

Kvantekryptografi

Ivan Damgård

February 15, 2002

1 Indledning

Kryptografi har lige siden tidernes morgen haft som mål at skabe sikker kommunikation over usikre kommunikationskanaler. I denne artikel vil vi koncentrere os om hemmeligholdelse, altså to parter - lad os kalde dem Alice og Bob - ønsker at udveksle en meddelelse således at deres værste fjende Eve ikke vil have nogen som helst anelse om hvad der er blevet sendt.

I praksis findes en række udmærkede og anvendelige løsninger på dette problem, som imidlertid alle har en ting til fælles: hvis Eve har tilstrækkelig mange ressourcer til rådighed (hvilket i praksis vil sige regnekraft), så kan alle disse systemer brydes, dvs. Eve kan alligevel finde ud af hvad der blev sendt. Det er ikke noget tilfælde, at det er sådan: i 40-erne skabte Shannon informationsteorien, og fandt bl.a. præcise betingelser for, hvornår absolut sikkerhed mod Eve kan lade sig gøre, dvs. hvad skal der til for at Eve intet får at vide, uanset hvor mange ressourcer hun har til rådighed. Det viser sig at være nødvendigt at Alice og Bob på forhånd er enige om en hemmelig nøgle K , dvs. K er en streng af bits k_1, \dots, k_n som er tilfældigt valgt, og som Eve ingen information har om. Man kan nu sende en meddelelse bestående af n bits $M = m_1, \dots, m_n$ krypteret v.hj.af K ved at sende $C = m_1 \oplus k_1, \dots, m_n \oplus k_n$, dvs. hver bit i meddelelsen adderes modulo 2 med en bit i nøglen. Det er let at se, at hvis Eve ingen information har om K , så er - selv givet C - enhver værdi for M lige sandsynlig, m.a.o. Eve har intet fået at vide. Dette kaldes *perfekt sikkerhed*.

Men Shannons resultat sagde så, at perfekt sikkerhed kræver at nøglen indeholder mindst lige så meget information som meddelelsen, dvs. hvis der n bits i meddelelsen, så skal antal bits i nøglen være mindst n , ligegyldigt hvordan krypteringen foregår. Ydermere kan hver nøgle kun bruges een gang, ellers mistes den perfekte sikkerhed. Denne form for kryptering kaldes derfor *One-Time Pad*.

Et system baseret udelukkende på one-time pads er af naturlige årsager helt uanvendeligt i praksis på grund af de indlysende problemer med at få nøglen på plads på sikker vis inden kommunikationen foregår. Derfor bruger

krypteringssystemer i praksis andre metoder hvor man genbruger den samme korte nøgle til adskillige meddelelser. Men - som forudsagt af Shannon - ethvert sådant system kan i princippet brydes hvis man bruger tid nok på det. Det ville naturligvis være OK, hvis vi med sikkerhed vidste at "tid nok" betyder adskillige millioner år, f.eks. Men desværre er det ikke lykkedes for nogen at konstruere et praktisk anvendeligt system, hvor vi med sikkerhed hvor meget tid der faktisk skal til for at bryde det. Derfor er kryptering i praksis i dag funderet på velunderbyggede formodninger, snarere end beviser. Og selvom vi havde sådanne beviser, så siger Shannon jo at vi aldrig vil kunne fjerne muligheden for at vore systemer kan brydes hvis de også skal være praktisk anvendelige.

Det ser jo alt sammen temmelig utilfredsstillende ud. Imidlertid har det i de senere år vist sig, at Shannon's pessimistiske resultater i virkeligheden bygger på nogle antagelser om hvad Eve i stand til at gøre, nemlig flg.:

- Eftersom vi ikke har fysisk kontrol over hele kommunikationskanalen, er Eve altid i stand til at se på kommunikationen og vil så få at vide præcis hvilke bits der er sendt mellem Alice og Bob (selvom hun måske ikke umiddelbart kan forstå meddelelsen).
- Efter at have set på kommunikationen, kan Eve vælge at lade den gå videre uændret til modtageren, som aldrig vil kunne opdage at andre har set på den.

Det kan umiddelbart virke selvindlysende, at disse antagelser må være rigtige, uanset hvordan kommunikationen foregår. Og så længe vi taler om almindelig digital kommunikation, så er antagelserne helt i orden. Faktisk mente forskere på området i næsten 50 år ikke engang at der var grund til at overveje om dette er en præcis model af verden.

2 Kvanteeinformation

Det kan derfor synes overraskende, at billedet skifter fuldstændigt, hvis vi bruger *kvantekommunikation*. Her sendes information kodet i tilstanden af meget små fysiske systemer, såsom elementarpartikler. Man bruger typisk de mindst mulige enheder af lys, nemlig fotoner. Når så små fysiske systemer er i spil, er vi nødt til at bruge kvantefysikken til at beskrive deres opførsel, hvilket har en del uventede konsekvenser.

F.eks. er det et grundlæggende princip i kvantefysik at når man måler på et fysisk system, som inden målingen er i en ukendt tilstand, så er det umuligt altid at bestemme systemets tilstand fuldstændigt; yderligere vil enhver måling med en vis sandsynlighed påvirke systemets tilstand. Det er meget vigtigt at forstå, at disse udsagn er absolutte, og intet har med teknologi at gøre: det er ligemeget hvor store summer vi investerer i at

lave en nøjagtig og skånsom måling af en elementarpartikels tilstand, det vil alligevel ikke være muligt at undgå at målingen påvirker partiklen: selve det faktum at jeg har fået en vis delvis information om dens tilstand medfører i sig selv at den blevet påvirket.

Ser vi nu igen på de to antagelser ovenfor om hvad Eve “naturligvis” kan gøre, så ses det klart, at de grundlæggende principper i kvantefysik vi har set på, præcis siger, at antagelserne er forkerte når vi bruger kvantekommunikation. Det betyder ikke i sig selv at ubetinget sikkerhed kan lade sig gøre i praksis med kvantekommunikation, men muligheden er i det mindste til stede. Vi skal nu se nærmere på hvordan kvantekommunikation opfører sig, og hvordan ubetinget sikkerhed faktisk kan opnås.

3 Qbits

I kvanteinformatik erstatter vi bits med kvantebits, også kaldet *qbits*. Hvor en klassisk bit enten er 0 eller 1, beskrives tilstanden af en kvantebit som en vektor af længde 1 i et komplekst vektorrum. Hvis vi følger den traditionelle notation og kalder de to basisvektorer for $|0\rangle$ og $|1\rangle$, så er tilstanden af en qbit generelt $\alpha |0\rangle + \beta |1\rangle$, hvor α, β er komplekse tal, så $|\alpha|^2 + |\beta|^2 = 1$. I det følgende vil holde os til tilfældet hvor koordinaterne er reelle, da det vil være tilstrækkeligt til at beskrive det vi har brug for. Man kan tænke på de to kanoniske basisvektorer som de to klassiske tilstande, en almindelig bit er begrænset til at have, dvs. en qbit er et “klassisk nul”, hhv. et “klassisk 1-tal”, hvis den er i tilstand $1 \cdot |0\rangle + 0 \cdot |1\rangle$, hhv. $0 \cdot |0\rangle + 1 \cdot |1\rangle$.

En mulig fysisk implementation af en qbit fås ved at betragte polarisationstilstanden af en foton. Polariseret lys er karakteriseret ved at alle fotoner i lysstrålen er enige om at “svinge” i en bestemt retning, f.eks. vandret eller lodret. Hver enkelt foton har derfor en polarisationstilstand, som kan beskrives ved en vinkel der fortæller hvor mange grader svingningsplanet er fra vandret. Så 0° er vandret polarisation, mens 90° er lodret. I kvantefysikkens formalisme beskrives dette i et vektorrum som før, idet vi udnævner basisvektoren $|0\rangle$ til at være vandret og $|1\rangle$ til at være lodret. Et foton der er polariseret lodret vil så være i tilstanden $0 \cdot |0\rangle + 1 \cdot |1\rangle$, mere generelt, hvis man er polariseret i en vinkel på v° , så er tilstanden $\cos(v) |0\rangle + \sin(v) |1\rangle$.

Det er nu muligt at sige noget mere præcist om, hvordan en måling foregår. Iflg. kvantefysikken er enhver måling på en qbit begrænset til at specificere to *ortogonale* tilstande (vektorer) V_0, V_1 og spørge qbitten om den er i tilstand V_0 eller V_1 . Det kan f.eks. lade sig gøre at spørge en foton om den er i tilstand $V_0 = |0\rangle$ eller $V_1 = |1\rangle$. Resultatet af målingen er bestemt som flg., når fotonen er i tilstand $\alpha |0\rangle + \beta |1\rangle$ inden målingen:

- Målingen vil give resultat $|0\rangle$ med sandsynlighed $|\alpha|^2$, og resultat $|1\rangle$ med sandsynlighed $|\beta|^2$ (det er derfor tilstande er defineret som vektorer)

af længde 1, da dette sikrer at summen af sandsynlighederne er 1).

- Efter målingen er qbitten *i den tilstand man har målt den til at være i*, og har glemt alt om den gamle tilstand.

Det skulle være klart hvordan de to principper i kvantefysik vi nævnte overfor materialiserer sig her i målinger på en qbit: generelt kan man ikke få noget præcist at vide om α og β ved en enkelt måling, og man får kun et enkelt forsøg: efter målingen er den gamle tilstand forsvundet. Man kunne tro, at det ville være muligt at lave en mere nøjagtig måling ved at fremstille nogle kopier af qbitten, og måle på alle kopierne, men desværre: en anden fundamental sætning i kvantefysik siger, at det er *umuligt* at lave en perfekt kopi af en ukendt tilstand (den såkaldte no-cloning sætning).

En generel måling, hvor V_0, V_1 ikke nødvendigvis er $|0\rangle, |1\rangle$ kan beskrives på lignende måde: givet starttilstanden $\alpha|0\rangle + \beta|1\rangle$ udregner man denne vektors koordinater i basen V_0, V_1 , og sandsynlighederne er nu givet ved disse koordinater på samme vis som overfor. Vi siger derfor at måler *i basen givet ved (V_0, V_1)* .

Selvom målinger ikke generelt giver fuldstændig information, er der dog visse specielle tilfælde, hvor en måling med sikkerhed fortæller hvad tilstanden var: hvis jeg på forhånd ved, at tilstanden er $|0\rangle$ eller $|1\rangle$, så kan jeg lave en måling der netop spørger om tilstanden er $|0\rangle$ eller $|1\rangle$, altså en måling i basen $(|0\rangle, |1\rangle)$, hvilket ifølge reglerne ovenfor altid vil give det rigtige svar. Men det er netop kun fordi målingen er indrettet efter den givne forhåndsviden. Antag, at vi istedet havde målt i basen der er drejet 45° , dvs. $(V_0, V_1) = (\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, -\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle)$. Det er ligetil at regne ud, at denne måling vil give resultat V_0 med sandsynlighed $1/2$ og V_1 med sandsynlighed $1/2$, ligegyldigt om vi måler på tilstanden $|0\rangle$ eller $|1\rangle$. Så i dette tilfælde giver målingen overhovedet ingen information om starttilstanden. Måske en bekræftelse af det gamle ord om, at et dumt spørgsmål fører til et dumt svar..

I det følgende vil + stå for den kanoniske basis $(|0\rangle, |1\rangle)$, mens \times vil stå for den "diagonale" basis $(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, -\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle)$. Endvidere vil vi bruge notationen $|0\rangle_\times = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ og $|1\rangle_\times = -\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. For at gøre notationen mere konsistent, vil vi også bruge $|0\rangle_+ = |0\rangle, |1\rangle_+ = |1\rangle$. Vi har så følgende mere generelle resultat, som følger umiddelbart af reglerne for målingers opførsel:

Sætning

Antag der måles på en qbit i tilstand $|0\rangle_+$ eller $|1\rangle_+$. En måling i +-basen vil fortælle med sandsynlighed 1 hvilken tilstand der er tale om. En måling i \times -basen giver et tilfældigt resultat, som ingen information indeholder om den målte tilstand. Antag dernæst at der måles på en qbit i tilstand $|0\rangle_\times$

eller $|1\rangle_x$. En måling i \times -basen vil fortælle med sandsynlighed 1 hvilken tilstand der er tale om. En måling i $+$ -basen giver et tilfældigt resultat, som ingen information indeholder om den målte tilstand.

4 Nøgleudveksling

Vi vil nu på, hvordan den opførsel qbits udviser, kan udnyttes til at skabe ubetinget sikkerhed. Bemærk først, at det er tilstrækkeligt at gøre det muligt for Alice og Bob at udveksle en tilfældig nøgle, som Eve ikke har information om, herefter kan one-time pad teknikken bruges til at sende selve meddelelsen krypteret.

Vi antager, at Alice er i stand til at sende qbits til Bob, men Eve kan undervejs gøre hvad som helst ved de qbits der bliver sendt - måle på dem, erstatte dem med andre qbits, etc. Vi antager også, at Alice kan kommunikere konventionelt med Bob, f.eks. over telefonen. Her er antagelsen at Eve har mulighed for at lytte med, men hun kan ikke ændre på det der bliver sagt. Der er altså ingen hemmeligholdelse givet "gratis" i modellen.

Vi udfører nu flg. protokol:

1. Alice vælger en række tilfældige bits $B = b_1, b_2, \dots, b_n$, og en række tilfældige baser $\theta = \theta_1, \dots, \theta_n$, hvor altså hver θ_i er enten $+$ eller \times . Hun sender qbits $|b_1\rangle_{\theta_1}, \dots, |b_n\rangle_{\theta_n}$ til Bob.
2. Bob vælger en tilfældig sekvens af baser $\hat{\theta} = \hat{\theta}_1, \dots, \hat{\theta}_n$, og måler qbit nr. i i basen $\hat{\theta}_i$. Hvert resultat kan på naturlig vis tolkes som en bit, lad de målte resultater være $\hat{b}_1, \dots, \hat{b}_n$.

På dette tidspunkt har Bob delvis information om den bitsekvens B Alice har sendt, i alt fald hvis Eve ikke har forstyrret kommunikationen: i ca. halvdelen af tilfældene vil $\theta_i = \hat{\theta}_i$, og det medfører iflg. sætningen ovenfor at $b_i = \hat{b}_i$. Problemet er blot at Bob ikke ved hvilke bit-positioner der er gode. Det løses ved flg. skridt:

1. Alice sender sekvensen af baser θ til Bob v.hj.af konventionel kommunikation.
2. Bob fortæller Alice hvilke i -værdier, der opfylder at $\theta_i = \hat{\theta}_i$. Alice og Bob kasserer bits på positioner hvor dette ikke er opfyldt, og beholder resten.

Vi har nu en situation, hvor Alice har en bitsekvens B' og Bob har \hat{B}' , begge af længde ca. $n/2$. Hvis Eve ikke har grebet ind i kommunikationen, så er det klart, at $B' = \hat{B}'$. På den anden side, betragt Eve's situation når Alice sender sine qbits: hvis hun vil vide noget som helst om B er hun

nødt til at måle (nogle af) qbittene. Men på dette tidspunkt har hun ingen information om θ , så hun ved ikke hvad den rigtige måling vil være for hver enkelt foton, og hun er altså nødt til at vælge sine målinger efter en eller anden strategi. Som et eksempel, lad os antage at hun vælger tilfældigt mellem en måling i $+$ eller i \times -basis. Hvis hun gætter rigtigt for den i 'te qbit, dvs. hun bruger θ_i til målingen, så vil hun få b_i som resultat. Hun kan så lave en ny qbit i præcis samme tilstand og sende den videre til Bob. Det vil ikke være værende muligt at se, at denne qbit har været angrebet. Men i halvdelen af tilfældene vil gættet være forkert, og Eve vil få en tilfældig bit \tilde{b}_i , som kun med sandsynlighed $1/2$ er lig med b_i . Eve ved jo imidlertid ikke på dette tidspunkt om hun har valgt den rigtige måling, så hun er henvist til at sende en qbit til Bob i den tilstand hun har målt. Da Bob's valg af baser når han måler er uafhængige af Eve's, vil denne strategi for Eve derfor betyde at ca. 25% af bittene i \hat{B}' er forskellige fra dem i B' . Til gengæld kender hun med sikkerhed ca. halvdelen af bittene i B' , eftersom Alice jo offentliggør θ , hvorefter Eve kender de positioner hvor hun gættede rigtigt.

Denne strategi for Eve er ikke den eneste mulige, f.eks. er Eve jo ikke begrænset til at måle i kun de to baser Alice og Bob bruger. Imidlertid kan man vise at det generelle princip vi illustrerede her er gyldigt generelt: jo flere målinger Eve foretager, jo mere får hun at vide, men samtidig vil det nødvendigvis føre til flere uoverenstemmelser mellem B' og \hat{B}' . Dette betyder omvendt, at hvis der faktisk er meget få uoverenstemmelser, så er Eve's information om B' meget begrænset. Derfor vil Alice og Bob nu vurdere hvor mange fejl der faktisk er:

1. Alice vælger en tilfældig indexmængde $I \subset \{1, 2, \dots, n\}$ af størrelse k og sender den til Bob.
2. Bob sender $\{\hat{b}_i \mid i \in I\}$ til Alice.
3. Alice sender til Bob det antal bits t i I hvor $b_i = \hat{b}_i$. Hvis $t/k \geq \epsilon$ (for et ϵ fastlagt på forhånd, se nedenfor), opgiver Alice og Bob, ellers fortsættes der.

Ideen her er for det første, at man med klassisk sandsynlighedsregning kan vise at et tilstrækkeligt stort k giver en meget præcis vurdering af den faktiske fejlrate; for det andet at man må forvente et vist antal fejl af naturlige årsager på grund af målefejl o.l., derfor må et $\epsilon > 0$ vælges herudfra.

Hvis Alice og Bob går videre herfra, så ved vi med stor sikkerhed, at fejlraten mellem B' og \hat{B}' er højst ϵ , og for det andet at ligegyldigt hvad Eve stiller op, så er hendes information om B' begrænset. For at blive helt færdige skal vi bruge nogle velkendte og klassiske teknikker, som det vil føre for vidt at komme ind på i detaljer her. For det første skal vi have rettet fejlene, så Alice og Bob er enige om samtlige bit, her kan f.eks. fejlkorrigerende koder

anvendes. For det andet har vi brug for at slippe af med den begrænsede mængde information Eve har. Dette er ikke helt ligetil: selvom vi ved at Eve kun kender få af de relevante bits, ved vi ikke hvilke hun kender. Løsningen er en teknik der kaldes *privacy amplification*: hvis Alice og Bob er enige om en bitsekvens X , og Eve's information om X er begrænset på passende vis, så er det altid muligt for Alice og Bob ved hjælp af *offentlig* kommunikation at beregne en *kortere* bitsekvens Y , hvorom Eve har en vilkårligt lille mængde information. Mere præcist, længden af Y kan vælges så Eve's information er mindre end en vilkårlig ønsket grænse.

Det er langt fra trivielt at vise at alt dette faktisk virker som ønsket, og protokollen har været kendt i lang tid, inden et egentligt bevis blev givet. Et sådant kan findes f.eks. i [1]. En lettilgængelig introduktion til kvantekryptografi kan findes i [2].

5 I virkeligheden

Der findes mange eksperimentelle implementationer af kvantekryptografi. Den mest almindelige teknik er at implementere qbits som fotoner, og bruge lyslederkabler som transportmedium. En fuldt funktionsdygtig prototype er fremstillet på Århus Universitet, mere information herom kan findes i [3]. Dette eksperiment fungerer over ca 20 Km, og det ser ud til at den nuværende teknologi vil kunne realisere afstande på op til 100 Km på sigt. Herefter vil nye ideer være nødvendige, men man ved allerede nu at der ikke er nogen principielle grænser for afstanden mellem Alice og Bob.

References

- [1] Nielsen and Chuang: *Quantum Computation and Quantum Information*, Cambridge University Press 2000.
- [2] Gilles Brassard: *Modern Cryptology*, Springer Verlag LNCS 325
- [3] <http://www.cki.au.dk>