtigt meget usandsynlige.