FFI-RAPPORT

19/02042

Kryptografisk sikring av autonome og ubemannede enheter

— eksisterende forskning

Martin Strand
Jan Henrik Wiik

Kryptografisk sikring av autonome og ubemannede enheter

– eksisterende forskning

Martin Strand
Jan Henrik Wiik

Forsvarets forskningsinstitutt (FFI) 8. november 2019

Emneord
Kryptografi
Informasjonssikkerhet
Ubemannede systemer
Autonomi

FFI-rapport
19/02042

Prosjektnummer
1472

Engelsk tittel
Securing autonomous and unmanned devices cryptographically – existing research

Elektronisk ISBN
978-82-464-3232-8

Godkjennere
Nils Nordbotten, *fungerende forskningssjef*

Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur.

Sammendrag

Stadig flere oppgaver skal løses med autonome og ubemannede enheter. Slike enheter kan utføre farlige oppdrag i både militær og sivil sektor uten å sette mennesker i fare, men samtidig gir det nye utfordringer for informasjonssikkerhet.

Formålet med denne rapporten er å se nærmere på hvordan vi kan sikre autonome og ubemannede enheter. Det er en rekke sikkerhetselementer en da må ta hensyn til. Vi har tatt utgangspunkt i følgende mål:

- Sikre kommunikasjonen til og fra enheten slik at uautoriserte ikke kan avlytte sensitiv informasjon (konfidensialitet).
- Sørge for at endringer i kommunikasjonsstrømmen blir oppdaget (integritet).
- Sikre at avsenderen virkelig er den som den utgir seg for å være. Mottakeren skal bare kunne godta meldingen dersom riktig avsender kan verifiseres (autentisitet).
- Sørge for at all informasjon som blir lagret på enheten, fortsetter å være sikker dersom enheten går tapt.
- Sørge for at alle sensitive data som prosesseres på enheten, for eksempel kart- og sensordata, blir ivaretatt på best mulig måte.

I denne rapporten går vi gjennom et utvalg av litteraturen som beskriver sikring av autonome og ubemannede enheter. Vi har særlig sett etter overordnede beskrivelser, definisjoner og løsninger. Resultatene kan dermed anvendes for å løse utfordringer som er felles for alle autonome enheter. Det er publisert lite forskning på feltet, så vi har utvidet søket til også å omfatte mobile ad hoc-nettverk, mobile sensornettverk og tingenes internett (IoT).

Litteraturen er sortert i tre hovedgrupper:

- Sikkerhetsmodeller: Hvordan andre forskere har resonnert rundt deltakere i et større system, sikkerhetskrav og tillitsantagelser.
- Kryptografiske algoritmer for lettvektsanvendelser: Hvilke algoritmer egner seg best når de skal brukes på enheter som har begrensninger som lav båndbredde, eller lite strøm, lagring eller prosesseringskraft.
- Praktiske forsøk: Enkelte forsøk med sikring av små enheter har blitt dokumentert i akademisk forskning, med interessante avveininger og resultater.

Hovedkonklusjonen er at forskningsfeltet fortsatt er umodent, og at det nødvendige teoretiske grunnlaget mangler. Vi ser likevel at det finnes beslektet arbeid fra kryptografien som det kan bygges videre på, og dessuten at de praktiske forsøkene er et godt utgangspunkt for videre arbeid.

Summary

An increasing number of missions are assigned to autonomous and unmanned devices. Such devices can carry out dangerous tasks in both military and civilian sector without jeopardising human lives. However, it raises new challenges for information security.

The purpose of this report is to look closer into how we can secure autonomous and unmanned devices. There are a number of security concerns to take into account. Our starting point is found in the following goals:

- Secure communications to and from the device so that unauthorised parties are unable to listen to sensitive information (confidentiality).
- Ensure that changes injected in the communication will be detected (integrity).
- Guarantee that the sender is the one it claims to be. The recipient should only accept the message if the sender can be verified (authenticity).
- Ensure that all information stored on the device remains secure if the device is lost.
- Securely process data on the device – e.g. map and sensor data.

We survey a selection of the available literature on how to secure autonomous and unmanned devices. We have in particular searched for general descriptions, definitions and solutions. The results are therefore applicable to common challenges for all autonomous devices. The body of published research on this exact field is small, and so the search was expanded to include mobile ad-hoc networks, mobile sensor networks and the internet of things (IoT).

The literature is sorted into three main groups:

- Security models: How other scientists have reasoned about players in a system, security requirements and trust assumptions.
- Cryptographic algorithms for lightweight applications: Which algorithms are best suited when used on devices with restrictions on bandwidth, power, storage or processing power.
- Practical experiments: Some attempts to secure small devices have been documented in academic research and showcase interesting considerations and results.

Our main conclusion is that the field of research is immature and lacks the necessary theoretical foundation. We do however find that there is related cryptographic work which can be built upon. The practical experiments are by themselves a good starting point for further work.

Innhold

Sammendrag 3

Summary 4

1 Innledning 7
- 1.1 Forutsetninger og avgrensninger 8
- 1.2 Organisering av rapporten 8

2 Arbeid med sikkerhetsmodellering 9
- 2.1 Bakgrunn: Sikkerhetsmodellering i kryptografien 9
- 2.2 Vurderte arbeider 9
- 2.3 Vår vurdering av modelleringslitteraturen 13

3 Artikler om algoritmer 14
- 3.1 Om kvantedatamaskiner 14
- 3.2 Symmetriske teknikker 14
- 3.3 Asymmetriske teknikker 17
- 3.4 Vurdering av aktuelle algoritmer 17

4 Praktiske forsøk fra akademisk forskning 18

5 Konklusjon 19
- 5.1 Videre arbeid 19

Ordliste 21

Referanser 23

1 Innledning

Det er høy oppmerksomhet rundt autonome og ubemannede plattformer. Slike systemer kan utføre farlige oppdrag i både militær og sivil sektor uten å sette mennesker i fare, men presenterer nye utfordringer for informasjonssikkerhet. Enhetene kan potensielt trenge gradert informasjon for å utføre oppdraget, og det er viktig at en enhet kan forsikre seg om at potensielle kommandoer kommer fra riktig avsender, uten å ha blitt endret på veien. Samtidig er det alltid en risiko for at enheten blir tatt til fange av uvedkommende, og de skal ikke kunne nyttiggjøre seg noe av informasjonen som er skissert over.

Vi ønsker å sikre autonome og ubemannede enheter med utgangspunkt i tre mål:

- Kommunikasjon til og fra enheten må sikres slik at uautoriserte ikke kan avlytte sensitiv informasjon (konfidensialitet), at man kan være trygg på at informasjonen er mottatt slik den var sendt (integritet), og at avsenderen virkelig er den som den utgir seg for å være (autentisitet).
- Når informasjon lagres på enheten, må den være kryptert slik at en motstander som overtar enheten ikke kan avlese informasjon.
- Hvis data skal prosesseres på enheten, hvordan kan det gjøres slik at beregningen på best mulig måte ivaretar sensitive opplysninger?

Det første punktet kan trenge litt motivasjon. Autentisitet er viktig uavhengig av kommunikasjonsform, men helt spesielt mellom maskin til maskin. Et menneske som mottar en ordre, vil intuitivt kunne oppdage dersom det er noe ved meldingen som opplagt ikke stemmer, som for eksempel at den er uleselig, selvmotsigende eller rett ut helt urimelig. Et eksempel kan være hvis oppdraget er å være livvakt for A, og den nye ordren sier at man skal angripe A. Dersom meldingen likevel går gjennom autentitetssjekken, kan man mistenke at kanalen har blitt kompromittert, og at man derfor dobbelsjekker på en annen måte. En maskin kan ikke gjøre den samme vurderingen, så det er desto viktigere å sikre at meldingen ble levert slik den var ment fra avsender. Dersom den har blitt endret, skal det oppdages og meldingen forkastes.

Et første skritt i dette arbeidet er å kartlegge eksisterende akademisk forskning på feltet. Som en del av kartleggingsarbeidet har vi også sett etter gode løsninger fra trådløse sensornettverk og tingenes internett. Det er domener som deler mange av de samme egenskapene og utfordringene som sikring av autonome enheter. I denne litteraturstudien har vi særlig sett etter overordnede beskrivelser, definisjoner og løsninger. Resultatene kan dermed anvendes på utfordringer alle autonome enheter har felles, framfor å være spesialisert på for eksempel flyvende droner, stasjonære sensorer eller undervannsfarkoster. Spesielt må man ta hensyn til at enhetene skal behandle gradert informasjon, samtidig som de kanskje skal opptre langt utenfor et område man selv kontrollerer. Da må man forvente at en motstander kan få tak i komplette enheter, og analysere dem mens de fortsatt er fullt funksjonable. En tilfredsstillende løsning bør tåle et slikt scenario.

Forskningslitteraturen er svært rik når det handler om å beskytte en enkelt kanal mellom to datamaskiner. Imidlertid er det flere kompliserende faktorer som melder seg når det blir mange enheter i samme nettverk, og spesielt når båndbredde, batterikapasitet og begrenset maskinvare gjør at man kanskje ikke kan bruke de løsningene som er i utstrakt sivil bruk i dag.

1.1 Forutsetninger og avgrensninger

Denne rapporten er primært et litteraturstudium, der artikler blir omtalt og vurdert med bakgrunn i et ønske om å finne egnede løsninger for å sikre autonome og ubemannede enheter. Mange slike enheter skal bruke minst mulig strøm, eller er avhengig av å sende så små datapakker som mulig. Vi har derfor bare gått inn i publiserte arbeider som omhandler enheter med begrensninger på ytelse eller båndbredde. Dersom man utvider søket til å inkludere systemer som er like kraftige som kontormaskiner, så er det umiddelbart en rekke andre verktøy som er tilgjengelige, og ville ført til en rapport som mer minnet om en lærebok i kryptografi enn en utforsking av hva som er gjort for å gi tilfredsstillende sikring av små enheter. At denne rapporten er kort, er i seg selv en indikasjon på hovedfunnet.

I utgangspunktet legger vi til grunn Dolev-Yao-modellen [12], som tilsier at man må betrakte nettverket for å være under motstanderens kontroll. Det innebærer at det er motstanderen som er ansvarlig for å levere meldinger, og kan overvåke, lese og modifisere all trafikk som ikke er tilstrekkelig beskyttet. Motstanderens beste strategi er som regel ikke å stanse all trafikk – da blir man oppdaget og kan stenges ute – så man kan anta at så godt som alle meldinger blir levert, men en konsekvens er at man bør ha mekanismer som garanterer for meldingsrekkefølgen og som gjør at man oppdager pakketap.

Vi antar som utgangspunkt at alle algoritmer og protokoller er offentlig kjent, og sikkerheten skal dermed utelukkende være avhengig av at nøkkelen holdes hemmelig. Det er mye enklere å skifte ut en kompromittert nøkkel, enn å skifte ut et helt kryptosystem fordi det inneholdt svake elementer som ikke tålte dagens lys.

Videre vil man fra et kryptologisk ståsted normalt anta at en motstander som overtar en enhet, er i stand til å lese ut all data, og potensielt overta styringen av den uten at det kan oppdages. Alt som ikke er kryptert – nøkler inkludert – vil dermed falle i motstanderens hender. Matematikken som ligger bak kryptologi kan gjøre mye, men kan ikke gi fullgod beskyttelse mot fysisk påvirkning av systemet. Et vellykket resultat er dermed ubetinget avhengig av vellykket tuklebeskyttelse (*tamper protection*), et helt eget forskningsfelt. Vi går ikke inn i det faget her, men noterer *a priori* at det er et samspill som kryptografien er avhengig av.

1.2 Organisering av rapporten

Rapporten er organisert i tre kapitler mellom innledningen og konklusjonen. Kapitlene deler forskningen vi har vurdert i tre hovedkategorier. I kapittel 2 diskuterer vi det som er gjort av formelt sikkerhetsmodelleringsarbeid. Deretter følger det en gjennomgang av artikler om lettvektskryptografi i kapittel 3 og reelle forsøk fra litteraturen i kapittel 4. Kapittel 5 inneholder konklusjoner og en oppsummering av hvilket arbeid som er nødvendig for veien videre.

2 Arbeid med sikkerhetsmodellering

For å få god sikkerhet er det først nødvendig å ha et klart bilde av hva man ønsker å forsvare, og mot hvem. Derfor er det nødvendig å gjøre et grundig arbeid med modelleringen. Det er vanlig å si at kryptografiske algoritmer skal sikre konfidensialitet, og ivareta integritet og autentisitet av data. Ved analyse av flere enheter som skal kommunisere blir det likevel et for grovmasket krav. For eksempel kan det hende at kommunikasjonen mellom enhet A og B blir kompromittert, men det skal i seg selv ikke føre til at ikke enhet B og C kan opprettholde sikker kommunikasjon.

I dette kapittelet går vi gjennom og diskuterer de arbeidene som er relevante for å lage en kryptologisk sikkerhetsmodell for autonome enheter.

2.1 Bakgrunn: Sikkerhetsmodellering i kryptografien

Vi starter med en kort beskrivelse av sikkerhetsmodelleringen i kryptografifaget. Vi gjør det ved å oppsummere et arbeid av Do, Martini og Choo [11]. Forfatterne har gått gjennom modelleringen av motstandere i kryptografi, mobiltelefoner og tingenes internett (*Internet of Things*, IoT). Inspirert av arbeidet som er gjort innen kryptografi, kommer de med anbefalinger til forskere som jobber i de to andre feltene.

Modelleringstradisjonen i kryptografi startet med Dolev og Yao [12], som beskrevet i innledningen. Arbeidet har blitt videreført av Bellare og Rogaway [5], og i talløse arbeider siden. Bellare og Rogaway introduserte ideen at motstanderen kunne sende *spørringer* til parter i nettverket, som for eksempel *Send* (en melding), *Reveal* (en nøkkel) eller *Corrupt* (som tar over kontrollen av en node). Det modellerer blant annet virkningen av å ha en utro tjener i organisasjonen.

Kryptografi-litteraturen tar i mindre grad hensyn til fysiske angrep, noe Do et al. nevner som en svakhet. Like fullt konkluderer de med at «[o]ther security-based research should look to cryptographic protocols as the gold standard for adversary models (...)». Like positive er de ikke til tilstanden i IoT-domenet: «IoT security, particularly, is a research field in its infancy.»

Forfatterne avslutter med tre anbefalinger for IoT-sikkerhetsmodellering:

1. Gjør konkrete antagelser om miljøet som enhetene skal brukes i.
2. Definer klart hva motstanderen må oppnå for å vinne.
3. Spesifiser nøyaktig hvilke kapabiliteter man antar at motstanderen har.

Dersom motstanderen gis sterkere kapabiliteter enn det man regner som realistisk, og man lykkes i å bevise at systemet like fullt vil være sikkert – at motstanderen ikke kan oppnå målene sine – vil man ha en sterk og etterprøvbar garanti for den operative bruken.

2.2 Vurderte arbeider

Det finnes lite forskning rettet direkte mot sikkerhet i autonome farkoster. I litteratursøket løftet vi derfor også blikket mot trådløse sensornettverk (*Wireless sensor networks, WSN*) og enheter

i tingenes internett. Fellesnevneren for autonome farkoster, trådløse sensornettverk og tingenes internett er at man kan ha et stort antall billige enheter, og som potensielt kan være til dels kraftig begrenset med tanke på beregningskraft, båndbredde og strømforsyning.

En del artikler ser ut til å hente inspirasjon fra arbeidet som er gjort med mobile ad-hoc-nettverk (MANET). Det er naturlig, siden slike nett i prinsippet er autonome. Vi vil dra fram en betraktning fra Sauverons presentasjon av et arbeid med sikkerhet i svermer av autonome enheter, og som vi kommer tilbake til senere. Der hevdes det at det ikke er tilstrekkelig med sikkerhetstiltakene fra MANET, som for eksempel at enhetene kan opptjene omdømme (*reputation*) ved å opptre i henhold til protokollen over lang tid. Vi må tvert i mot gå ut fra at en enhet under motstanderens kontroll vil opptre fullt og helt i henhold til protokollen til den gjennomfører angrepet sitt, og da er det for sent å redusere renommeet. Tilsvarende, om man skal ekstrapolere Sauverons argument, må man aldri kunne la en enhet som har opptrådt i strid med protokollen sin få tilbake tillit.

Vi går nå gjennom de aktuelle arbeidene som behandler sikkerhetsmodellering, artikkel for artikkel.

Marzi og Marzi [22] ønsker å sikre trådløse sensornettverk, og legger til grunn et tillitsbasert system, der nodene i nettverket i fellesskap beregner hvilke andre noder de har tillit til. Det er to hovedtilnærminger: Den første er en modell inspirert fra biologi, der «maur» legger igjen «feromoner», og som samlet sett gir en ideel vei gjennom grafen av enheter. Den andre er basert på en nodes vurdering av alle sine naboer.

For begge modellene mangler det imidlertid en analyse av hvilke antagelser man kan gjøre om motstanderens evner, og modellen går dermed implisitt ut fra at angriperen vil gi fra seg noen hint om at ikke alt er som det skal, som igjen fører til nedsatt tillit til de relevante nodene.

Pathak og Patil [25] har forsøkt å beskrive hvordan man kan håndtere roaming-problemet på en effektiv måte; hvordan en node kan flytte seg fra dekningsområdet rundt én node og til en annen, og med minimal overhead for reautentisering i nettverket. Forfatterne lister pseudokode som skal implementere denne funksjonaliteten.

Det følger ikke med noen analyse av sikkerheten i systemet gitt av pseudokoden, og det måles heller ikke opp mot noen forhåndsdefinerte mål. Forfatterne går videre ikke inn på hvordan mekanismene fungerer i eksisterende nettverk, som for eksempel WiFi og GSM.

I et – formelt sett upublisert – manuskript fra 2013 går Sen [29] gjennom sikkerhetsutfordringen i trådløse sensornettverk over flere nivå: iboende begrensninger, sikkerhetskrav, aktuelle sårbarheter og mulige løsninger. Artikkelen gir en omfattende oversikt over problemer og løsninger.

Begrensningene har vi også vært innom over, men det er verdt å dra fram opplysningen om at hver enkelt *bit* som skal sendes kan koste like mye strøm som å utføre mange instruksjoner [16, 29]. Det innebærer at minimering av kommunikasjonen ikke bare er viktig dersom det er overføringskapasiteten som er lav, men også når strøm er den kritiske ressursen. Den konkrete vurderingen kommer an på utstyret som skal brukes.

Sen lister opp følgende sikkerhets- og funksjonalitetskrav som de viktigste. Vi inkluderer en løs beskrivelse av hver til bruk i senere diskusjon.

Datakonfidensialitet Dersom dataene sendes via en nabonode, skal den ikke kunne lese data med mindre den eksplisitt er autorisert til det, og tilstrekkelig mye data må krypteres for å beskytte mot trafikkanalyse. Uvedkommede skal selvsagt ikke kunne tolke noe av den krypterte dataen.

Dataintegritet Ingen melding skal kunne endres [uten at det kan oppdages] mens den er i transport mellom avsender og mottaker.

Tilgjengelighet Tjenestene i nettverket skal være tilgjengelige selv om systemet er under angrep, for eksempel fra et *Denial of Service*-angrep (DoS).

Ferske data Mottatte data skal være sendt nylig, og det skal ikke være mulig for en motstander å spille av tidligere meldinger med gamle sensordata på nytt.

Selvorganisering En node som har hatt nedetid skal ikke være avhengig av en ekstern oppsettstjeneste for å komme seg tilbake i nettverket.

Sikker lokalisering Man skal ved hjelp av nettverket kunne lokalisere en node presist.

Tidssynkronisering Alle enhetene i nettverket skal gå etter samme klokke.

Autentisering Man må kunne verifisere at en melding kommer fra den noden som er oppgitt som avsender.

Forfatteren går videre til å liste opp en rekke angrep på trådløse sensornettverk, fordelt på de ulike lagene i nettverksstrukturen (fysisk, link, nettverk og transport). Vi går ikke detaljert inn på de foreslåtte angrepene. Det er like fullt verdt å merke seg at svært mange av angrepene som faller innenfor kryptografiens domene kan avverges ved hjelp av tilstrekkelig autentisering.

Sen påpeker videre at symmetriske løsninger er raskere og mer strømgjerrige, men at det er et åpent problem å finne gode nøkkeldistribusjonsløsninger basert på symmetriske teknikker. I tilfeller med mange enheter som går inn og ut fra nettverket er det spesielt viktig å sørge for at nøkkelmateriellet til enhver tid gjenspeiler deltakerne i nettverket.

Sikkerhetskravene over er omfattende, og er godt innrettet – de handler om hvilke garantier man kan stille utad, og ikke hvordan nodenes indre liv skal fungere.

Dette leder oss over til en artikkel av Akram et al. [1]. I det de omtaler som et *position paper* har gruppen jobbet med autonome svermer av ubemannede flyvende farkoster (*Unmanned Aerial Vehicles, UAV*)[1].

Artikkelen tar for seg sikkerhetskrav for UAV-er, en sterk fiendemodell og hvordan man kan sikre UAV-er mot angrep (spesielt mot å bli fysisk fanget). Etter å ha omtalt potensielle angrep og funksjonskrav, lanserer forfatterne sin egen liste av sikkerhetskrav:

1. UAV-ene skal være styrt av en sikker komponent (*secure element*, SE).
2. Enten hele UAV-en, eller i det minste den sikre komponenten, skal være fysisk beskyttet mot tukling (*tamper resistance*).
3. Den sikre komponenten skal kunne motstå en angriper som overtar en funksjonell enhet.
4. UAV-en må ha en unik ID.
5. UAV-en må ha implementert kryptografiske algoritmer som kan ivareta konfidensialtet og integritet innad i svermen.
6. UAV-en må ha sikker lagring for sensitive opplysninger.
7. UAV-en skal fungere som en plattform, slik at sikkerheten er uavhengig av de enkelte oppgavene den tilpasses til.

[1]Legg merke til ordenes rekkefølge: Dette er en autonom sverm, ikke en sverm av autonome farkoster.

Dersom alle kravene over kan oppfylles, introduserer Akram et al. også et nytt funksjonalitetskrav, som går ut på at det kan opprettes en sikker kanal mellom de sikre komponentene, parallelt med den kommunikasjonen som allerede foregår på tvers av UAV-ene i svermen.

Forfatterne foreslår videre en løsning som kan ivareta alle de overnevnte kravene, samt det ekstra funksjonalitetskravet. Etter å ha observert at eksisterende løsninger, som RFID og trådløse sensornoder ikke oppfyller kravene, peker man på kapable smartkort som et naturlig utgangspunkt. I korte trekk ønsker man å koble smartkortet til en radiosender, og dermed oppnå kommunikasjon direkte mellom SE-ene.

Om en sammenligner disse sikkerhetskravene med listen fra Sen, er vurderingen at de er mer rettet mot designet av enheten, og ikke hvilke garantier man skal kunne ha uten å måtte kjenne til de indre mekanismene og implementasjonene. Vi mener derfor det er riktig å ta med seg virkningene av disse sikkerhetskravene, men at de ikke er egnet til videre forskning innenfor en kryptologisk ramme.

De siste arbeidene vi skal vie plass til i dette kapittelet kommer fra det EU-finansierte forskningsprogrammet RERUM (*REliable, Resilient and secUre IoT for sMart city applications*) (2013–2016). I det som mest av alt framstår som en programerklæring ved prosjektstart, slår Pöhls et al. fast [27] at "RERUM will work on the definition of an authentication process for hetereogeneous objects with different computational and connection capabilities", og deres målsettinger virket generelt å være sammenfallende med våre.

Fra samme prosjekt omtaler Fragkiadakis, Angelakis og Tragos [13] tre aktuelle angrepsfamilier mot trådløse sensornettverk. De to første familiene er basert på at angriperende kan injisere troverdige meldinger i nettverket, og er forholdsvis enkele å forsvare seg mot ved hjelp av autentiseringsmekanismer, den tredje handler om DoS-angrep, som for for denne rapportens vedkommende er utenfor temakretsen.

Artikkelen er en oversiktsartikkel, og vier mest plass til en beskrivelse av aktuelle angrep. At det vies så mye plass til de to første kategoriene av angrep kan tyde på at det ikke rutinemessig innarbeides autentiseringsløsninger i slike nettverk.

Det tredje RERUM-bidraget [14] vi ønsker å nevne tar for seg følgende scenario: Sensorer samler inn en del data, signerer, og sender videre i nettverket. Noen av dataene er det ikke relevant å sende videre etter at de har nådd et valgt sted i nettverket, mens det i andre sammenhenger kan være nødvendig å samle opp data i større pakker før man videresender. Målet er å kunne sende disse dataene videre slik at ingen som observerer data lenger ut i nettverket kan se om den har fått all data, eller om det er et resultat av sammensetninger og utskillinger av pakker. Med andre ord, alle tenkelige sammensetninger av data skal være uskillbar fra situasjonen der dataene kommer samlet fra én avsender. Det kan for eksempel brukes til å gjemme hvor mange sensorer det er i et nettverk, og hvilke sensorer som har samlet inn hva.

Hovedideen er å merke hver datapakke med en merkelapp, og signere meldingen og merkelappen samtidig. Signaturen kan senere oppdateres til å ta med flere meldinger og merkelapper, eller man kan fjerne meldinger og merkelapper. Systemet er basert på hashfunksjoner og det asymmetriske kryptoststemet RSA. Forfatternes undersøkelser tilsier at systemet kan brukes på enheter med liten beregningskapasitet.

Som vi kommer tilbake til i kapittel 3, er etablerte asymmetriske systemer generelt – og RSA

spesielt – usikre mot kvantedatamaskiner. Arbeidet til Frädrich et al. [14] er derfor ikke direkte overførbart til våre krav, men kan være til inspirasjon.

RERUM gikk ut med store mål, men vi kan ikke se at de har lykkes med å oppnå dem. Det vil være nødvendig å arbeide videre i den samme retningen.

2.3 Vår vurdering av modelleringslitteraturen

Kildetilfanget over er snevert, men framstår representativt for tilstanden i litteraturen. RERUM-artiklene og andre underbygger et inntrykk av at sivile sensornettverk generelt er svakt sikret, og at det ikke rutinemessig innføres elementer som kan garantere for autentisiteten til data i nettverket. Inntrykket forsterkes av Do et al. sin karakterisering av modenheten i IoT-sikkerhet.

Ved siden av å notere oss den dynamiske signeringsløsningen til Frädrich et al. [14], bør man ta med seg videre sikkerhetskravene til henholdsvis Sen og Akram et al. Av dem er førstnevntes best innrettet for det generelle tilfellet, men en bør også vurdere en generalisering av sistnevntes.

3 Artikler om algoritmer

Det er utfordrende å lage gode kryptografiske algoritmer (også kalt et *chiffer* – flere chifre), og generelt kreves det mange års utvikling fra bunnen. Algoritmene deles i to klasser, symmetriske og asymmetriske. For algoritmer i den første klassen bruker både avsender og mottaker den samme nøkkelen. I det andre tilfellet finnes det distinkte private og offentlige nøkler. Den offentlige nøkkelen brukes til å kryptere, men gjør det ikke mulig å dekryptere. Den private nøkkelen har den omvendte funksjonen.

3.1 Om kvantedatamaskiner

I vår litteraturgjennomgang har vi spesifikt sett etter kvantesikre løsninger. Det innebærer at verken en kvantedatamaskin eller en klassisk datamaskin skal kunne knekke algoritmen effektivt. Shors algoritme [31] på en kvantedatamaskin kan brukes til å gjøre alle de velkjente asymmetriske algoritmene fullstendig usikre, men rammer bare noen få symmetriske systemer. For generiske symmetriske algoritmer er foreløpig det beste angrepet ved hjelp av Grovers algoritme [15]. Uten å gå inn i detaljene er konsekvensen av Grovers algoritme at man må øke nøkkelstørrelsen for å få samme sikkerhetsnivå som tidligere. Den rådende tommelfingerregelen er at nøklene må dobles for å oppnå samme sikkerhet. For ha 128 bit sikkerhet, skal vi derfor bruke 256 bit nøkler. Imidlertid kan det argumenteres for at den praktiske sikkerheten ikke reduseres like mye som den teoretiske. Et viktig punkt i evalueringen av kryptosystemer er likevel at de tillater nøkler opp til 256 bit.

3.2 Symmetriske teknikker

Det er vanligvis umulig å bevise at et symmetrisk chiffer er sikkert. Derfor må man bruke naturvitenskaplig metode og utsette et foreslått system for falsifisering. Dersom forslaget motstår alle angrep etter tilstrekkelig oppmerksomhet fra eksperter med forskjellige innfallsvinkler, vil man over tid ha tillit nok til å bruke algoritmen i faktiske systemer. Dette kapittelet grupperer artikler som har vurdert og introdusert kryptografiske algoritmer for enheter med lite maskinvare eller båndbredde. Det er noe overlapp mellom denne litteraturstudien og en selvstendig vurdering av lettvektschifre utført av Tor Helleseth på oppdrag av FFI [35]. Vi legger her større vekt på sikkerhet mot kvantedatamaskiner.

Den mest utbredte algoritmen i dag er AES (*Advanced Encryption Standard*), som ble standardisert i 2001 etter en åpen konkurranse. AES har talløse sivile anvendelser, og brukes også i flere graderte systemer[2] [32]. Bonnetain, Naya-Plasencia og Schrottenloher [6] forsøker å angripe AES med teknikker tilgjengelige til en kvantedatamaskin, men konkluderer med at de ikke finner bedre angrep mot 256 bit AES enn det som allerede er kjent ved hjelp av Grovers algoritme sammen med klassiske angrep.

[2]AES sin forgjenger, DES, var 25 år gammel da den ble byttet ut i 2001, og det hadde vært stor utvikling på den tiden. Selv om det ikke er satt i gang en prosess for å erstatte AES er det likevel riktig å følge med på utviklingen på feltet.

AES brukes typisk i en *modus* som kan gi kryptosystemer med de ønskede egenskapene. Den aller enkleste modusen er *Electronic Code Book* (ECM), der hver klartekst alltid blir kryptert til den samme, like lange chifferteksten. ECM mangler tilfeldige inndata, og det har alvorlige følger for praktisk sikkerhet.

En ønsker å bruke en modus som ikke gir for mye merarbeid, men som likevel kan gi gode sikkerhetsgarantier. Til referanse er den vanligste modusen i moderne AES-systemer *Galois/Counter Mode*, som også garanterer for dataenes autentisitet; faguttrykket er *Authenticated Encryption* (AE).

Videre kan symmetriske chiffer deles inn i to grupper:

- Flytchifre, som lager en tilsynelatende tilfeldig bit-rekke som kombineres med datastrømmen ved hjelp av XOR-operasjonen, og blokkchifre som behandler et antall bit (en *blokk*, for AES er blokkstørrelsen på 128 bit) om gangen, og returnerer en kryptert meldingsblokk av samme størrelse.
- Blokkchifre, som har generelt noen fordeler over rene flytchifre, for eksempel at det er enklere å få til beskyttelse av integritet og autentisitet, men kan bare sende ut hele blokker. Dersom en ønsker å kryptere ekstremt lite data om gangen vil man derfor måtte sende en stor overhead hver gang.

Vi skal nå omtale to artikler [8, 33] som vurderer lettvektschifre. De aktuelle algoritmene er AES-182, CLEFIA-128, DESXL, HIGHT, IDEA, KATAN, KTANTAN, KLEIN, LBLOCK, LED, mCrypton, MIBS, Noekeon, Piccolo, PRESENT, TEA, XTEA, TWIN, TWINE, SEA, SKIPJACK og PRINCE. Artiklene gir en rask oversikt over algoritmene, og bruker deretter ressursmålinger [8] og oversikt over kjente angrep [33] for å vurdere systemene.

Før vi går inn på artiklenes vurderinger, observerer vi at alle unntatt varianter av AES, CLEFIA og SEA bare støtter nøkler opp til 128 bit (eller lavere). Basert på diskusjonen i kapittel 3.1, ser vi derfor bort fra den store majoriteten av listen over.

En analyse av faktisk kjøretid for kryptering og dekryptering med de tre gjenstående systemene viser at AES bruker vesentlig mindre prosessortid, og samtidig også mindre minne.

AES kjøres med fulle blokker, og for korte meldinger kan det gi en del ekstraarbeid, *overhead*. Ekstraarbeidet er uavhengig av lengden av meldingen. For lange forsendelser utgjør det derfor prosentvis veldig lite, mens det kan ta uforholdsmessig lang tid når det er snakk om korte meldinger. Andreeva et al. [3] har modifisert AES for å redusere mengden overhead for hver kryptering, og gitt resultatet navnet ForkAES. Forfatterne løser problemet ved å bruke AES-algoritmen på en ny måte, men som er basert på tidligere arbeid. Banik et al. [4] sår tvil om sikkerheten i ForkAES. De presenterer ikke et komplett brudd for en variant som er litt forenklet, noe som reduserer den komfortable sikkerhetsmarginen.

For mobilnettverksteknologiene LTE og 5G kan man bruke tre chifre: AES (i en modus som gjør det om til et flytchiffer), og flytchifrene SNOW-3G og ZUC [24].

I 2014 var det frist for innsending av bidrag i CAESAR-konkurransen (*Competition for Authenticated Encrytion: Security, Applicability, and Robustness*)[3], som har som mål å finne nye kryptosystemer

[3] `https://competitions.cr.yp.to/caesar.html`

som er designet for å ivareta autentisitet og konfidensialitet på samme tid. Den 20. april 2019 ble det annonsert en vinnerporteføljе. I klassen for lettvektsanvendelser ble Ascon og ACORN utnevnt til henholdsvis første- og andrevalg. Begge støtter maksimalt nøkler av 128 bit lengde.

Konkurransen utpekte to likestilte valg for anvendelser som krever høy ytelse: Den nye algoritmen AEGIS-128 (som også finnes i en 256 bit variant, men ikke aktivt anbefalt), og modusen OCB, som for eksempel kan brukes sammen med AES.

Til anvendelsene som krever høyest grad av sikkerhet er det kåret to vinnere i rekkefølge, Deoxys-II og COLM. Bare førstnevnte kan bruke 256 bit nøkler. Deoxys-II er basert på AES, men skal være både sikrere og mer effektiv enn AES i GCM-modus.

Høsten 2018 startet NIST (*National Institute of Science and Technology*) en standardiseringsprosess for lettvektskrypto, med 56 kandidater i første runde og 32 i andre runde. Av de som allerede er nevnt, er Ascon og ForkAES kandidater [34].

Vi ser nærmere på ytterligere en av kandidatene til NIST-prosessen. Naito et al. [23] har foreslått en ny modus (*SAEB*) som i enda større grad enn GCM og OCB skal være egnet til lettvektsoppgaver. Forfatterne definerer fem sentrale egenskaper som de greier å oppnå, mens andre moduser kun oppnår noen av disse.

Minimal tilstandsstørrelse Modusen skal ikke kreve mer minne enn det som allerede kreves av det underliggende chifferet.

Uten invers Algoritmen tar mindre plass på enheten fordi man ikke trenger å ha med en egen implementasjon av dekrypteringskretsen.

Kun XOR Utover det underliggende chifferet trenger ikke modusen å utføre andre operasjoner enn XOR.

Online Hver datablokk prosesseres kun én gang, slik at den ikke trenger å bli lagret i minnet mellom prosesseringene.

Effektiv håndtering av statisk tilleggsdata Ofte har man tilleggsdata som ikke skal krypteres, men som man likevel ønsker å autentisere. Dersom man har slik data som skal brukes hver gang data krypteres, skal det holde at den er blitt prosessert én gang for alle.

Uavhengig av disse prosessene har Kumar et al. [20] introdusert et nytt blokkchiffer for lettvektsanvendelser, spesielt IoT. Forfatterne siterer imidlertid ingen anerkjente verk på feltet, og artikkelen inneholder lite analyse om systemets sikkerhet utover noen enkle statistiske mål. I lys av diskusjonen tidligere om hva som skal til for at fagfeltet skal føle seg trygg på en ny algoritme, framstår artikkelen som et godt eksempel på noe en bør være forsiktig med.

Når man har valgt et chiffer, må man også ha en implementasjon. Sharma, Bala og Verma [30] har gått gjennom flere rammeverk, og beskriver og sammenligner disse. Av disse er det tre som er tenkt brukt til symmetrisk lettvektskrypto: SPIN, LEAP og TinySec.

De to første bruker algoritmen RC5 fra 1994, og vies ikke ytterligere plass her, siden RC5 regnes som usikker i dag. De tredje, TinySec, kan bruke et vilkårlig blokkchiffer, inkludert AES. TinySec er en modul til sensoroperativsystemet TinyOS, som nå er i versjon 2. Imidlertid virker det som om TinySec ikke har blitt videreutviklet siden versjon 1.

3.3 Asymmetriske teknikker

Som nevnt tidligere er dagens etablerte asymmetriske teknikker usikre mot kvantedatamaskiner. For systemer som skal beskytte konfidensialitet over flere tiår er det derfor nødvendig å fase ut slike teknikker allerede i dag. NIST har startet en standardiseringsprosess for nye asymmetriske og kvantesikre systemer. Innsendingsfristen var høsten 2017, og av 82 opprinnelige forslag er det nå 26 forslag som behandles videre i runde 2 [2]. En rapport som dette er dermed ikke stedet for å gå i detalj på alle forslagene ennå.

Imidlertid er det et manuskript det er verdt å nevne for å vise hvilke avveiinger man må gjøre i en slik prosess, sett opp mot vårt lettvektsmål. Én av de grunnleggende ideene baserer seg på matematiske understrukturer på elliptiske kurver, *Supersingular Isogeny Diffie-Hellman*, og som kan gi forholdsvis små nøkler. Koppermann et al. [19] har implementert kandidaten SIKE på en ressursbegrenset enhet. På en Cortex M4-prosessor[4], tok nøkkelgenereringen alene 18 sekunder. Til sammenligning brukte en annen kandidat, NewHope [26], 0,1 sekunder på en tilsvarende prosesor, men genererte en nøkkel som var fire ganger så stor.

Nettopp nøkkelstørrelser er en vesentlig utfordring. Khalid et al. [18] noterer seg at løsninger basert på *latticer*, ett av de til nå mest studerte verktøyene å legge til grunn for kvantesikker kryptografi, er svært gunstige når det kommer til nøkkelstørrelse og enkel implementasjon, men at de fortsatt er svært mye større enn løsningene som brukes i dag.

Kannwischer et al. [17] har laget et rammeverk for å sammenligne kandidatene i runde 2 på en ARM Cortex M4, med 196 kB arbeidsminne og 1 MB ROM. Av de 26 kandidatene var det 11 som de av forskjellige grunner ikke kunne implementere på enheten. Forfatterne gir noen innledende resultater fra prøvekjøringer, men understreker at de på grunn av ulik optimalisering ikke er direkte sammenlignbare.

3.4 Vurdering av aktuelle algoritmer

Basert på andres analyse av effektivitet, er det rimelig å observere at AES i egnet modus kommer godt ut i sammenligning med de andre algoritmene i vurderinger gjort i artikkelutvalget vårt.

Om man ønsker både kvantesikkerhet og asymmetriske teknikker kan ikke man forvente noe tidligst før NIST-standardiseringen er ferdig, og man må antageligvis være forberedt på at parametrene vil være større enn det som er i bruk i dag.

[4]En slik prosessor kan være et et rimelig valg for en liten autonom enhet.

4 Praktiske forsøk fra akademisk forskning

Vi har tidligere i rapporten sett at forskningslitteraturen ennå ikke er fyldig når det kommer til sikkerhetsmodellering av autonome enheter. Til tross for dette er det gjennomført praktiske forsøk og med tilsynelatende gode resultater. Vi diskuterer slike i dette kapittelet.

Dini og Duca [10] har beskrevet en løsning for akustisk undervannskommunikasjon. Løsningen har videre blitt testet ut i Trondheimsfjorden [7] med oppløftende resultater. Hovedutfordringen under vann er en svært liten båndbredde, og med store meldingstap.

For konfidensialitet bruker forfatterne et blokkchiffer i CTS-modus for å fjerne ekstra *padding* av meldingen[5]. Målet er å gjøre meldinger mindre. Integritet og autentisitet ivaretas ved hjelp av en trunkert hashfunksjon med bare 32 bit. Det sparer båndbredden, men ville normalt sett vært så lite at man fikk et sikkerhetsproblem. Forfatterne forsvarer valget ved at deres utstyr bare kan motta omtrent tre meldinger i sekundet[6], og at det derfor vil ta 25 år å sende tilstrekkelig mange meldinger til å kunne knekke systemets sikkerhet med en rimelig sannsynlighet.

Nøkkeldistribusjon og oppdatering i nettverket når en node går ut, skjer med en algoritme kalt S2RP. Algoritmen minimerer antall bytes det er nødvendig å sende, i og med at den bare krever at man sender nøkkelen i seg selv. Autentisering av nøkkelen skjer ved å beregne hashverdien av den mottatte nøkkelen, og sammenligne med den forrige nøkkelen. Nøklene er forhåndsgenerert slik at hver nøkkel er hashen til den forrige. Deretter distribueres de i omvendt rekkefølge.

Nettverket vil nødvendigvis være distributert og ad-hoc, så det kreves kontrollmeldinger mellom nodene for ruting. Disse må også autentiseres. Dini og Duca har også designet og implementert "SeFLOOD", en kryptert versjon av FLOOD-protokollen [28].

Systemet til Dini og Duca virker gjennomtenkt og fornuftig, og er verdt å skjele til i videre utvikling. Spesielt er den praktiske avveiingen på lengden av hashfunksjonen interessant, men observer at argumentet er avhengig av de faktiske forholdene man jobber under, og derfor må gjøres for hver enkelt anvendelse.

Vi avslutter denne delen med et akademisk arbeid som forhåpentligvis kan antyde litt om hva framtiden kan bringe. Cheon et al. [9] har utviklet et homomorft lettvektschiffer som er i stand til å beregne korrekt respons for rotorene på et quadkopter, slik at dronen kan fly dit den skal basert på en veirute og sensordata. Scenarioet er at sensorene signerer sine krypterte data, kontrolleren ombord beregner korrekt respons for rotorene – mens dataene fortsatt er krypterte – og rotorene verifiserer autentisiteten og dekrypterer riktig turtall. Hvis autentiseringen går galt, returnerer dronen tilbake til utgangspunktet. Konsekvensen er blant annet at kontrolleren ikke lenger kan lekke informasjon.

Fascinerende nok er dette ikke bare en teoretisk modell, det finnes også et filmklipp som demonstrerer funksjonaliteten med en flyvende drone. Det forteller oss at kryptografien kan spille en stor rolle i å garantere sikkerhet selv der man i dag tenker at man ikke har noen valg.

[5] Padding er data som legges til en melding for å fylle opp en blokk.
[6] 500 bps båndbredde og meldingslengde på 184 bit.

5 Konklusjon

Vårt mål er å kunne sikre kommunikasjonen til og mellom autonome og ubemannede enheter uten å bruke mer båndbredde, batteri eller berengningskraft enn nødvendig. Meldingene som sendes skal være uforståelige for uvedkommende; det skal ikke finnes tvil om at sensorinformasjon faktisk stammer fra det lille helikopteret dypt bak motstanderens linjer, og den selvstendige bilen skal ikke utføre ordre med mindre beskjeden kommer fra riktig sted. Den frittstående undervannsroboten skal ikke trenge å bruke unødvendig mye strøm og båndbredde på å overføre altfor store meldinger.

Vi har forutsatt at vi har å gjøre med en særdeles kompetent motstander, som er i stand til å skaffe seg perfekt kunnskap om alle algoritmer og systemer. Motstanderen vil kunne kapre en enhet, og er i stand til å avlese alt ukryptert innhold. Videre antar vi at enheten fortsatt fungerer, men at den nå er styrt av motstanderen.

Basert på vår kjennskap til kryptografiske teknikker, vil det kunne finnes gode løsninger på alle utfordringene skissert over. Spesielt må vi stille svært høye krav til autentiseringen av all trafikk.

Selv om løsningene kan finnes, kommer det ikke av seg selv. Basert på litteraturen som er omtalt i denne rapporten, er det naturlig å konkludere i fire punkter:

1. Det er gjort en del arbeid med modellering, men lite av det er tilstrekkelig formelt og grundig til at vi kan bygge på det. Grunnarbeidet er ikke gjort for oss.
2. Det er interessant å følge med på utviklingen av nye chifre for lettvektsanvendelser, den klart vanligste algoritmen AES er fortsatt svært konkurransedyktig.
3. På grunn av muligheten for fungerende kvantedatamaskiner vil det være mange år til man igjen kan bruke rent asymmetriske teknikker for å sikre konfidensialitet over lang tid.
4. Det er gjennomført vellykkede praktiske forsøk. De kan tilpasses, og kan sammen med et solid teoretisk grunnlag være utgangspunkt for nye løsninger.

5.1 Videre arbeid

Parallelt med denne rapporten er det utført et arbeid med å kartlegge sikkerhetsløsningene i eksisterende produkter på markedet, samt å kartlegge de operative behovene [21].

Konklusjonene viser behovet for videre forskning på dette området. FFI kan bistå med følgende aktiviteter:

- Definere felles sikkerhetskrav for autonome enheter. Slike mål skal være kvantifiserbare, og ikke avhenge av det indre livet til enheten. For eksempel kan man kreve «Data skal alltid være sporbar tilbake til sin avsendernode». Et slikt utsagn betyr at enheten må signere meldingen på et egnet vis, og at ingen noder langs veien skal kunne modifisere meldingen.
- I tillegg vil det utvilsomt i arbeidet dukke opp en rekke konkrete scenarier der det vil være mulig å foreslå enkle og effektive løsninger, og der det tidligere ikke har blitt lagt inn noe sikkerhet fra før.

- Trusselen om en fungerende kvantedatamaskin kan ikke ignoreres. For prosjektet står det derfor sentralt å finne løsninger basert på symmetriske teknikker samtidig som vi holder et blikk på utviklingen av nye, kvantesikre algoritmer.
- Til sist gjentar vi behovet for å ha beskyttelse mot fysisk påvirkning av enhetene (tuklebeskyttelse, *tamper protection*). Det kan ikke løses av kryptografi alene, og viser at problemet er reelt tverrfaglig.

Ordliste

ad-hoc-nettverk et nettverk der enhetene snakker direkte sammen uten en sentral infrastruktur; enheter kan gjerne komme og gå fra nettverket. 10, 18

AES *Advanced Encryption Standard*, den mest brukte algoritmen for symmetrisk kryptografi i verden; ble valgt ut som vinner i en åpen konkurranse arrangert/fasilitert av NIST; kryptologer og myndigheter har jevnt over høy tillit til AES når den brukes på riktig måte. 14

asymmetrisk kryptografi et konsept der det er mulig å offentliggjøre en nøkkel, for eksempel for å kryptere eller verifisere en signatur; samtidig kan bare den private nøkkelen brukes til å dekryptere eller signere (jf. symmetrisk kryptografi). 14

autentisitet en egenskap som garanterer at en kryptert melding ble sendt av en aktør som er den han/hun utgir seg for å være. 9

chiffer et kryptosystem, et sett med algoritmer som krypterer og dekrypterer meldinger, for eksempel AES. 14

Fully Homomorphic Encryption direkte oversatt *fullstendig homomorf kryptering*, en samling av kryptosystemer der dekrypteringsfunksjonen er *homomorf*, slik at f.eks. summen av to chiffertekster vil dekrypteres til summen av de krypterte verdiene; formålet er å utføre hele algoritmer på krypterte data. 18

Grovers algoritme en algoritme for kvantedatamaskiner som gjør det mulig å søke gjennom en uordnet mengde med n elementer ved å bare bruke omtrent $\sqrt{n}$ tid; konsekvensen er at alle kryptosystemer minimum må kvadrere nøkkelrommet sitt (som betyr å doble nøkkellengden) for å oppnå samme sikkerhet mot kvantedatamaskiner som de tidligere hadde mot klassiske datamaskiner; grunnen til at man bør bruke 256 bit-nøkler i AES, mot 128 bit tidligere. 14

hashfunksjon en funksjon som komprimerer vilkårlig lang input til en kort streng av forhåndsdefinert lengde; typiske egenskaper: små endringer i input gir store endringer i output, gitt en gyldig output skal det være vanskelig å finne tilsvarende input, gitt en melding m som gir hash h skal det i praksis være umulig å finne en annen melding som gir samme hash, og det skal være like umulig å finne to meldinger som gir samme hash, uansett hvilken. 12, 18

homomorfi en matematisk funksjon mellom to algebraiske strukturer, og som bevarer strukturen, f.eks. potensreglene: $x^a \cdot x^b = x^{a+b}$; selv om multiplikasjon endres til addisjon beholdes den grunnleggende strukturen. 18, 21

integritet en ønsket egenskap som sikrer at meldingen ikke har blitt endret siden den ble sendt; et kryptosystem bør *bevare* integriteten til meldingen, også mot en angriper. 9

IoT *Internet of Things*, eller tingenes internett; en betegnelse på det at svært mange små enheter som sensorer, droner, varmeovner og brødristere er tilkoblet internett, og der enhetene snakker sammen uten at det nødvendigvis er mennesker med i kommunikasjonen. 9

konfidensialitet én av egenskapene et kryptosystem kan gi til meldingen, en garanti om at chifferteksten ikke lekker informasjon om det som er kryptert; det er flere forskjellige definisjoner, avhengig av hvor kraftige angrepstaktikker motstanderen har tilgang til. 9

kvantedatamaskin en datamaskin som opererer på *kvantebit*; elementer som ikke er 0 eller 1, men som eksisterer i en superposisjon mellom begge; posisjonen avhenger av en sannsynlighetsfordeling som kan manipuleres. 14

kvantesikker et kryptosystem er kvantesikkert dersom det ikke eksisterer effektive algoritmer for kvantedatamaskiner som kan knekke systemet; et system kan være sikkert i den klassiske modellen – mot vanlige datamaskiner – men ikke mot kvantedatamaskiner, som f.eks. RSA. 14

NIST *National Institute of Standards and Technology*, en amerikansk sivil institusjon som i denne sammenhengen er relevant fordi den har gjennomført flere gode standardiseringsprosesser for kryptografi der både algoritmer og kriterier har vært transparente. 16

RSA fra opphavsmennene Rivest, Shamir og Adleman, som i 1977 lanserte det første kryptosystemet med en offentlig nøkkel; RSA slik den ble presentert regnes i dag som usikker, men varianter som pakker inn meldingen i tilfeldighet er fortsatt i bruk, spesielt som signatur-system. 12

Shors algoritme en algoritme for kvantedatamaskiner som blant annet gjør det mulig å faktorisere og løse diskrete logaritmer på kort tid; hovedideen er å finne sykluser i den underliggende matematiske strukturen ved hjelp av verktøy som ikke er tilgjengelige for vanlige datamaskiner. 14

signatur data som kobler innholdet i en pakke eller dokument til en offentlig nøkkel og potensielt en identitet; kan brukes til å gi meldingen autentisitet. 12

symmetrisk kryptografi et konsept der to eller flere parter sitter med identisk, hemmelig nøkkelmateriale eller utfører de samme algoritmene (jf. asymmetrisk kryptografi). 14

XOR *eXclusive OR*, en logisk port (eller funksjon av to bit), som gir ut TRUE (1) hvis de to argumentene er ulike, ellers er output FALSE (0); XOR er slik at $y \,\mathsf{XOR}\, x \,\mathsf{XOR}\, x = y$. 15

Referanser

[1] Raja Naeem Akram, Pierre-François Bonnefoi, Serge Chaumette, Konstantinos Markantonakis og Damien Sauveron. «Secure Autonomous UAVs Fleets by Using New Specific Embedded Secure Elements». I: *2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, China, August 23-26, 2016*. IEEE, 2016, s. 606–614. ISBN: 978-1-5090-3205-1. DOI: 10.1109/TrustCom.2016.0116. URL: https://doi.org/10.1109/TrustCom.2016.0116.

[2] Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, Carl Miller David Cooper and Quynh Dang and, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone og Yi-Kai Liu. *Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process*. Tekn. rapp. National Institute of Standards og Technology, 2019.

[3] Elena Andreeva, Reza Reyhanitabar, Kerem Varici og Damian Vizár. «Forking a Blockcipher for Authenticated Encryption of Very Short Messages». I: *IACR Cryptology ePrint Archive* 2018 (2018), s. 916. URL: https://eprint.iacr.org/2018/916.

[4] Subhadeep Banik, Jannis Bossert, Amit Jana, Eik List, Stefan Lucks, Willi Meier, Mostafizar Rahman, Dhiman Saha og Yu Sasaki. «Cryptanalysis of ForkAES». I: *ACNS 19*. Red. av Robert H. Deng, Valérie Gauthier-Umaña, Martín Ochoa og Moti Yung. Bd. 11464. LNCS. Bogota, Colombia: Springer, Heidelberg, Germany, jun. 2019, s. 43–63. DOI: 10.1007/978-3-030-21568-2_3.

[5] Mihir Bellare og Phillip Rogaway. «Entity Authentication and Key Distribution». I: *CRYPTO'93*. Red. av Douglas R. Stinson. Bd. 773. LNCS. Santa Barbara, CA, USA: Springer, Heidelberg, Germany, aug. 1994, s. 232–249. DOI: 10.1007/3-540-48329-2_21.

[6] Xavier Bonnetain, María Naya-Plasencia og André Schrottenloher. «Quantum Security Analysis of AES». I: *IACR Trans. Symm. Cryptol.* 2019.2 (2019), s. 55–93. ISSN: 2519-173X. DOI: 10.13154/tosc.v2019.i2.55-93.

[7] Andrea Caiti, Vincenzo Calabrò, Andrea Munafò, Gianluca Dini og Angelica Lo Duca. «Mobile Underwater Sensor Networks for Protection and Security: Field Experience at the UAN11 Experiment». I: *J. Field Robotics* 30.2 (2013), s. 237–253. DOI: 10.1002/rob.21447. URL: https://doi.org/10.1002/rob.21447.

[8] Mickaël Cazorla, Kevin Marquet og Marine Minier. «Survey and Benchmark of Lightweight Block Ciphers for Wireless Sensor Networks». I: *SECRYPT 2013 - Proceedings of the 10th International Conference on Security and Cryptography, Reykjavik, Iceland, 29-31 July, 2013*. Red. av Pierangela Samarati. SciTePress, 2013, s. 543–548. ISBN: 978-989-8565-73-0. URL: http://ieeexplore.ieee.org/document/7223213/.

[9] Jung Hee Cheon, Kyoohyung Han, Seong-Min Hong, Hyoun Jin Kim, Junsoo Kim, Suseong Kim, Hosung Seo, Hyungbo Shim og Yongsoo Song. «Toward a Secure Drone System: Flying With Real-Time Homomorphic Authenticated Encryption». I: *IEEE Access* 6 (2018), s. 24325–24339. DOI: 10.1109/ACCESS.2018.2819189. URL: https://doi.org/10.1109/ACCESS.2018.2819189.

[10] Gianluca Dini og Angelica Lo Duca. «A Secure Communication Suite for Underwater Acoustic Sensor Networks». I: *Sensors* 12.11 (2012), s. 15133–15158. DOI: 10.3390/s121115133. URL: https://doi.org/10.3390/s121115133.

[11] Quang Do, Ben Martini og Kim-Kwang Raymond Choo. «The Role of the Adversary Model in Applied Security Research». I: *Computers & Security* (2018). ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2018.12.002. URL: http://www.sciencedirect.com/science/article/pii/S0167404818306369.

[12] Danny Dolev og Andrew Chi-Chih Yao. «On the Security of Public Key Protocols (Extended Abstract)». I: *22nd FOCS*. Nashville, TN, USA: IEEE Computer Society Press, okt. 1981, s. 350–357. DOI: 10.1109/SFCS.1981.32.

[13] Alexandros Fragkiadakis, Vangelis Angelakis og Elias Z. Tragos. «Securing Cognitive Wireless Sensor Networks: A Survey». I: *International Journal of Distributed Sensor Networks* 10.3 (2014), s. 393248. DOI: 10.1155/2014/393248. eprint: https://doi.org/10.1155/2014/393248. URL: https://doi.org/10.1155/2014/393248.

[14] Christoph Frädrich, Henrich C. Pöhls, Wolfgang Popp, Noëlle Rakotondravony og Kai Samelin. «Integrity and Authenticity Protection with Selective Disclosure Control in the Cloud & IoT». I: *ICICS 16*. Red. av Kwok-Yan Lam, Chi-Hung Chi og Sihan Qing. Bd. 9977. LNCS. Singapore: Springer, Heidelberg, Germany, nov. 2016, s. 197–213. DOI: 10.1007/978-3-319-50011-9_16.

[15] Lov K. Grover. «A Fast Quantum Mechanical Algorithm for Database Search». I: *28th ACM STOC*. Philadephia, PA, USA: ACM Press, mai 1996, s. 212–219. DOI: 10.1145/237814.237866.

[16] Jason Hill, Robert Szewczyk, Alec Woo, Seth Hollar, David Culler og Kristofer Pister. «System Architecture Directions for Networked Sensors». I: *Proceedings of the Ninth International Conference on Architectural Support for Programming Languages and Operating Systems*. ASPLOS IX. Cambridge, Massachusetts, USA: ACM, 2000, s. 93–104. ISBN: 1-58113-317-0. DOI: 10.1145/378993.379006. URL: http://doi.acm.org/10.1145/378993.379006.

[17] Matthias J. Kannwischer, Joost Rijneveld, Peter Schwabe og Ko Stoffelen. *pqm4: Testing and Benchmarking NIST PQC on ARM Cortex-M4*. Cryptology ePrint Archive, Report 2019/844. https://eprint.iacr.org/2019/844. 2019.

[18] Ayesha Khalid, Sarah McCarthy, Weiqiang Liu og Maire O'Neill. *Lattice-based Cryptography for IoT in A Quantum World: Are We Ready?* Cryptology ePrint Archive, Report 2019/681. https://eprint.iacr.org/2019/681. 2019.

[19] Philipp Koppermann, Eduard Pop, Johann Heyszl og Georg Sigl. *18 Seconds to Key Exchange: Limitations of Supersingular Isogeny Diffie-Hellman on Embedded Devices*. Cryptology ePrint Archive, Report 2018/932. https://eprint.iacr.org/2018/932. 2018.

[20] Manish Kumar, Sunil Kumar, Rajat Budhiraja, M. K. Das og Sanjeev Singh. «Lightweight Data Security Model for IoT Applications: A Dynamic Key Approach». I: *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, China, December 15-18, 2016*. Red. av

Xingang Liu, Tie Qiu, Bin Guo, Kaixuan Lu, Zhaolong Ning, Mianxiong Dong og Yayong Li. IEEE, 2016, s. 424–428. ISBN: 978-1-5090-5880-8. DOI: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.100. URL: https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2016.100.

[21] Federico Mancini, Bjørn Bjerketveit, Lars Erik Olsen, Rune Fardal, Bjørn Møller Greve, Jan Henrik Wiik og Solveig Bruvoll. *Information security for unmanned and autonomous vehicles – main challenges and relevant operational concepts*. FFI-rapport 19/00888. Unntatt offentlighet. FFI, 2019.

[22] Hosein Marzi og Arash Marzi. «A security model for wireless sensor networks». I: *2014 IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA)*. Mai 2014, s. 64–69. DOI: 10.1109/CIVEMSA.2014.6841440. URL: https://doi.org/10.1109/CIVEMSA.2014.6841440.

[23] Yusuke Naito, Mitsuru Matsui, Takeshi Sugawara og Daisuke Suzuki. «SAEB: A Lightweight Blockcipher-Based AEAD Mode of Operation». I: *IACR TCHES* 2018.2 (2018). https://tches.iacr.org/index.php/TCHES/article/view/885, s. 192–217. ISSN: 2569-2925. DOI: 10.13154/tches.v2018.i2.192-217.

[24] Karl Norrmann, Prajwol Kumar Nakarmi og Eva Fogelström. *5G security – enabling a trustworthy 5G system*. White paper GFMC-18:000078. Ericsson, mar. 2018.

[25] Ganesh R. Pathak og Suhas H. Patil. «Mathematical Model of Security Framework for Routing Layer Protocol in Wireless Sensor Networks». I: *Procedia Computer Science* 78 (2016). 1st International Conference on Information Security & Privacy 2015, s. 579–586. ISSN: 1877-0509. DOI: https://doi.org/10.1016/j.procs.2016.02.121. URL: http://www.sciencedirect.com/science/article/pii/S187705091600123X.

[26] Thomas Poppelmann, Erdem Alkim, Roberto Avanzi, Joppe Bos, Léo Ducas, Antonio de la Piedra, Peter Schwabe og Douglas Stebila. *NewHope*. Tekn. rapp. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions. National Institute of Standards og Technology, 2017.

[27] Henrich C. Pöhls, Vangelis Angelakis, Santiago Suppan, Kai Fischer, George C. Oikonomou, Elias Z. Tragos, Rodrigo Diaz Rodriguez og Theodoros Mouroutis. «RERUM: Building a reliable IoT upon privacy- and security- enabled smart objects». I: *2014 IEEE Wireless Communications and Networking Conference Workshops, WCNC Workshops, Istanbul, Turkey, April 6-9, 2014*. IEEE, 2014, s. 122–127. ISBN: 978-1-4799-3086-9. DOI: 10.1109/WCNCW.2014.6934872. URL: https://doi.org/10.1109/WCNCW.2014.6934872.

[28] Helge Rustad. «A Lightweight Protocol Suite for Underwater Communication». I: *23rd International Conference on Advanced Information Networking and Applications, AINA 2009, Workshops Proceedings, Bradford, United Kingdom, May 26-29, 2009*. IEEE Computer Society, 2009, s. 1172–1177. ISBN: 978-0-7695-3639-2. DOI: 10.1109/WAINA.2009.173. URL: https://doi.org/10.1109/WAINA.2009.173.

[29] Jaydip Sen. «Security in Wireless Sensor Networks». I: *CoRR* abs/1301.5065 (2013). arXiv: 1301.5065. URL: http://arxiv.org/abs/1301.5065.

[30] Gaurav Sharma, Suman Bala og Anil K. Verma. «Security Frameworks for Wireless Sensor Networks-Review». I: *Procedia Technology* 6 (2012). 2nd International Conference on Communication, Computing & Security [ICCCS-2012], s. 978–987. ISSN: 2212-0173. DOI: https://doi.org/10.1016/j.protcy.2012.10.119. URL: http://www.sciencedirect.com/science/article/pii/S2212017312006640.

[31] Peter W. Shor. «Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer». I: *SIAM J. Comput.* 26.5 (1997), s. 1484–1509. DOI: 10.1137/S0097539795293172. URL: https://doi.org/10.1137/S0097539795293172.

[32] Nasjonal sikkerhetsmyndighet. *NSM Cryptographic Requirements*. Veiledning. 2016. URL: https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/ncr3.1.pdf.

[33] Hala Tawalbeh, Sonia Hashish, Loai Tawalbeh og Anwar Aldairi. «Security in Wireless Sensor Networks Using Lightweight Cryptography». I: *Journal of Information Assurance and Security* 12 (nov. 2017), s. 118–123.

[34] Meltem Sönmez Turan, Kerry McKay, Çağdaş Çalık, Donghoon Chang og Lawrence Bassham. *Status Report on the First Round of the NIST Lightweight Cryptography Standardization Process*. Tekn. rapp. National Institute of Standards og Technology, 2019.

[35] Eli Winjum og Tor Helleseth. *Lettvektkryptografi – En gjennomgang av status*. FFI-internnotat 19/00529. FFI, 2019.

About FFI

The Norwegian Defence Research Establishment (FFI) was founded 11th of April 1946. It is organised as an administrative agency subordinate to the Ministry of Defence.

FFI's MISSION

FFI is the prime institution responsible for defence related research in Norway. Its principal mission is to carry out research and development to meet the requirements of the Armed Forces. FFI has the role of chief adviser to the political and military leadership. In particular, the institute shall focus on aspects of the development in science and technology that can influence our security policy or defence planning.

FFI's VISION

FFI turns knowledge and ideas into an efficient defence.

FFI's CHARACTERISTICS

Creative, daring, broad-minded and responsible.

Om FFI

Forsvarets forskningsinstitutt ble etablert 11. april 1946. Instituttet er organisert som et forvaltningsorgan med særskilte fullmakter underlagt Forsvarsdepartementet.

FFIs FORMÅL

Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som kan påvirke forutsetningene for sikkerhetspolitikken eller forsvarsplanleggingen.

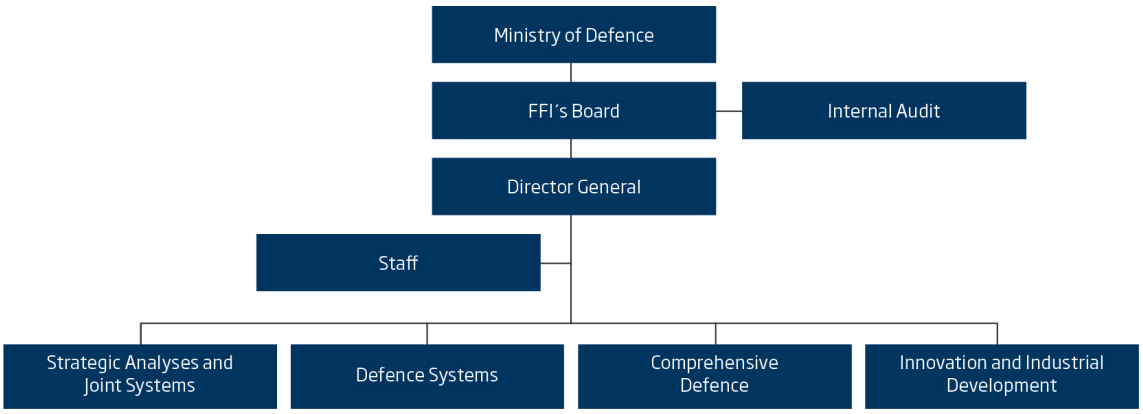
FFIs VISJON

FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs VERDIER

Skapende, drivende, vidsynt og ansvarlig.

FFI's organisation



Forsvarets forskningsinstitutt
Postboks 25
2027 Kjeller

Besøksadresse:
Instituttveien 20
2007 Kjeller

Telefon: 63 80 70 00
Telefaks: 63 80 71 15
Epost: ffi@ffi.no

Norwegian Defence Research Establishment (FFI)
P.O. Box 25
NO-2027 Kjeller

Office address:
Instituttveien 20
N-2007 Kjeller

Telephone: +47 63 80 70 00
Telefax: +47 63 80 71 15
Email: ffi@ffi.no

FFI Forsvarets forskningsinstitutt
Norwegian Defence Research Establishment