Kryptolog-mangel: – I fjor ble det bare to nordmenn som tok doktorgrad i kryptologi. Vi trenger mange flere, sier Tjerand Silde som er førsteamanuensis og forskningsgruppeleder for NTNU Applied Cryptology Lab. FOTO: TORMOD HAUGSTAD

Skker nøkkel: Tjerand Silde er deltidsansatt i det Oslo-baserte selskapet Pone Biometrics som er i ferd med å lansere kvantesikker autentisering gjennom systemet Offpad som baserer seg på fingeravtrykk fremfor passord. FOTO: HANS HAUGSTAD

SKAL SIKRE OSS MOT KVANTEDATA-MASKINER

All informasjon som stater har samlet inn via nettsnoking i dag vil kunne leses i fremtiden om den er aldri så godt kryptert.

TEKST
ODD RICHARD VALMOT
orv@tu.no

Kvantedatamaskiner lover oss en ufattelig økning av regnekraften på visse beregninger. Vi vil få bedre værmeldinger og masse andre resultater som vi i dag bruker superdatamaskiner til, eller rett og slett ikke har datakraft til. Dessverre gjelder dette også evnen til å dekryptere informasjon som er lagret med dagens mest avanserte teknologi.

I dag har vi det såkalte RSA-kryptosystemet som brukes til å kryptere og signere dokumenter slik at de ikke kan leses av uvedkommende og at utstederen kan verifiseres. Teknologien er basert på at det benyttes en algoritme basert på en offentlig og en privat nøkkel. Den offentlige kan gis ut til alle, men den private holdes hemmelig. Det er en matematisk forbindelse mellom den offentlige og private nøkkelen, men det er umulig å utlede den private fra den offentlige. Hvis informasjon krypteres med den offentlige nøkkelen, kan den bare leses av den som har den private nøkkelen.

SIKKERT SYSTEM, ENNÅ

RSA-kryptering er regnet som helt sikkert i dag. Spesielt nå det brukes nøkler med svært mange bits.

– Vi tror dagens teknologi vil være sikker i veldig mange år ennå, men det er skyer på himmelen. Den kraften som følger med utviklingen av såkalte kvantedatamaskiner, kan brukes til å dekryptere den informasjonen som er kryptert med dagens metoder, sier Tjerand Silde som er førsteamanuensis ved NTNUs Institutt for informasjonssikkerhet og kommunikasjonsteknologi.

Men han understreker at det vil ta tid. Kvantedatamaskiner er helt i starten og det vil ta mange år, kanskje flere tiår, før de er kraftige nok til å knekke dagens kryptering.

– Da høres det kanskje ikke så ille ut, men husk at veldig mange stater har tappet nettet og lagret enorme informasjonsmengder. Også den som er kryptert. Det betyr at stater som Russland, Kina og andre land vil kunne lese denne informasjonen når de får tilgang til nok kvantemaskinkapasitet.

Mange norske virksomheter har utrykt bekymring for sikkerheten til informasjon vi hittil har kunnet stole på. Finansielle transaksjoner, helsedata og svært mye annen informasjon vil være utsatt når den nye teknologien for å dekryptere er på plass.

KVANTESIKKER KRYPTERING

Fordi informasjonen som er lagret kryptert med dagens teknologi må ansees som potensielt tapt i fremtiden, arbeides det med ny såkalt kvantesikker kryptering. Det foreligger allerede forslag til en standard som kan benyttes i dag. Planen er at den nye standarden skal endelig vedtas neste år. Men selv om standardene kommer på plass, vil det neppe bli krav om at all offentlig informasjon skal krypteres kvantesikkert med en gang, men for eksempel innen slutten av tiåret.

– Jeg mener at vi bør bytte ut RSA i dag, både for nøkkelutveksling/kryptering og for signaturer, mot kvantesikre alternativer. Den nye standarden vil bestå av en krypteringsalgoritme og tre signaturalgoritmer. Brukeren kan selv velge hvilken signatur som skal benyttes, de er like sikre, men har ulike fordeler og ulemper med tanke på tid og størrelser og minnebruk, sier Silde.

«Vi bør bytte ut RSA i dag, både for nøkkelutveksling/ kryptering og for signaturer, mot kvantesikre alternativer»

Tjerand Silde, førsteamanuensis ved NTNUs Institutt for informasjonssikkerhet og kommunikasjonsteknologi

PÅ VANLIGE DATAMASKINER

Selv om kvantesikker kryptering skal beskytte informasjon mot den enorme regnekraften kvantedatamaskiner kan tilby, er det ikke slik at man trenger tilsvarende økning i datakraft for å kryptere data på en sikker måte.

– Vi kommer til å bruke vanlige datamaskiner til å kryptere informasjonen. Riktignok snakker vi om en hundredobling av informasjonen, men det er bare den som går med til selve krypteringen. Det aller meste av det som lagres eller sendes, er selve informasjonen. Det som kommer til å bli et problem er når små IoT-enheter som sender veldig små datamengder skal gjøres kvantesikre. Da kan mengden data som går med til sikring av informasjonen langt overgå datamengden som må beskyttes. Dagens IoT-enheter er ikke bygget for slike oppgaver, sier Tjerand Silde.

Selv om fremtiden til dagens krypterte informasjon ser mørk ut, vil det ta lang tid før den kan dekrypteres. Silde mener det vil være behov for maskiner som kan håndtere 20 millioner såkalte qubits, som er en vanlig måte å indikere kvanteytelse på. Problemet kan ligge flere tiår fram i tiden uten at det bør være en sovepute.

AUTENTISERING

– Dagens kvantedatamaskiner er på noen titalls qubits og mange av de går med til å korrigere for støy, som er et problem når vi bruker kvantefysikken til regnekraft. Derfor skiller vi mellom logiske og fysiske qubits. Slik er det jo ikke med dagens prosessorkraft, sier Silde.

Han jobber deltid i selskapet Pone Biometrics som allerede tilbyr kvantesikker autentisering gjennom programvaren Offpad. Men selv om den er aldri så fremtidssikker, understreker han at slik teknologi ikke på noen måte er en tryllestav som fikser all datasikkerhet.

– Dette hjelper ikke mot slike banale feil som at noen klikker på en lenke de ikke burde gjøre, eller blir lurt til å gjøre ting via nettet og en rekke andre former for dataangrep. Her finnes det andre verktøy som fungerer i dag og som gir bedre sikkerhet, slik som Offpad, som er laget for også å være phishing-resistent, i tilfellet folk blir lurt til å logge inn på feil nettsider og gi fra seg passord og lignende, sier han. ●