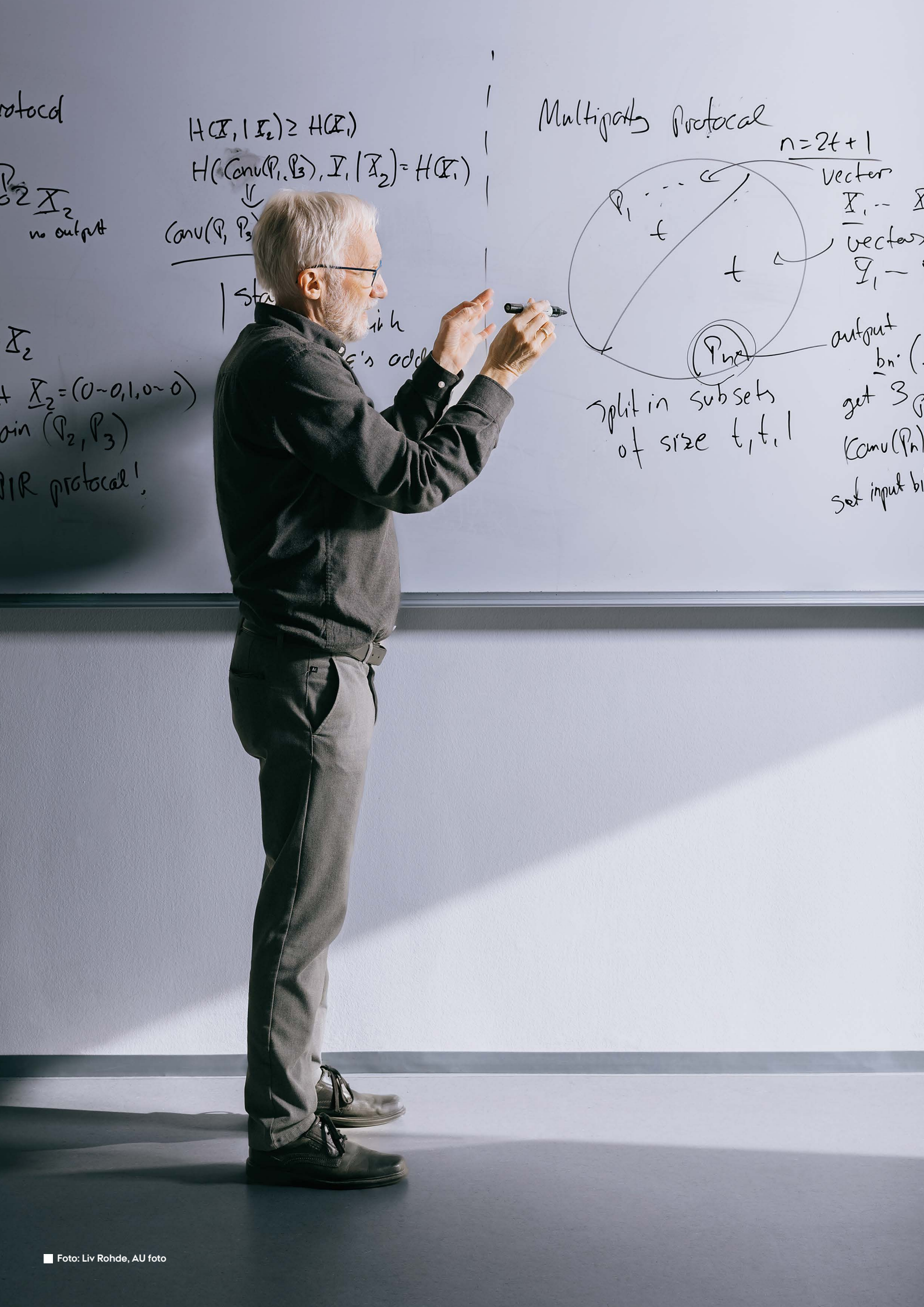
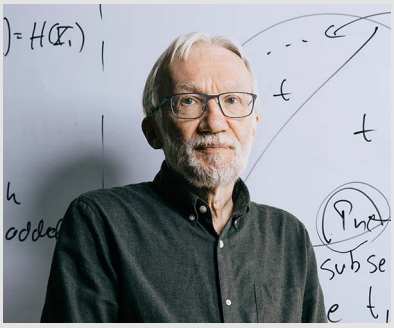


Foto: Liv Rohde, AU foto

Cybersikkerhed: Internettets fundament

Kunsten at sørge for, at kun de rette personer har adgang til den rette delmængde information, er en forudsætning for, at vi kan have et internet. Og dette fundament under internettet har professor Ivan Damgaard beskæftiget sig med hele sin karriere.

■ Carsten R. Kjaer, Aktuel Naturvidenskab.



OM IVAN DAMGAARD

Ivan Damgård er professor i datalogi ved Aarhus Universitet. Han forsker i kryptologi og datasikkerhed og den matematik der ligger bag. Et centralt emne i Ivans forskning er såkaldt multiparty computation – en teknologi der blandt andet kan sikre, at personlige data kun anvendes til de formål som ejeren har godkendt – uden at man behøver at stole på alle de aktører, der indgår.

Ivan er desuden medstifter af virksomhederne Cryptomathic, Partisia og Sepior.

ivan@cs.au.dk

Hvad tænker du, hvis jeg siger "cybersikkerhed"? Du vil måske umiddelbart tænke på hackere. Og deraf følger intuitivt, at forskning i cybersikkerhed må gå ud på, hvordan vi som individer og samfund beskytter os mod "onde" mennesker (eller måske stater), der vil bryde ind i vores computersystemer for at stjæle følsomme data eller overtage kontrollen med computeren. Når Ivan Damgaard på Computer Science i Aarhus tænker på cybersikkerhed, tænker han egentlig ikke så meget på hackere. For ham handler cybersikkerhed om noget mere grundlæggende – nemlig om den sikkerhed, der er nødvendig for, at vi kan have et internet og et digitalt samfund. For langt, langt de fleste af dem, vi skal "beskytte" os mod, er nemlig ikke hackere, men venner og bekendte, bankfolk, internetbutikker, forretningsforbindelser, ansatte i den offentlige forvaltning mv. – ja simpelthen "alle de andre", som vi ikke har lyst til at dele alle vores hemmeligheder med.

»Set i det helt store historiske perspektiv var kryptering oprindelig noget, der primært havde med militæret at gøre. Her var der en fjende, man ikke måtte afsløre hemmeligheder for, og dem, man kommunikerede med, var ens eget "hold", som man stolede på. I dag er verden meget mere kompliceret. Her kommunikerer vi på et internet, hvor alle i princippet kan læse med, hvis ikke vores data er krypterede. Og dem, vi kommunikerer med, deler vi ikke nødvendigvis interesser med. Derfor må vi sikre os, at vi altid kun giver modtagerne netop de informationer, vi ønsker at give dem«, forklarer Ivan Damgaard.

Cybersikkerhed handler om mange ting

Ivan Damgaard er professor i datalogi ved Aarhus Universitet, og han har siden 1980'erne forsket i kryptologi og datasikkerhed og den matematik, der ligger bag. Han er derfor en oplagt guide til at tage os med ind i det maskinrum, hvor fundamentet til nutidens og fremtidens teknikker til at håndtere cybersikkerhed bliver støbt.

Ivan Damgaards hjemmebane indenfor det brogede felt, vi overordnet kalder cybersikkerhed, er kryptologien. Det kan kort defineres som videnskaben om at hemmeligholde og autentificere information. Og det foregår grundlæggende ved at kode information ved hjælp af matematiske procedurer. Det sikrer, at kun den rigtige modtager kan læse informationen, og at ingen kan manipulere med den uden at blive opdaget. Kryptologi udgør derfor en hjørnesten i alt, hvad der har med cybersikkerhed at gøre.

Men cybersikkerhed handler ikke kun om kryptologi.

»Der er for eksempel også en meget praktisk orienteret del af feltet, der handler om, hvordan man sætter systemer op, så de er sikre mod indbrud. Men også sikre mod, at brugerne af et system, der burde være sikkert, tager forkerte beslutninger. Det, vi kalder "human-computer-interaction", forbinder vi normalt ikke med cybersikkerhed, men det bør vi gøre, for mennesker er ofte det svage led i kæden«, fortæller Ivan Damgaard.

Han illustrerer den pointe med, at da vi gik over til MitID i stedet for NemID, skete der et skift i, hvordan folk prøvede at svindle.

»Man gik over til at forsøge at snyde mennesker til at overføre penge. Simpelthen fordi MitID er svært at bryde. Hvis det nemmeste er at snyde mennesket – så er det det, man går efter«, siger Ivan Damgaard.

Er computeren sårbar, når den regner?

Hvis vi vender os mod Ivans eget felt, kryptologien, er det efter hans egne ord der, "hvor man laver værktøjerne". Behovet for krypte-

ring er som nævnt blevet så stort, fordi internettet fungerer, som det gør. Nettet består af en hulens masse computere, og de folk, der sidder bag dem, er alle mulige mennesker med mere eller mindre rent mel i posen. Hvis vi bare sendte vores data ud på nettet, uden at gøre noget ved dem, ville alle kunne se dem – og manipulere med dem.

»Man kan sige, at det, vi laver, er noget, som i første omgang skal lukke alle de store huller – altså så man ikke bare kan sidde derhjemme og høste alle mulige data«, siger Ivan Damgaard. »Den næste bekymring er så hackere. Og hackere findes jo kun fordi, der "nedenunder" nettet findes en hel masse kryptering, der får det til at fungere.«

Som eksempel på, hvad kryptologiske værktøjer skal kunne, nævner Ivan Damgaard, at data også skal være sikre, mens man regner på dem.

»De fleste vil nok tænke, at når en computer regner på nogle data, må disse data også være tilgængelige i computeren, mens den regner. Og så må man jo kunne få fat i de data, hvis man bryder ind i computeren, mens den regner på data. Men det kan vi godt sikre os imod« siger Ivan Damgaard.

Umiddelbart er der to forskellige metoder, man kan anvende. Den ene er, at computeren slet ikke "pakker data ud", når den regner på dem. Man regner altså på krypterede data, og man får dermed også et krypteret resultat, som først åbnes senere. Hvis nogen bryder ind og stjæler data i processen, vil de altså stadig være krypterede. Ivan Damgaard sammenligner metoden med en lukket kasse, hvor man gennem nogle handsker i kassen kan stikke hænderne ind og gøre forskellige ting ved det, der er i kassen – for eksempel trykke på nogle knapper inde i kassen – men selve genstanden i kassen kan man ikke se.

Når computere deler beregninger

Den anden metode kan illustreres med et eksempel. Hvis et flyselskab gerne vil vide, om der findes personer på deres passagerlister, der er terrormistænkte, vil efterretningstjenesten jo ligge inde med en liste over personer, der netop er terrormistænkte. Men hverken flyselskabet eller efterretningstjenesten vil bare udlevere deres respektive lister til den anden part. Så der er brug for en metode, der kan lave en fælles udregning på de samlede data, der kan fortælle, om der er en eller flere personer,

Foto: Colourbox

SUKKERROER SATTE GANG I MULTIPARTY COMPUTATION

Da Ivan Damgaard og kolleger i 1980'erne udviklede princippet i at regne på delmængder af fælles data på tværs af mange computere – multiparty computation – var det ren grundforskning. Her fandt de blandt andet også matematiske svar på, hvor mange indbrud, man maksimalt kan tåle, for at systemet stadig er sikkert.

Først i løbet af nullerne begyndte man for alvor at interesse sig for mulige praktiske anvendelser. Og i 2008 så den første industrielle anvendelse dagens lys – og det var i Danmark.

Baggrunden var behovet for en handelsplads, hvor man kunne købe og sælge kontrakter, som gav en landmand lov til at producere et bestemt antal tons sukkerroer med støtte fra EU. I 2006 var der en reform af EU-støtten til sukkerproduktion, hvilket reducerede støtten, og derfor opstod der et behov for i en fart at få flyttet produktionen hen til områder, hvor det bedre kunne betale sig at dyrke sukkerroer (støtten havde i udgangspunktet været så stor, at det kunne betale sig næsten overalt). Når man skulle handle på denne handelsplads, var det vigtigt, at det beløb, man ønskede at købe eller sælge for, forblev privat information. Opgaven var altså at finde ud af, hvem der skulle handle med hvem, uden at buddene blev afsløret for andre.

Det lykkedes ved hjælp af multiparty computation, og det var det første eksempel i virkelighedens verden på brug af denne teknik. Og det gav mange andre blod på tanden. Det udmøntede sig også i spin off firmaet Particia, som stadig findes i dag.

Der er siden sket en kæmpemæssig udvikling i hastigheden af disse løsninger, og mange virksomheder arbejder med udvikling af metoderne. For eksempel har industrigiganten Bosch en forskningsafdeling, der arbejder med det i forhold til forsyningskæder – altså hvordan man flytter varer rundt, uden at alle, der er med i kæden, skal offentliggøre deres forretningsstrategier. ■

Tegning: Susanne Rauff Møller

KAN MAN LYTTE SIG TIL DATA?

Hvis man vil stjæle data fra en computer, skal man bryde ind i den. Men er det nu også nødvendigt? Faktisk er det et af de spørgsmål, man bliver nødt til at overveje inden for cybersikkerhedsforskningen. For det kan jo være, at man ved at måle på computeren udefra – for eksempel på lyden eller på strålingen fra den, når den regner på data – kan afsløre noget om de data, den regner på. Der findes ifølge Ivan Damgaard eksempler på eksotiske angreb, hvor man netop har forsøgt at laver den slags målinger på computere. Derfor er der også brug for teknikker til at beskytte os mod det. Det kan for eksempel være at sørge for, at computeren bruger lige lang tid på at regne på data, uanset hvad den regner på. ■

	Per	Ulla	Hans	Signe	Løn	Gennemsnit:
Per	10000	2000	20000	18000	50000	
Ulla	3000	-5000	33000	24000	55000	
Hans	11500	9000	13000	15500	49000	
Signe	6000	-33000	48000	31000	52000	
Sum	30500	-27000	11400	88500	20600	51500

HEMMELIGE BEREGNINGER I FÆLLESSKAB

Hvordan kan flere personer være fælles om en udregning uden at afsløre information for hinanden? Lad os sige, at medarbejderne i en afdeling i en virksomhed gerne vil vide, hvad gennemsnitslønnen er i afdelingen, men de har ikke lyst til at afsløre, hvad netop de selv får i løn. Skemaet viser et eksempel med fire medarbejdere. Tricket er, at hver enkelt medarbejder deler sin egen løn op i et antal tilfældige tal (svarende til antallet af medarbejdere – her fire), der tilsammen summerer op til ens faktiske løn. Det ene tal beholder man selv (markeret med rødt i tabellen), mens man sender et af de andre tal til hver af de andre tre personer. Derefter lægger hver enkelt person de fire tal sammen, som de nu sidder med, og sender resultatet til alle de andre. Det smarte er nu, at hvis man lægger de fire beregningsresultater sammen, giver det den samlede løn i afdelingen (grøn) – og så skal man bare dividere med fire for at få gennemsnitslønnen. ■

der står på begge lister. Uden at afsløre andet end det. Princippet bag, at en beregning kan udføres på flere computere, som hver især kun har adgang til en delmængde af data – kaldet multiparty computation – udviklede Ivan Damgaard og hans kolleger allerede tilbage i 1980'erne.

»Dengang var det ren grundforskning,« siger Ivan Damgaard. »Vi var bare nysgerrige på, om det overhovedet kunne lade sig gøre. Ingen troede dengang på, at det ville komme ud og blive anvendt i praksis. Det var alt for langsomt og teoretisk. Men i 2008 var vi faktisk med til at udvikle verdens første løsning, hvor metoden blev brugt i praksis – nemlig til at handle sukkerroe-kontrakter i Danmark.« (se faktaboks).

I dag er værktøjer til multiparty computation vidt udbredte. For eksempel har Google en tjeneste, hvor de samler data ind fra mistænkelige steder, hvor huggede passwords er til salg på nettet. Google har derfor en stor database med lækkede passwords og en tjeneste, hvor man selv kan tjekke, om nogle af ens passwords findes på den liste. Vel at mærke uden at du skal sende alle dine passwords til Google.

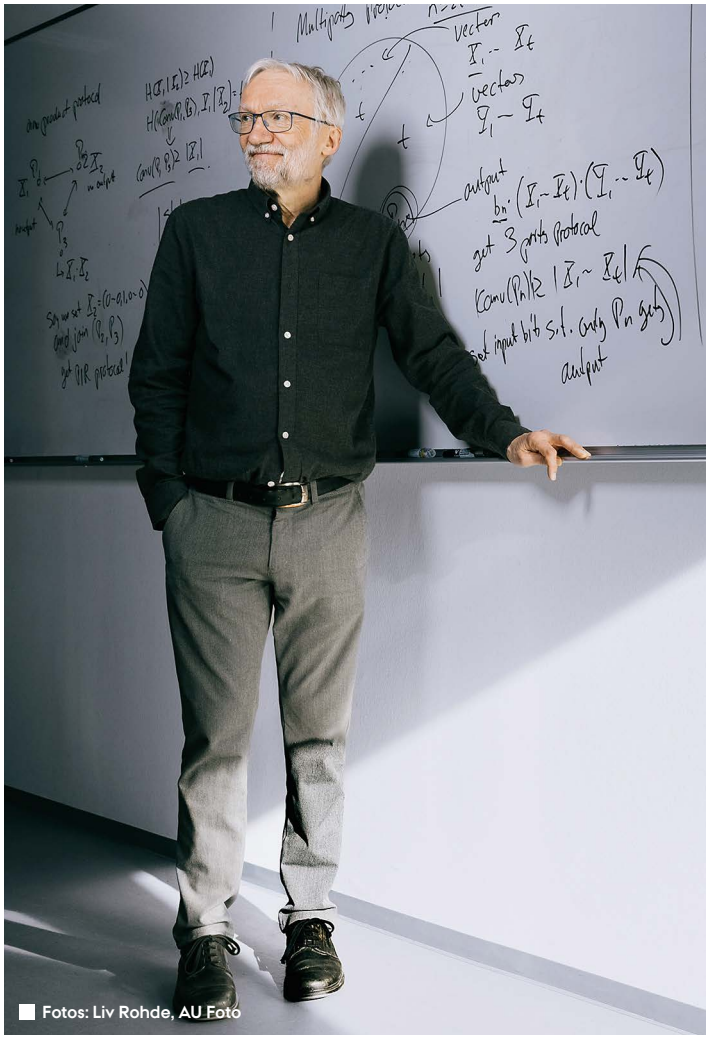
»Teknikken har selvfølgelig en pris: Sådanne beregninger kan ikke foregå lige så hurtigt, som hvis alle data var samlet i én computer. Det betyder i praksis, at vi ikke kan regne på "big data" på denne måde – men mellemstørrelse kan vi,« siger Ivan Damgaard.

Der foregår derfor også stadig udvikling indenfor feltet, der går ud på at kunne udføre den type beregninger hurtigere og mere effektivt.

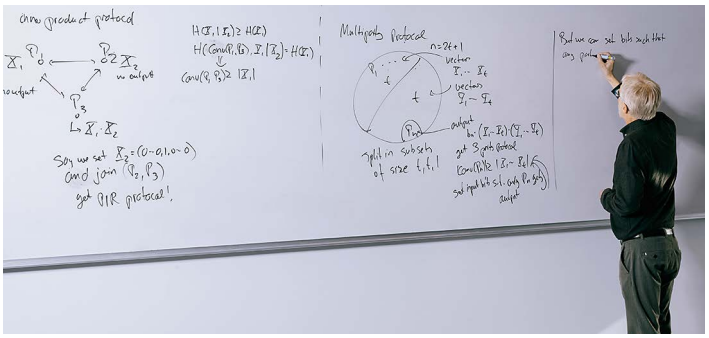
Truslen fra kvantecomputeren

Et af de store områder indenfor forskningen i cybersikkerhed handler om den potentielle trussel fra kvantecomputere. Kryptering er traditionelt bygget på en type matematisk bevis, som er meget vanskelig for en almindelig computer at løse, nemlig såkaldt faktorisering. Det tager udgangspunkt i, at det er meget vanskeligt at regne ud, hvilke to primtal, der ganget med hinanden giver et bestemt tal – for eksempel at tallet 8051 fremkommer ved at gange 83 med 97 (til gengæld er det meget nemt at kontrollere, at 83 ganget med 97 netop giver 8051). Jo større tal, jo sværere er det.

Problemet er nu, at en kvantecomputer i princippet er rigtig god til at regne lige præ-



Fotos: Liv Rohde, AU Foto



»For det mest grundlæggende – det der skal til, for at internettet kan fortsætte sine daglige funktioner – er løsningerne stort set på plads«.

cis den type matematiske problemer ud. Hvis det lykkes at udvikle kraftfulde kvantecomputere, vil utallige systemer verden over derfor være i fare for at blive hacket.

For at imødegå denne trussel, bliver vi derfor nødt til at bygge kryptering på beregningsproblemer, der er vanskelige at løse for en kvantecomputer — og som kan køre på helt almindelige computere. Sådanne krypteringsteknikker findes allerede.

»I princippet er denne overgang til "post quantum computing" en 1:1-udskiftning«, siger Ivan Damgaard. »I forskningsmiljøet er der allerede udviklet flere sæt af værktøjer, som er på vej ud i praktisk brug. For eksempel har et team i min egen forskningsgruppe foreslået en ny kvantesikker digital signatur, der lige nu evalueres af den amerikanske standardiseringsmyndighed NIST. Får den grønt lys dér, ender den næsten med garanti som industristandard — og dermed i alt fra offentlige systemer til private virksomheder verden over.«

Et gigantisk opgraderingsprojekt

Selvom teknologien findes, er det langt fra ligetil at få hele internettet over på kvantesikre løsninger. Der er utallige systemer, enheder og protokoller, som skal opdateres — både hardware og software.

Et eksempel er internetprotokollen TLS, som sikrer, at man kan browse sikker på nettet – den er aktiv, når du ser et lille hængelås-symbol i adresselinjen i din browser. Hvis en server bruger den nyeste version af denne protokol, er de kvantesikre algoritmer faktisk allerede indbygget. Browserne Chrome, Firefox og mange andre bruger den automatisk — hvis serveren i den anden ende altså understøtter det.

Problemet er bare, at der er et enormt efterslæb. Mange systemer ude i verden er ikke blevet opdateret endnu, og det kan tage år at få dem alle med.

»For det mest grundlæggende — det der skal til, for at internettet kan fortsætte sine daglige funktioner — er løsningerne stort set på plads. Standarder er på vej, og mange er begyndt at implementere dem. Men for de mere avancerede funktioner er der stadig store udfordringer,« siger Ivan Damgaard.

Han forklarer, at det for eksempel gælder mange af de små enheder, hvor softwaren er indbygget i hardwaren, og som for eksempel indgår i det, vi kalder "internet of things" (IoT). Udfordringen er her, at de nye kvantesikre algoritmer typisk fylder langt mere end de gamle, og så er der simpelthen ikke plads til at skifte dem ud. Det kommer til at give hardwareproducenterne designproblemer – medmindre forskere kan gøre algoritmerne meget mere kompakte, eller måske finde helt andre løsninger.

En stor forskningsopgave venter

»En anden udfordring er de systemer, hvor en hemmelig nøgle er fordelt mellem flere enheder – som telefon, computer og server. Det gør man for at undgå, at man kan hacke et system ved at bryde ind et enkelt sted. I dag fungerer løsninger på den slags kryptering elegant i klassiske systemer, men i kvantesikre algoritmer kan den samme proces ikke udføres lige så smidigt. Der er derfor behov for helt nye metoder,« siger Ivan Damgaard.

Endelig nævner han også systemer, der bygger på såkaldte zero-knowledge-beviser (det er også den type bevis, der ligger bag eksemplet med flyselskabet og terrormistænkte ovenfor). Det er teknologi designet til, at man kun afslører netop den delmængde af en større mængde information, som man ønsker. Det er i øvrigt også en teknik, der er vidt anvendt i hele block chain-sektoren (som jo blandt andet anvendes til kryptovaluta).

I øjeblikket arbejder EU på en fælles digital identitet – en såkaldt EU-wallet. Den skal EU-borgerne kunne bruge til at bevise ting om sig selv – for eksempel, at de er over 18 år og borgere i et EU-land – uden at afsløre mere end nødvendigt. Men også i den type systemer gælder det, at traditionelle algoritmer kører meget effektivt, mens de kvantesikre versioner bliver langt tungere. Der forestår derfor en stor forskningsopgave i at gøre dem brugbare i praksis.

Vi skal i gang nu!

I virkeligheden er der ingen der ved, hvornår – eller om der nogensinde – bliver udviklet en fungerende kvantecomputer, der vil kunne bryde de eksisterende krypteringsalgoritmer.
Men som Ivan Damgaard forklarer det, bliver vi nødt til at forberede os på det.

»Spørgsmålet er, hvordan vi forholder os til en sandsynlighed på for eksempel 10 % for, at der findes en kvantecomputer, der kan bryde vores nuværende kryptering i midten af 2030'erne. Den sandsynlighed kan lyde lav, men konsekvensen vil jo være en form for digital kollaps til den tid, hvis ikke vi har gjort noget i mellemtiden. Og det vil tage mindst ti år at gøre vores systemer kvantesikre, så derfor skal vi i gang nu.« ■