
Satakunnan ammattikorkeakoulu

Mikko Rantala

# TIETOTURVALLINEN LANGATON KAUKO-OHJAIN

Tietotekniikan koulutusohjelma

2008

TIETOTURVALLINEN LANGATON KAUKO-OHJAIN

Rantala, Mikko
Satakunnan ammattikorkeakoulu
Tietotekniikan koulutusohjelma
Joulukuu 2008
Perkiö, Tauno
UDK: 62–519, 621.39, 654.9
Sivumäärä: 49

Asiasanat: tietoturva, langaton tiedonsiirto, kauko-ohjaus, sulautettu tietotekniikka

---

Tämän opinnäytetyön tavoitteena oli suunnitella ja rakentaa sähköiselle lukolle langaton kauko-ohjain, joka salaa osan radioliikenteestä lukon oviyksikön ja kauko-ohjaimen välillä. Lisäksi tarkoitus oli tutkia infrapunan soveltuvuutta salausavainten vaihtoon ja salauksen vaikutusta langattomaan kommunikointiin.

Vaatimusmäärittelyn pohjalta suunniteltiin ja rakennettiin laitteisto, johon valittiin vähävirtaisia komponentteja. Ohjelmiston toteutuksessa pyrittiin mahdollisimman tehokkaasti hyödyntämään laitteiston unitiloja virrankulutuksen pienentämiseksi. Salauksen vaikutuksia järjestelmän virrankulutukseen ja radioliikenteeseen mitattiin ja tutkittiin tasapainon löytämiseksi turvallisuuden ja prosessointinopeuden välillä.

Mittauksissa ja analysoinnissa keskityttiin salaukseen ja sen vaikutuksiin järjestelmän eri toimintoihin. Tuloksia tulkittaessa pyrittiin käsittelemään salauksen vaikutuksia myös laajemmalla tasolla, jotta analyysin tuloksia voisi hyödyntää myös tulevaisuuden projekteissa.

SECURE WIRELESS REMOTE

Rantala, Mikko
Satakunta University of Applied Sciences
Degree Programme in Information Technology
December 2008
Perkiö, Tauno
UDC: 62–519, 621.39, 654.9
Number of Pages: 49

Key Words: information security, wireless communication, remote control, embedded computing

---

The purpose of this Bachelor's thesis was to design and build a wireless remote and a door unit for an electric lock, research the effects of encryption on radio traffic and the suitability of infrared in transmitting encryption keys.

Based on the requirements specification the hardware was designed and built with low power consumption components. Software was designed and implemented to be as power efficient as possible by using the microcontrollers sleep states. The effects of encryption to the system's power consumption and radio traffic were measured and researched to find a balance between security and processing speed.

Measurements and analysis focused on encryption and its effects in the different functionalities of the system. The results on encryption were also analyzed on a broader level in order to provide research data that could be utilized in future projects.

SISÄLLYS

# SYMBOLI- JA TERMILUETTELO

ACK – (Acknowledged) Kuittaus hyväksytystä vastaanotetusta sanomasta.

CRC – (Cyclic Redundancy Check) Tiivistealgoritmi, jota käytetään virheentarkistusmenetelmänä.

EEPROM – (Electrically Erasable Programmable Read Only Memory) Muistityyppi, joka säilyttää tietonsa käyttöjännitteen hävitessä.

FR-4 – (Flame Retardant 4) Korkealaatuinen piirilevymateriaali.

GFSK – (Gaussian Frequency Shift Keying) Taajuussiirtokoodaus on modulaatiotekniikka, jossa ykkösiä ja nollia esittäviä positiivisia ja negatiivisia taajuusvaihteluita tasoitetaan Gauss-suotimella.

ISM-taajuusalue – (Industrial, Scientific and Medical) Teolliseen, tieteelliseen ja lääketieteelliseen käyttöön tarkoitettu maailmanlaajuinen radiotaajuuskaista, jonka käyttö ei vaadi erillistä lupaa.

ITU – (International Telecommunication Union) YK:n alainen järjestö, jonka tehtäviä ovat standardointi, radiotaajuuksien jakaminen ja puhelinverkkojen yhteyskäytäntöjen kansainvälinen organisointi.

IEEE – (Institute of Electrical and Electronics Engineers) Kansainvälinen, yleishyödyllinen tekniikan alan järjestö.

JTAG – (Joint Test Action Group) IEEE standardi 1149.1

MAC – (Message Authentication Code) Algoritmi, jota käytetään virheentarkistus-menetelmänä.

MCU – (Microcontroller) Mikrokontrolleri, ohjelmoitava integroitu piiri.

MIPS – (Million instructions per second) Miljoona suoritettua konekielistä käskyä per sekunti, näitä lukuja ei voi vertailla eri prosessoriarkkitehtuurien välillä.

NACK – (Not Acknowledged) Kuittaus hylätystä vastaanotetusta sanomasta.

PDIP – (Plastic Dual Inline Package) Elektroniikassa käytetty suorakulmainen kotelotyyppi.

RC-5 – Lohkosalausalgoritmi, joka on tunnettu yksinkertaisuudestaan ja joustavuudestaan.

RSA Laboratories – EMC Corporation:n tutkimuskeskus. Alun perin nimetty RSA-salauksen julkistajien nimien mukaan (Rivest, Shamir ja Adleman).

SPI – (Serial Peripheral Interface Bus) Sarjaliikenneväylä.

SYNC – (Synchronise) Radiosanoma, jolla aloitetaan kauko-ohjaimen ja oviyksikön välinen viestintäistunto.

WABS-tutkimusryhmä – (Wireless Automated Building Systems) Langattomat automatisoidut rakennusjärjestelmät-tutkimusryhmä.

XOR – (Exclusive or) Looginen operaatio, jonka tulos on tosi vain ja ainoastaan silloin, kun vain toinen kahdesta syötteestä on tosi.

# 1 JOHDANTO

Langaton ja automatisoitu kiinteistönhallinta on kehittyvä ala, jonka tärkeys on kasvanut mm. energian hinnan nousun, väestön ikääntymisen ja ihmisten mukavuuden halun takia. Alan tutkimuksen yksi suurimpia haasteita on yhdistää kasvavat vaatimukset monimutkaisemmista toiminnoista, laajemmista ominaisuuksista, toiminnan turvallisuudesta sekä matalasta virrankulutuksesta. Viime vuosien kehitys elektroniikan miniatyrisaation ja varsinkin sulautettujen langattomien laitteiden osalta on tehnyt langattomat ja energiatehokkaat verkot taloudellisesti houkutteleviksi yrityksille.

Tampereen teknillisen yliopiston elektroniikan laitoksen Rauman tutkimusyksikössä on käynnissä WABS–tutkimusryhmän (Wireless Automated Building Systems) alueellisesti ja tutkimuksellisesti merkittävä ECOmfort Living-projekti, joka keskittyy langattomiin sensori- ja laitesovelluksiin, joiden avulla voidaan parantaa rakennusten energiatehokkuutta, joustavuutta sekä käytettävyyttä. /1, 2/ Yhteistyökumppaneina ja rahoittajina toimivat useat satakuntalaiset ja muut suomalaiset yritykset, joilla on suuri asema talotekniikka-alalla. Kansainvälisyyttä projektiin tuo yhteistyö University of California Berkeleyn yliopiston kanssa. WABS–tutkimusryhmällä on ollut useita projekteja, joissa on tutkittu langatonta tiedonsiirtoa sekä mm. energian sieppaamista ympäristöstä pienlaitteiden käyttövoimaksi.

Tässä opinnäytetyössä, joka on osa ECOmfort Living–projektia, suunniteltiin ja toteutettiin radioyhteyden salaava kauko-ohjain, joka kommunikoi sähköistä lukkoa ohjaavan oviyksikön kanssa. Työn tarkoituksena oli tarjota yliopistolle tutkimustietoa salauksen vaikutuksesta radioliikenteeseen sekä virrankulutukseen ja tutkia infrapunan soveltuvuutta salausavaimien vaihtoon. Projektin tavoitteita olivat: tietoturvallinen ja luotettava kommunikointi kauko-ohjaimen ja oviyksikön välillä, virrankulutuksen minimointi paristojen eliniän maksimoimiseksi ja helpon käyttöliittymän kehitys. Kehitettävän laitteen rajallinen prosessointinopeus, muistinmäärä ja tarve kommunikoida oviyksikön kanssa langattomasti asettivat työlle useita haasteita. Tie-

toturvallinen kauko-ohjaus vaatii tiedonsiirron salausta ja osapuolien tunnistamista, mikä kasvattaa vaadittavan prosessoinnin ja siirrettävän tiedon määrää.

Työn rakenne on seuraavanlainen. Toisessa luvussa esitellään projektiin liittynyt tutkimus tietoturvasta, salauksesta ja elektroniikan virrankulutuksesta. Tietoturvan ja salauksen peruskäsitteet käydään lyhyesti läpi ja projektia koskevia yksityiskohtia selitetään tarkemmin. Kolmannessa luvussa selostetaan yksityiskohtaisesti laitteisto- ja ohjelmistotason ratkaisut, myös käyttöliittymä esitellään tässä luvussa. Ohjelmisto esitetään laitteistoa yleisemmällä tasolla, liitteistä löytyy koodi yksityiskohtien tarkastelua varten. Luku neljä sisältää mittaustulokset, mittausympäristö käydään myös lyhyesti läpi. Viidennessä ja viimeisessä luvussa esitetään mittaustulosten analyysi, yhteenveto aiempien lukujen tuloksista, järjestelmässä olevista puutteista ja jatkokehitysmahdollisuuksista. Analyysissa keskitytään erityisesti salaukseen.

# 2 TEORIA JA TAUSTAT

## 2.1 Tietoturva

Tämän projektin lähtökohtana on ajatus, että järjestelmän turvallisuus syntyy langattoman liikenteen turvallisuudesta. Mikrokontrolleriteollisuudessa useat valmistajat myyvät tietoturvallisiksi väittämiään tuotteita, jotka voidaan itse asiassa lähes kaikki murtaa jos hyökkääjällä on oikeat laitteet käytössä. /3/ Fyysisen tietoturvallisuuden tutkimus ja kehitys on kokonaan oma alansa elektroniikassa ja tietotekniikassa.

### 2.1.1 Mitä tietoturva on?

Tietoturva on tässä projektissa keskeinen käsite, joka tarkoittaa tiedon käsittelyn suojaamista luvattomalta käytöltä, tarkastelulta, häirinnältä, muuntamiselta ja tuhoamiselta. Julkisissa verkoissa liikenteen tarkastelua on mahdotonta havaita ja estää, mikäli käytetty antenni säteilee laajalle alueelle. Näin ollen turvallista kauko-ohjausta kehitettäessä täytyy siis olettaa mahdollisen hyökkääjän kuuntelevan liikennettä rajoituksitta.

Langattoman liikenteen häirintä on helppoa voimakkaalla sähkömagneettisella signaalilla, mikä voi johtaa tiedon tuhoutumiseen. Sekä häirintää että kuuntelua voidaan yrittää välttää erilaisilla tekniikoilla kuten taajuushyppelyllä tai naamioimalla signaali kohinaksi. Näitä tekniikoita pohditaan jatkokehitysosiossa, mutta niihin ei keskitytä projektin varsinaisessa tutkimuksessa.

Tiedon luvaton muuntaminen on olemassa olevan signaalin vääristämistä hyökkääjän tarkoituksiin. Korruptoitunut tieto voidaan havaita liittämällä käytettyihin sanomiin MAC- (Message Authentication Code) tai CRC-pääte (Cyclic Redundancy Check), joka lasketaan viestistä sekä lähetys- että vastaanottopäässä. Väärennetystä viestistä

laskettu MAC/CRC-pääte on eri kuin viestin mukana tullut pääte, mikä varoittaa väärennöksestä.

Sekä kauko-ohjaimen että oviyksikön suunnittelussa on pyritty ottamaan huomioon vaatimukset kohtuullisesta turvallisuudesta sekä mahdolliset hyökkäykset, joita laitteisiin voidaan kohdistaa. Suunnittelun aikana huomioitiin yllämainitut tietoturvan muodostavat kohdat, näitä kaikkia pyritään varmistamaan tehokkaalla ohjelmoinnilla ja tiedonsiirron salauksella.

### 2.1.2 Tietoturvan murtuminen

Yksi tämän projektin lähtökohta on realistinen suhtautuminen ihmisten kehittämiin turvallisuustuotteisiin: ”Sen minkä joku ihminen on lukinnut voi toinen ihminen myös murtaa”.

Järjestelmän tietoturvalle kaksi suurinta uhkaa ovat salauksen murtuminen ja kauko-ohjaimen päätyminen hyökkääjän käsiin. Jos salaus murtuu, viestejä voidaan lukea, muokata ja lähettää ilman, että järjestelmä havaitsee turvallisuuden pettäneen. Kauko-ohjaimen muisti sisältää laajennetun salausavaimen, jolla koko järjestelmä on avoin hyökkääjälle. Toipuminen turvallisuuden pettämisestä voi tapahtua vaihtamalla salausavainta ja lukon avausnumeroa, ennen kuin hyökkääjä on päässyt käyttämään luvattomasti hankkimaansa salausavainta.

## 2.2 Salaus

### 2.2.1 Mitä salaus on?

Salaus on tiedon todellisen muodon piilottamista epätoivottujen tahojen tarkkailulta. Nykyaikaiset salausmenetelmät perustuvat matematiikkaan ja tietojenkäsittelyyn, joilla salaaminen eli kryptaus pyrkii muuntamaan alkuperäisen selväkielisentekstin satunnaiselta vaikuttavaan muotoon, jota ei pystytä ilman oikeaa avainta purkamaan

eli dekryptaamaan. Salausta käytetään nykyään lähes kaikissa sähköisissä laitteissa ja tietokoneohjelmissa, jotka käsittelevät luottamuksellisia tietoja.

Salausalgoritmeja on kahdenlaisia: symmetriset ja asymmetriset. Asymmetriset algoritmit hyödyntävät julkista avainta, suuria alkulukuja, diskreetin logaritmin ongelmaa ja ovat laskennallisesti raskaita. Symmetriset algoritmit taas pyrkivät sotkemaan yhteyden selvä- ja salatekstin välillä ja ovat laskennallisesti nopeampia kuin asymmetriset algoritmit. Symmetristen algoritmien heikkoutena on yhteinen salattu avain, jonka täytyy löytyä molemmilta osapuolilta salausta ja purkua varten. Yhteinen salattu avain tarvitsee myös turvallisen tavan, jolla jakaa se kaikille sitä käyttäville osapuolille.

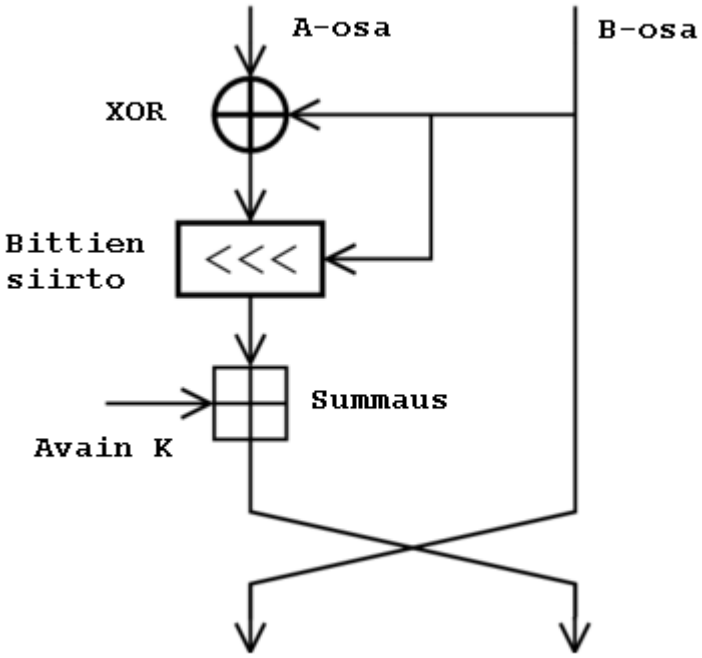
Tätä projektia varten tutkittiin useita eri algoritmeja ja osittain aikaisempien suositusten perusteella valittiin RC5, joka on ominaisuuksiltaan hyvin joustava symmetrinen algoritmi. /4, 5/ Joustavuus on ohjelmiston toteutuksen kannalta äärimmäisen tärkeä tekijä laitteistossa, jonka muisti, prosessointivoima ja pariston ikä on rajoitettu.

### 2.2.2 RC5-salaus

RC5 on Ronald L. Rivestin vuonna 1994 kehittämä symmetrinen lohkoalgoritmi, joka on tunnettu alalla yksinkertaisuudestaan ja joustavuudestaan. Algoritmi on patentoitu USA:ssa, mutta ei muualla maailmassa. Salaimen toiminta on hyvin yksinkertainen ja perustuu kolmeen operaatioon: summaukseen, XOR- (Exclusive or) ja rotaatio-operaatioihin. Ennen kuin salaus voidaan suorittaa, täytyy salausavain laajentaa, tätä laajennettua avainta käytetään salauksen tai sen purkamisen yhteydessä. Laajentamista varten avain luodaan yleensä jollakin satunnaislukugeneraattorilla. RC5:n turvallisuus riippuukin täysin avaimesta, koska algoritmi on tunnettu. Salausavain täytyy vaihtaa, jos se on paljastunut tai turvallisuutta halutaan varmistaa säännöllisillä avainten uudistamisilla.

Kuvassa 1 on esitetty puolet yhdestä RC5-kierroksesta. Salattava selväkielinen teksti on jaettu kahteen osaan A ja B. Aluksi tehdään bittikohtainen XOR osien A ja B kesken. Saatua tekstiä siirretään yhdessä B osan kanssa rotaatio-operaatiossa ja lopuksi

teksti summataan palaan laajennettua avainta. Esim. 12-kierroksisessa salauksessa operaatio toistettaisiin 24 kertaa.




**Kuva 1** Puoli kierrosta RC5 salauksesta

Salausalgoritmissa on kolme parametria, joita muuttamalla voidaan valita haluttu tasapaino turvallisuuden ja nopeuden välillä. Käytetyt parametrit ilmoitetaan seuraavassa muodossa: RC5- w/r/b, jossa *w* on sanan koko bitteinä, *r* kierrosten lukumäärä ja *b* avaimen koko tavuina.

Ensimmäinen parametri *w* voi saada arvot 16, 32 tai 64, selväkielisen ja salatun tekstin koko 2w. Oletuskoko *w*:lle on 32 bittiä.

Toinen parametri *r* voi saada arvot väliltä 0-255. Yleisesti hyväksyttyjä kierroslukumääriä ovat 12–20.

Kolmas parametri *b* voi saada arvot väliltä 0-255. Alkuperäinen suositus avaimen kooksi on 128-bittiä. RC5-avaimia on laskettu hajautetusti Distributed.net- sivustolla, joka perustettiin vastauksena RSA-laboratories:n haasteelle murtaa RC5-salaus. 64-

bittisen oikean avaimen laskeminen hajautetusti kesti 5 vuotta, 72-bittisen avaimen kaikkien mahdollisuuksien laskeminen nykyaikaisilla työasemilla hajautetusti kestänee noin 1000 vuotta. /6/ Toisaalta jo ensimmäinen laskettu avain voi olla oikea. Avainpituuden kasvattaminen laajentaa avainavaruutta eli oikean avaimen löytämisen todennäköisyys pienenee yhtä laskettua avainta kohti.

Algoritmin tarkkaa toimintaa ei kuvata tässä dokumentissa. Rivestin julkaisussa on kattava selostus algoritmin perusteista /5/. Luvussa 3 käydään läpi lyhyesti valittu RC5- toimintatila.

## 2.3 Virrankulutus

Virrankulutuksen minimoiminen sekä kauko-ohjaimessa että oviyksikössä oli tärkeä osa projektia. Molemmat laitteet ovat paristokäyttöisiä, joten kummassakin pyrittiin hyödyntämään unitiloja mahdollisimman tehokkaasti. Luvussa 5 on laskettu virrankulutuksia kummallekin laitteelle eri toimintatiloissa; laskut on suoritettu sekä datalehtien että mitattujen arvojen perusteella.

### 2.3.1 Kauko-ohjain

Kauko-ohjaimen tarkkoja käyttöaikoja ja käyttökertojen lukumäärää ei voida tarkasti ennustaa. Tämän vuoksi tehtiin tiettyjä olettamuksia virrankulutuksen jakautumisesta. Ensimmäinen olettamus koskee aktiivisen ajan kestoa: ohjain herää vain lyhyeksi aikaa suorittamaan käyttäjän haluamat toimenpiteet ja sammuttaa sen jälkeen itsensä. Toinen olettamus, joka on seurausta ensimmäisestä, on että, ohjain on todennäköisesti suuren osan (> 99 %) eliniästään sammutettuna.

Näistä kahdesta olettamuksesta voitiin todeta kokonaisvirrankulutuksen riippuvan enemmän unitilan kuin aktiivisen tilan virrankulutuksesta. Aktiivisen tilan virrankulutus on tietysti myös tärkeää minimoida sopivilla komponenteilla ja ohjelmoinnilla.

### 2.3.2 Oviyksikkö

Kauko-ohjaimen käyttöaikojen satunnaisuuden vuoksi oviyksikkö ei voi milloinkaan ennustaa, koska sen kanssa kommunikoidaan. Näin ollen käytettävyyden takaamiseksi oviyksikön täytyy väliajoin herätä kuuntelemaan siirtotietä viestien varalta. Oviyksikön virrankulutuksen mallintamista helpottaa sen ennalta määrätty toimintasykli, mutta vaikeuttaa vastaanottoon liittyvät satunnaisuudet kauko-ohjaimesta johtuen. Näitä satunnaisuuksia tarkastellaan luvussa 5. Virrankulutusta lisäävät myös lukkoa ohjaavat komponentit, joita oviyksikkö kontrolloi.

## 2.4 Siirtotie

TTY:n Rauman yksikössä on tutkittu eri radiotaajuuksien soveltuvuutta tiedonsiirtoon useita eri projekteja varten. Erityistä huomiota on kiinnitetty ISM (Industrial, Scientific and Medical)-taajuuksiin. Osittain näiden tutkimusten ja aikaisempien projektien positiivisten kokemuksien perusteella valittiin 433 MHz ISM-taajuusalue, joka tarjoaa erinomaisen kantaman ja esteiden läpäisykyvyn avoimessa maastossa sekä sisätiloissa. Korkeammat taajuudet tarjoavat suuremman tiedonsiirtokapasiteetin, joka ei tälle järjestelmälle ole tarpeellinen sanomien lyhyyden vuoksi. ISM- taajuuksia on useita ja ne ovat nähtävillä ITU:n (International Telecommunication Union) sivuilla. Viestintäviraston websivuilla olevista määräyksistä 4 J/2007 ja 15 X/2007 M sekä taajuusjakotaulukosta on nähtävissä tarkat määrittelyt, joita noudatetaan Suomessa. /7, 8/

# 3 LAITTEISTON JA OHJELMISTON TOTEUTUS

Tämä luku käsittelee sekä laitteistoa että ohjelmistoa. Laitteisto-osa keskittyy valittuihin komponentteihin sekä käytettyihin työmenetelmiin ja ohjelmisto-osa kertoo ohjelmointikielestä sekä – työstä.

## 3.1 Laitteisto

Tutkimusvaiheen lopussa luodun vaatimusmäärittelydokumentin perusteella pystyttiin luomaan lista tarvittavista komponenteista, joita järjestelmää tarvittaisiin. Radiokommunikointiin valittiin TTY:n Rauman tutkimusyksikössä DI-työnsä tehneen Jaakko Vierikon tekemät radiomoduulit. /9/ Valmiit moduulit otettiin käyttöön useasta syystä: radiomoduulien kokoaminen olisi tietyiltä osin ollut vaikeaa, radiomoduulin valmistaminen ei olisi tuonut projektiin merkittävää lisäarvoa ja projektin aikaa saatiin siirrettyä muihin tehtäviin. Tarvitut komponentit vaatimusmäärittelyn mukaan on esitelty taulukossa 1.

**Taulukko 1** Vaatimusmäärittelyn mukaisesti tarvitut komponentit

| **Komponentti** | **Nimi** | **Mahd. huomioitavaa** |
|---|---|---|
| Mikrokontrolleri | ATmega644PV-10PU | Max 10 MHz |
| Radiopiiri | nRF905 | 433/868/915 MHz |
| Infrapunayksikkö | TFBS4650 | Lähetinvastaanotin |
| Regulaattori | MCP1824 | 3V ulostulojännite |
| 32 kHZ kide | Epson Toyocom C-Type | Reaaliaikakello |
| Kalvonäppäimistö | Ei tunnettu | 4 näppäintä |
| LEDit + muut yleiset komponentit | - | Vastuksia, kondensaattoreita, yms. |

Piirilevyt suunniteltiin Cadsoftin EAGLE 4.16r2 Light-ohjelmalla, joka on ilmainen versio ohjelmistosta tietyin rajoituksin. Kummassakin sekä kauko-ohjaimessa että oviyksikössä käytetään samaa piirilevyä. Näin voitiin tehdä, koska kumpikin laite

käyttää lähes täysin samoja komponentteja. Näiden kahden laitteen lisäksi tehtiin pieni piirilevy, jossa on lukon avaava rele ja muutama muu komponentti. EAGLE ohjelmalla tuotettiin gerber-tiedostot, jotka vietiin CircuitCam 4.0-ohjelmaan. CircuitCam tuottaa piirilevyjyrsimen vaatiman tiedoston. Jyrsintä ohjattiin Boardmaster-ohjelmalla käyttäen LPKF Protomat C100/HF-laitetta. Kaikki komponentit juotettiin käsin FR-4 (Flame Retardant 4) materiaalista valmistetuille piirilevyille, mikä onnistui yllättävän hyvin, vaikka muutaman komponentin vedot olivat erittäin lähellä toisiaan. Kauko-ohjaimessa ja oviyksikössä tarvittiin lähes samat osat muutamaa taulukossa 1 mainittua komponenttia lukuun ottamatta. Valmis laitteisto on esitelty kuvassa 2.


**Kuva 2** Kauko-ohjain, oviyksikkö ja lukko

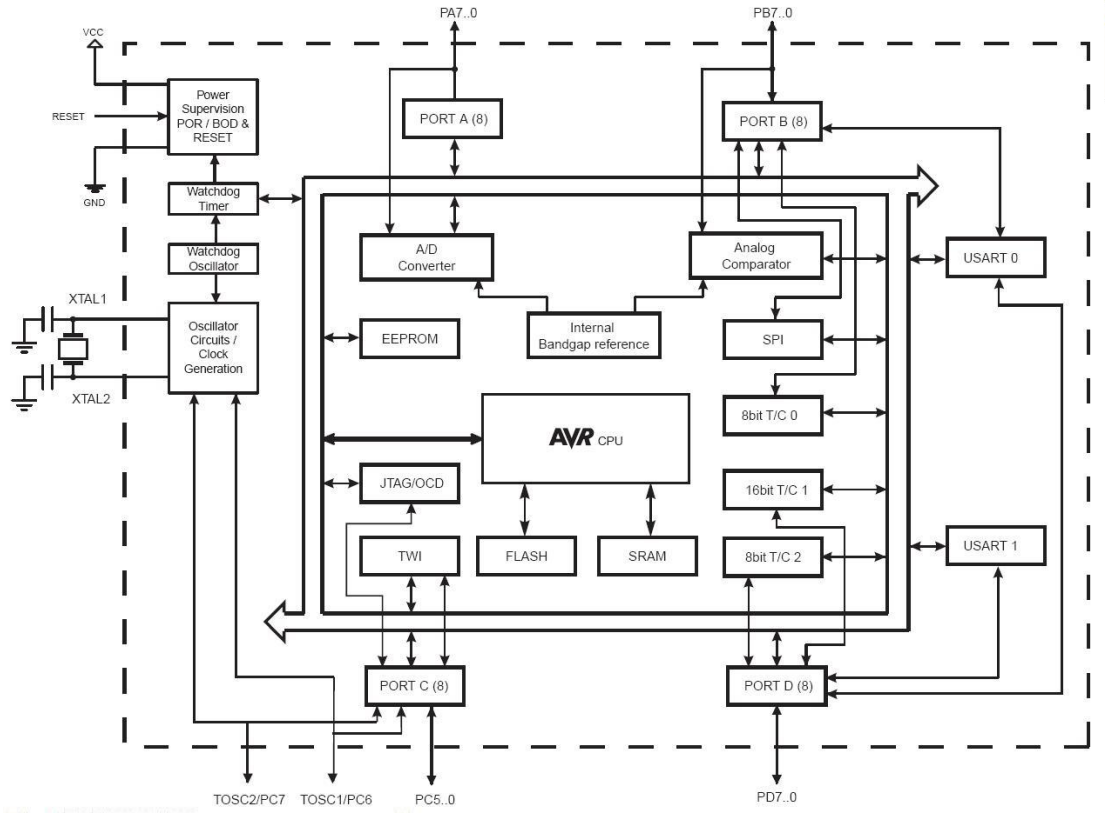
### 3.1.1 Tärkeimmät komponentit yksityiskohtaisemmin

**Mikrokontrolleri**

Mikrokontrolleri (MCU) on laite, joka sisältää prosessorin, erilaisia muisteja, I/O-väyliä ja mallista riippuen eri lisälaitteita. Näiden osien integroiminen samaan piiriin säästää sekä tilaa piirilevyltä että suunnittelijan työaikaa, kaikkia piiristä löytyviä lisälaitteita ei luetella tässä dokumentissa. MCU käsittelee sekä kauko-ohjaimessa että oviyksikössä radio- ja infrapunaliikenteen, salauksen ja ajastukset. Kauko-ohjaimessa käsittelyä lisäävät näppäinpainallukset ja oviyksikössä lukon ohjaus.

TTY:n Rauman tutkimusyksikössä on aikaisemmissa projekteissa käytetty sekä Atmelin ATmega- että Microchipin PIC- mikrokontrollereita. Koska opinnäytetyön tekijä tunsi paremmin Atmelin mikrokontrollerit, päädyttiin valitsemaan Atmelin prosessori. Atmel Corporation valmistaa useita erimallisia mikrokontrollereita, AVR-arkkitehtuuriin perustuvat pico-sarjan 8-bittiset ATmegat ovat ominaisuuksiltaan monipuolisia ja virrankulutukseltaan matalia.

Atmelin tuotelistaa tutkittaessa päädyttiin ATmega644PV MCU:hun. Tästä mikrokontrollerista löytyy myös pinniyhteensopivat 324P ja 164P mallit, joissa on vähemmän SRAM-, Flash- ja EEPROM (Electrically Erasable Programmable Read Only Memory)- muistia. Valinta mitoitettiin tarkoituksella järeämmäksi, jotta vielä tässä vaiheessa tuntematon koodi tulisi varmasti mahtumaan 644PV:hen. ATmega-mikrokontrollereilla on myös hyvä MIPS (Million instructions per second) per MHz-suhde, jonka tärkeyttä käsitellään tarkemmin luvussa 5. Atmega644P:n lohkokaavio on esitetty kuvassa 3 ja ominaisuudet lyhyesti taulukossa 2.




**Kuva 3** ATmega644P lohkokaavio /10/

**Taulukko 2** ATmega644PV ominaisuudet /10/

| **Ominaisuus** | **Arvot/tyyppi** |
|---|---|
| Prosessori | 1-8 MHz sisäinen, 1-10 MHz ulkoinen |
| SRAM | 4 kt |
| EEPROM | 2 kt |
| Flash-muisti | 64 kt |
| Ohjelmoitavat I/O-linjat | 32 kpl |

Tärkeimpiä lisälaitteita olivat JTAG (Joint Test Action Group)- liitäntä piirin ohjelmointia ja debuggausta varten, SPI (Serial Peripheral Interface Bus)- väylä kommunikointiin radiomoduulin kanssa ja sisäinen 8-bitin ajastin/laskuri TIMER2. Muut lisälaitteet ovat sammutettuina. Tässä projektissa prosessoria ajettiin 1 MHz:n taajuudella, vaikkakin tiettyjä testitapauksia varten kellotaajuus nostettiin 8 MHz:iin. Tuotetuilla piirilevyillä on myös paikka ulkoiselle kellolle, jotka ovat tarkemmin kalibroituja kuin sisäiset ja voivat tuottaa korkeampia taajuuksia. Prosessorin toiminnan kannalta tärkeä lisäkomponentti on 32 kHz kide, jolla prosessori voidaan herättää Power Save-tilasta.

Prosessori viettää kummassakin laitteessa suurimman osan ajastaan Power Save-tilassa virran säästämiseksi. Power Save-tilasta herääminen kestää noin 6 kellojaksoa, käyttöjännitteen kadotessa hetkellisesti herääminen kestää pisimmillään n. 65 ms. Projektissa käytettiin 40-pinnistä PDIP (Plastic Dual Inline Package)-pakkausta, joka voidaan asettaa sille tarkoitettuun kantaan ilman pysyvää kiinnitystä. Prototyyppien tekeminen helpottuu huomattavasti käytettäessä PDIP-pakattuja prosessoreita niiden helpon vaihdettavuuden vuoksi. Valitun prosessorin virrankulutus on esitetty taulukossa 3.

**Taulukko 3** Virrankulutuksia datalehden mukaan

| **Tila** | **1 MHz** | **8 MHz** |
|---|---|---|
| Aktiivinen | 0,75 mA | 4,1 mA |
| Idle | 0,23 mA | 0,75 mA |
| Power Save 32 kHz kiteen kanssa | 0,61 µA | 0,61 µA |

**Radiopiiri**

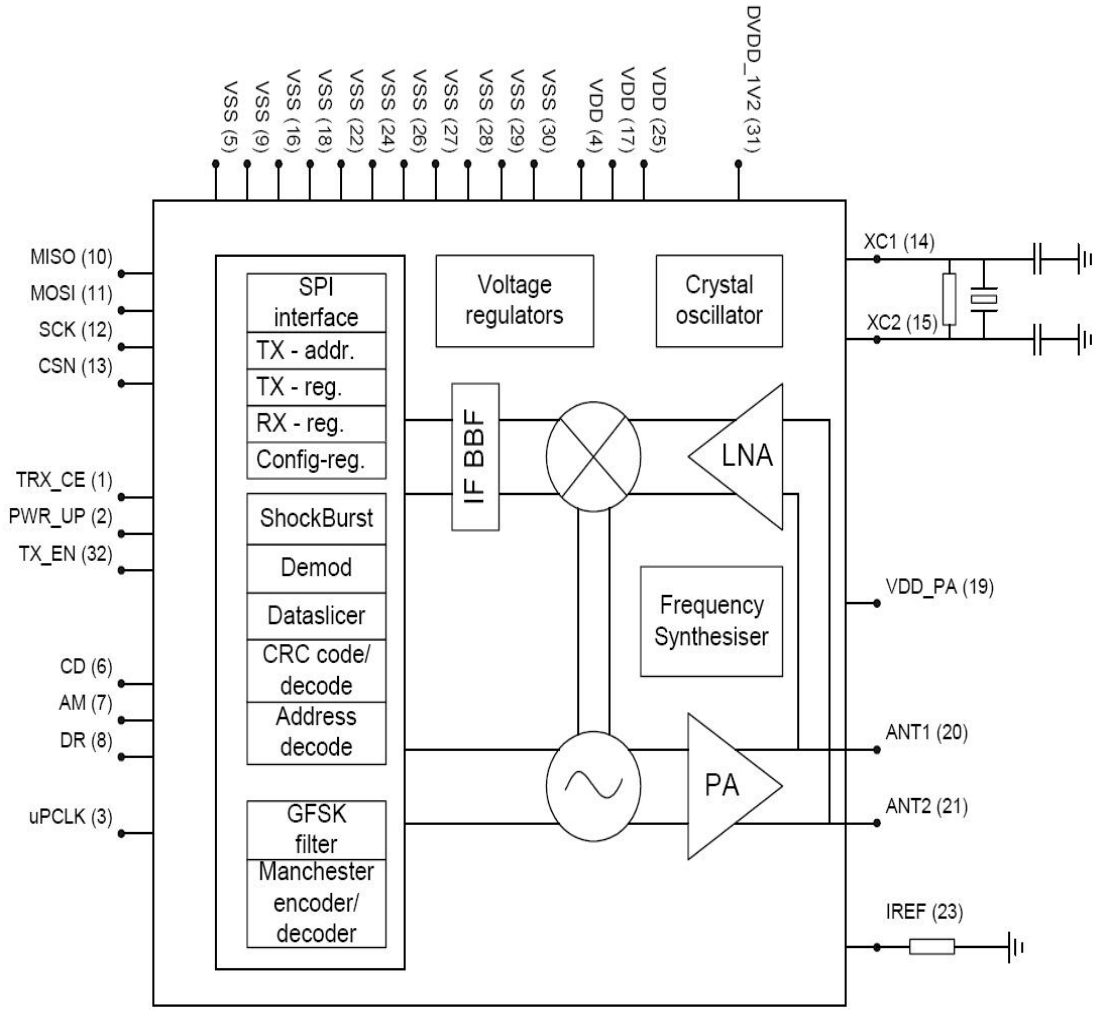
Radiopiiri on komponentti, joka muuntaa mikrokontrollerilta tulevan datan siirtotielle radiosignaaliksi antennin ja sovituskomponenttien kautta, yhdessä nämä komponentit muodostavat lähetinvastaanottimen. Lähetys ja vastaanotto eivät voi olla samaan aikaan päällä samassa laitteessa. Radiolähetinvastaanottimille kyky siirtyä nopeasti unitilaan toiminnan loputtua on tärkeä virrankulutuksen madaltamiseksi.

Tässä työssä käytetty Nordic Semiconductorin valmistama radiopiiri nRF905 voidaan yhdistää mikrokontrolleriin SPI-väylän ja ohjelmoitavien I/O-linjojen kautta. nRF905 kykenee toimimaan 433 tai 868 ja 915 MHz taajuusalueella. Radiopiirille lähetetty data muunnetaan GFSK (Gaussian Frequency Shift Keying)-moduloiduksi ja Manchester-koodatuksi 50 kb/s signaaliksi. nRF905 osaa itse muodostaa paketin, joka koostuu esiosasta, lähetysosoitteesta, dataosasta ja CRC:sta. Yhteen pakettiin mahtuu maksimissaan 32 tavua hyötydataa. Virrankulutusta nRF905:ssä pystyttiin optimoimaan hyödyntämällä Shockburst-ominaisuutta, jonka avulla radiopiiri viestii mikrokontrollerille löydetystä kantoaallosta, tulevasta paketista, luettavasta datasta tai lähetyksen valmistumisesta. Ominaisuuden ansiosta mikrokontrollerin ei tarvitse jatkuvasti vahtia radiopiiriä, mikä sallii tehokkaamman ohjelmiston luomisen unitilo-

ja käsitellessä. /11/ Virrankulutukset datalehden mukaan on esitetty taulukossa 4 ja lohkokaavio kuvassa 4.

**Taulukko 4** Virrankulutuksia datalehden mukaan (16 MHz kellotaajuus)

| Tila | Virrankulutus |
|---|---|
| Standby | 32 µA |
| Vastaanotto | 12,2 mA |
| Vastaanotto pienennetyllä teholla | 10,5 mA |
| Lähetys -10 dBm teho | 9 mA |
| Lähetys 10 dBm teho | 30 mA |
| Power Down | 2,5 µA |

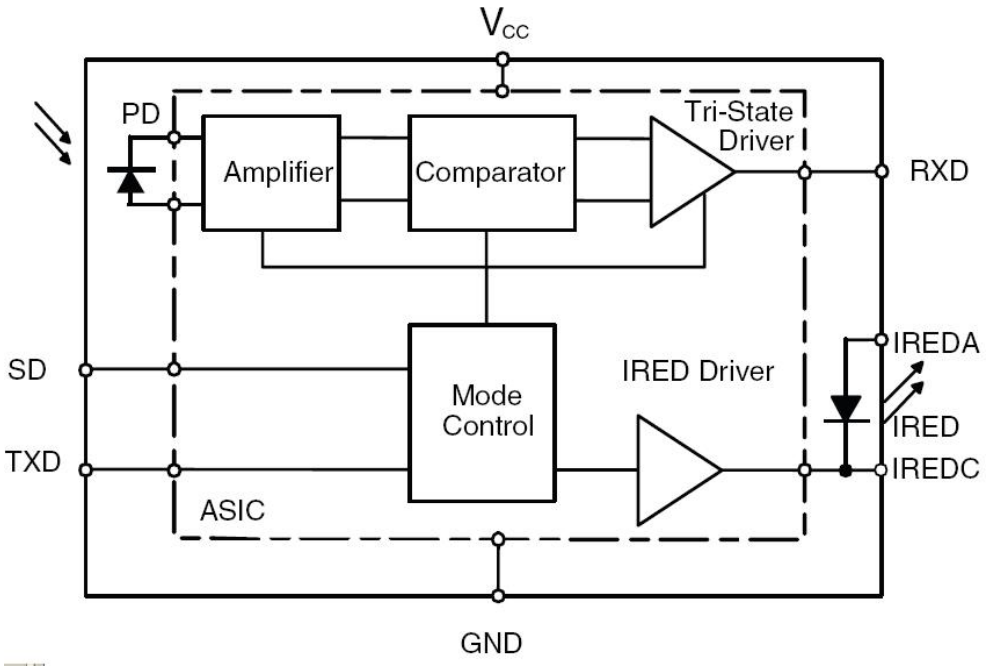



**Kuva 4** nRF905 lohkokaavio

**Infrapunalähetinvastaanotin**

Yksi projektin pääkohdista oli symmetrisen salausavaimen jakaminen turvallisella tavalla. Laitteiden radiomoduulit eivät sovellu tähän tehtävään niiden laajan kuuluvuuden vuoksi. TTY:n Rauman tutkimusyksikössä on pohdittu useita eri vaihtoehtoja, ja tätä projektia varten päätettiin tutkia infrapunan soveltuvuutta avainten jakamiseen. Infrapunasäteily on ihmissilmälle näkymätöntä sähkömagneettista säteilyä, joka sijaitsee näkyvän valon ja mikroaaltojen välissä. Infrapunasäteilyä käytetään hyväksi laajalti sekä sotilaallisissa että siviilisovelluksissa.

Infrapuna on siirtotienä turvallisempi kuin radiotie. Siirtoetäisyys on yleensä muutamista kymmenistä senteistä muutamiin metreihin, mikä haittaa signaalin tarkkailua, vaikka infrapuna voikin heijastua tietyistä pinnoista. Signaali itsessään moduloidaan yksinkertaisella tavalla, infrapunavalon läsnäolo merkitsee loogista ykköstä ja puute loogista nollaa. Projektiin valittiin Vishayn IrDA-yhteensopiva infrapunalähetinvastaanotin TFBS4650, valinta tehtiin laitteen matalan käyttöjännitealueen ja yhdistetyn lähetinvastaanotin toiminnallisuuden vuoksi /12/. Kuvassa 5 on esitetty komponentin lohkokaavio.

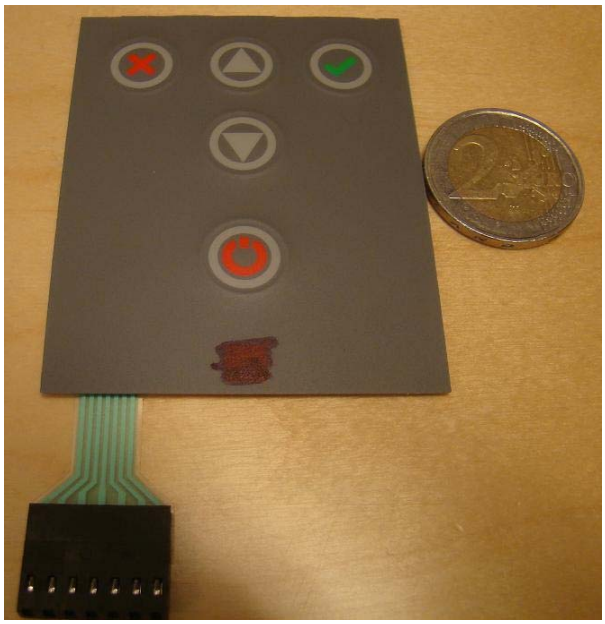



**Kuva 5** TFBS4650 lohkokaavio

TFBS4650 on kooltaan pieni (6,8 mm * 2,8 mm * 1,6 mm) ja pystyy maksimissaan 115 kbit/s tiedonsiirtonopeuteen.

### 3.1.2 Kauko-ohjain

Kauko-ohjain, kuten oviyksikkö, saa käyttöjännitteensä kolmesta 1,5 voltin AA-paristosta. Piirilevyn regulaattori laskee 4,5 voltin sisään tulevan jännitteen 3,0 voltiksi. Regulaattoria käytetään kahdesta eri syystä. Ensinnäkin muutamat komponentit eivät kestäisi suoraa 4,5 voltin käyttöjännitettä ja toiseksi regulaattori turvaa laitteen toimintaa pitemmäksi ajaksi, kun paristojen jännite alkaa ajan kuluessa tippua. Laitteen käyttäminen perustuu kuvassa 6 esitettyyn kalvonäppäimistöön, jossa on viisi näppäintä ja näistä neljä ylintä on käytössä. Kolme ylintä näppäintä vasemmalta oikealle ovat numerot 1-3 ja näiden alapuolella oleva näppäin numero neljä. Käyttäjän näppäiltyä neljä numeroa, kauko-ohjain yrittää aloittaa keskustelun oviyksikön kanssa. Laitteessa olevat LEDit, punainen ja vihreä, kertovat välkähtämällä, oliko toimenpide onnistunut vai ei. Vihreä LED ilmoittaa onnistuneesta toimenpiteestä. Liitteessä 2 on esitetty sekä kauko-ohjaimen että oviyksikön piirikaavio.



**Kuva 6** Kalvonäppäimistö

### 3.1.3 Oviyksikkö

Oviyksikön lukkoa ohjaavat komponentit on sijoiteltu erilliselle pienelle piirilevylle, joka sisältää releen, estosuuntaisen diodin ja transistorin etuvastuksen kanssa. Diodi on piirilevyllä estämässä releen toiminnasta mahdollisesti aiheutuvia haitallisia virtapiikkejä ja transistori virranvahvistimena. Erillinen pieni piirilevy on esitetty liitteessä 1.

### 3.1.4 Sähköinen lukko

Järjestelmässä käytetty lukko on kuvassa 1 esitetty Schlage FE595, jossa on ulkopuolen kuoressa näppäinlukko ja avaimenreikä lukon avaamista varten. Sisäpuolen kuoressa on vipu, jolla lukko voidaan asettaa lukittu/lukitsematon-tilaan. Lukko käyttää 9 voltin paristoa sisäistä elektroniikkaansa varten, joka valmistajan datalehden mukaan käyttöasteesta riippuen sisältää 300–600 mAh /13/. Lukon oma elektroniikka ei vie sähköä silloin kun se ei ole käytössä. Sisäpuolen vivun havaittiin sulkevan kytkimen, ja tämä asetti kaksi virtajohdinta oikosulkuun ja avasi lukituksen. Lukon avaaminen oviyksiköstä perustuu releen pitämiseen suljetussa tilassa määritellyn ajan verran, mikä oikosulkee virtajohtimet ja avaa lukon. Käytetty rele on normaalisti avoin. Lukko palautuu vivun määrittämään tilaan, jos oviyksiköstä katoaa käyttöjännite.

## 3.2 Ohjelmisto

### 3.2.1 Kehitysympäristö

Kehitysympäristönä oli AVR Studio 4.13 SP2 ja WinAVR 20080610 mukana tuleva avr-gcc kääntäjä. Ohjelmointia varten oli SAMK:n Tekniikan Porin yksiköstä lainattu Atmel AVR STK500 Starter Kit ja myöhemmin hankittiin sekä ohjelmointia että debuggausta varten Atmel AVR JTAGICE mkII.

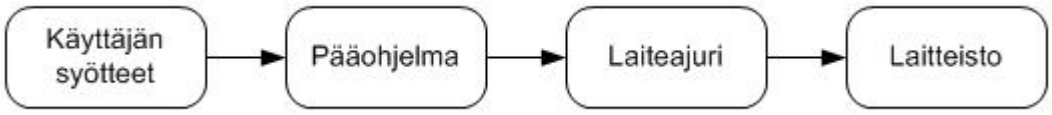
AVR Studio on Atmelin kehittämä vapaasti ladattavissa oleva ohjelmistonkehitykseen ja debuggaukseen suunniteltu IDE, jonka mukana tulee assembler kääntäjä. Avoimen lähdekoodin WinAVR on kokoelma ohjelmia Atmel AVR RISC-prosessoreiden ohjelmointiin ja debuggaukseen, tärkein näistä ohjelmista oli avr-gcc kääntäjä, jonka voi yhdistää AVR Studio-ohjelmaan. Ohjelmistokieleksi vaihtoehtoina olivat assembler tai C. Assembler tuottaa osaavan ohjelmoijan käsissä paremmin optimoitua koodia ja sallii mikrokontrollerin tarkemman hallinnan, mutta on hitaampaa kirjoittaa ja lukea kuin C, joka on korkean tason kieli ja tuottaa enemmän helppolukuista koodia pienemmässä ajassa kuin assembler; huonoja puolia ovat suurempi koodin koko ja heikompi optimisaatio. Projektiin valittiin C-kieli koska se arvioitiin helppokäyttöisemmäksi ohjelmointikieleksi tälle projektille.

### 3.2.2 Laitteiden ohjelmisto yleisesti

Toteutettavan ohjelmiston toimintoja rajaa laitteisto, joka määrittää käytettävissä olevat ominaisuudet, hyvällä ohjelmoinnilla voidaan laitteiston tarjoamia mahdollisuuksia hyödyntää tehokkaasti. Sulautetussa tietotekniikassa on laitteen monimutkaisuudesta riippuen mahdollisuus toteuttaa ohjelmisto käyttöjärjestelmällä keskeytyksien avulla tai imperatiivisesti yksi käsky kerrallaan etenevässä järjestyksessä. Käyttöjärjestelmäratkaisu todettiin tarpeettomaksi projektin ohjelmiston yksinkertaisuuden vuoksi, käytetty toteutus on sekoitus keskeytystoiminnallisuutta ja peräkkäin suoritettuja käskyjä. Ohjelmiston perustoiminta-ajatus kummassakin laitteessa on

unitilassa pysyminen, kunnes herätään keskeytyksen toimesta suorittamaan jotakin tehtävää, keskeytys voi johtaa pitempään käsittelyyn, jossa käytetään peräkkäin suoritettuja käskyjä.

Laitteiden ohjelmisto jaettiin pää-, alustus- ja laiteajuritiedostoihin. Laiteajurit sisältävät tarvittavat aliohjelmat eri lisälaitteiden ja väylien käyttöön, alustustiedosto sisältää asetukset mikrokontrollerin I/O-linjoille ja lisälaitteille ja päätiedosto varsinaisen ohjelmakoodin sekä keskeytykset. Toimintojen jakaminen erillisiin tiedostoihin helpottaa muutosten tekoa sekä uudelleenkäytettävyyttä. Laiteajurit ja alustustiedosto kirjoitettiin ensin, koska käytetyt väylät, lisälaitteet ja I/O-linjat olivat jo tiedossa. Kummankin laitteen päätiedostot kehittyivät kirjoitusprosessin aikana, suurimmat parannukset tulivat ajoitusten tarkentamisesta, aliohjelmien joustavuuden lisäämisestä parametrien kautta sekä ajastinten tehokkaammasta hyödyntämisestä. Kuvassa 7 on esitetty eri tiedostojen sijainti laitteen toimintaketjussa.

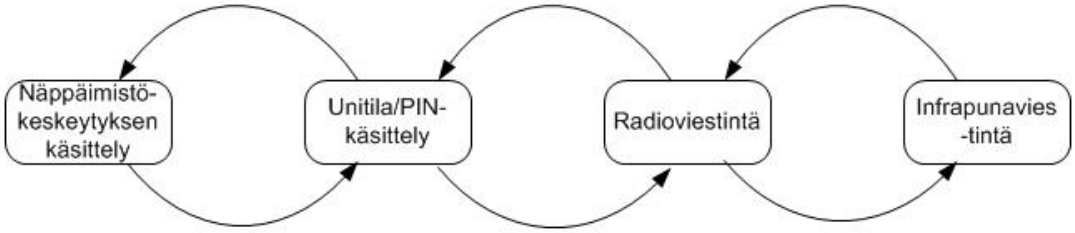



**Kuva 7** Tiedostojen sijainti toimintaketjussa

### 3.2.3 Kauko-ohjaimen toimintalogiikka

Kauko-ohjain on laite, joka herää toimimaan vain ja ainoastaan käyttäjän näppäinpainallusten toimesta. Herätykseen käytetään I/O-linjan tasonmuutoksen keskeytystä, jossa tarkistetaan, missä tilassa linja on ja sen perusteella päätetään, kirjataanko näppäinpainallus vai onko kyseessä nouseva näppäin. Painalluksen tapahtuessa kirjataan näppäintä vastaava numero, joita kerätään kunnes PIN-luvussa on tarvittu määrä numeroita, luvun pituus on järjestelmän tämän hetkisessä toteutuksessa määritelty neljän numeron pituiseksi. Ohjelma palaa unitilaan painalluksen jälkeen, mikäli PIN-luku ei ole vielä täysin muodostettu. PIN-luvun täyttyessä siirrytään radioviestintäosaan. Kauko-ohjain ei ota mitään kantaa PIN-lukuun vaan välittää sen oviyksikölle,

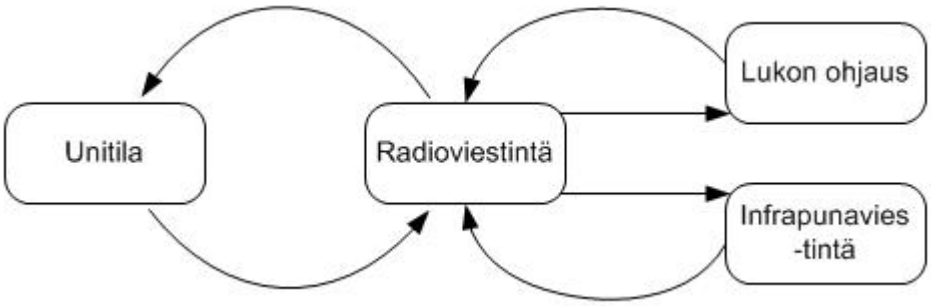
jossa päätetään suoritettava toiminto. Kuvassa 8 on esitetty kauko-ohjaimen eri tilat ja siirtymät niiden välillä.




**Kuva 8** Kauko-ohjaimen toiminta tilatasolla

### 3.2.4 Oviyksikön toimintalogiikka

Oviyksikön täytyy olla jatkuvasti valmiina vastaanottamaan kauko-ohjaimen lähettämiä sanomia, jatkuva radiotien kuuntelu ei kuitenkaan pariston eliniän kannalta ole järkevää. Laite herää tietyin väliajoin kuuntelemaan radiotietä tulevien viestien varalta. Jos oviyksikkö vastaanottaa sille tarkoitetun synkronointisanoman, aloitetaan radioviestintä. PIN-lukuihin liitetyt toiminnot löytyvät vain ja ainoastaan oviyksikön muistista, näiden lukujen perusteella vastaanotettu sanoma joko hylätään tai käynnistetään siihen liitetty toiminto. Kuvassa 9 on esitetty oviyksikön eri tilat ja siirtymät niiden välillä.




**Kuva 9** Oviyksikön toiminta tilatasolla

## 3.3 Radioprotokolla

Ohjelmistossa ei käytetty valmista protokollaa, vaan sen tekeminen oli osa opinnäytetyötä. Luvussa 2.3 käsiteltiin jo lyhyesti kauko-ohjaimen käyttöluonteen kommunikoinnille asettamia vaatimuksia, jotka vaikuttavat suorasti myös radioprotokollaan. Virrankulutuksen optimaalista mallia mietittäessä ymmärrettiin oviyksikön suurempi virrankulutus kauko-ohjaimeen verrattuna, mikä johtuu oviyksikön tarpeesta herätä tietyin väliajoin kuuntelemaan radiotietä. Ainoa tapa jolla virrankulutusta pystytään protokollan toimesta merkittävästi madaltamaan oviyksikössä, on kasvattaa radiotien kuunteluun tarkoitettujen jaksojen aikaväliä. Jotta järjestelmän toiminta-varmuus radioviestien havaitsemisen suhteen pysyisi yhä mahdollisimman korkeana, kauko-ohjaimen täytyy lähettää vastaavasti pitempiä synkronointipurskeita. Pitkät synkronointipurskeet, joiden tarkoitus on ilmoittaa oviyksikölle alkavasta keskustelusta, lisäävät virrankulutusta kauko-ohjaimessa, mutta tasaavat koko järjestelmän virrankulutusta ja siten oviyksikön elinikää. Luvussa 5 on pohdittu eripituisten synkronointijaksojen vaikutusta koko järjestelmän elinikään.

### 3.3.1 Sanomatyypit ja pakettirakenne

Protokolla käyttää neljää erilaista sanomatyyppiä, jotka ovat SYNC (Synchronise), PIN, ACK (Acknowledged) ja NACK (Not Acknowledged). SYNC toimii keskustelun aloittajana ja se sisältää TIMER2-laskurin arvon, joka on väliltä $1 > x > 0$ sekuntia. PIN sanoma on salattu ja sisältää käyttäjän näppäilemän PIN-luvun. ACK ja NACK ovat oviyksikön vastaussanomia. Taulukossa 5 on esitetty radiopiirin sanoman yleinen rakenne ja varsinaisen datapaketin rakenne on esitetty taulukossa 6.

**Taulukko 5** Radiopiirin sanoman rakenne

| | | | |
|---|---|---|---|
| Preamble 10 bit | Address 8 bit | Payload 8–72 bit | CRC 16 bit |

**Taulukko 6** Payload rakenne

| | | |
|---|---|---|
| Msg_type 8 bit | TIMER2_value 8 bit, vain SYNC-sanomat | Data 64 bit, vain PIN-sanomat |

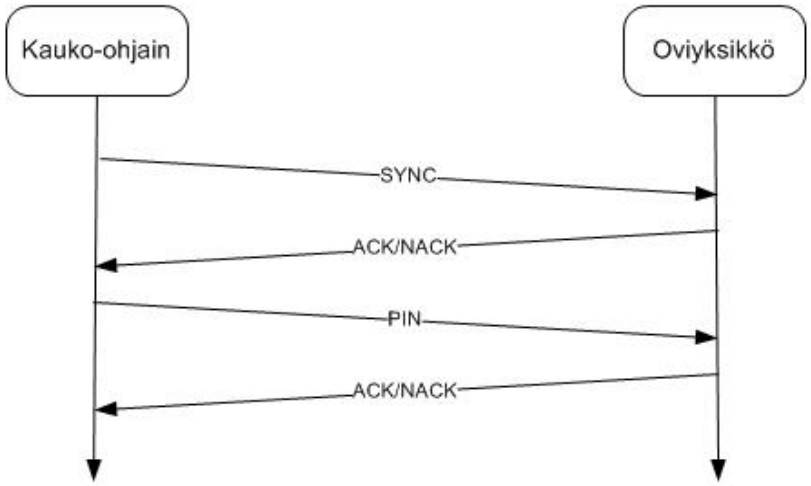
Preamble on radiopiirin lisäämä 10 bittiä pitkä bittikuvio, joka auttaa vastaanotinta tulevan sanoman aistinnassa. Address-osa voi olla 1-4 tavua pitkä riippuen toteutuksen tarpeista, pitempi osoite on parempi, jos halutaan välttää tahattomat vastaanotot monta laitetta sisältävissä verkoissa. Payload sisältää varsinaisen lähetettävän datan ja voi olla 1-32 tavua pitkä. Radiopiiri lisää haluttaessa automaattisesti 8- tai 16-bittiä pitkän CRC:n. Payload osa sisältää ensimmäiseksi 8-bitin viestityypin, jonka perusteella laitteet tunnistavat käsiteltävän sanoman. TIMER2-arvo sisältyy vain SYNC-sanomiin. Data koostuu salatusta PIN-luvusta.

### 3.3.2 Protokollan toiminta

Tässä luvussa käsitellyn termin “kommunikaatiotapahtuma” merkitys sisältää muutamia eroja laitteesta riippuen. Kauko-ohjaimen kommunikaatiotapahtuma alkaa synkronisaatiopurskeesta ja päättyy toiseen oviyksikön ACK/NACK-sanomaan. Oviyksikön kommunikaatiotapahtuma alkaa siitä, kun sille tarkoitettu synkronointisanoma on havaittu ja päättyy toisen ACK/NACK-sanoman lähetykseen kauko-ohjaimelle.

Radiokeskustelu laitteiden välillä alkaa vain ja ainoastaan käyttäjän näppäiltyä PIN-sanoman. Ensimmäinen lähetettävä viesti on kauko-ohjaimen SYNC-sanoma, jota lähetetään jatkuvasti yhden sekunnin ajan, jos siirtotiellä ei havaita liikennettä. Oviyksikkö herää 898 ms välein kuuntelemaan siirtotietä mahdollisten sanomien varalta, kuuntelu kestää 7,8 ms. Vastaanotettu synkronointisanoma sisältää TIMER2-laskurin arvon, josta oviyksikkö pystyy laskemaan kuinka kauan synkronointipurskетta lähetetään. Laskurin saavuttaessa maksimiarvonsa oviyksikkö odottaa vielä millisekunnin ja lähettää sen jälkeen ACK-sanoman, jos vastaanotettu synkronointisanoma oli odotetun mukainen tai NACK-sanoman, jos synkronointisanomassa oli virhe. ACK-sanoman vastaanottaessaan kauko-ohjain kokoaa PIN-sanoman, salaa sen ja lähettää oviyksikölle. Oviyksikössä salaus puretaan ja lähetyslaskurin arvo tarkistetaan laitteen muistissa olevia arvoja vastaan. Jos lähetyslaskuri ei ole sama kuin oviyksikössä oleva, laskureita verrataan muutamalla lähiarvolla ja tämän epäonnistuessa vastataan NACK-sanomalla. Kauko-ohjaimesta on mahdollista lähettää etuoikeutettu sanoma, jolla lähetyslaskurit voidaan nollata kummassakin laitteessa. Lähe-

tyslaskurien vastatessa toisiaan tarkistetaan vastaako PIN-luku jotain oviyksikön muistissa olevaa komentoa. Jos vastaava luku löytyy, lähetetään ACK-sanoma, kasvatetaan lähetyslaskuria oviyksikössä ja suoritetaan PIN-lukua vastaava toiminto, muussa tapauksessa lähetetään NACK. Kauko-ohjaimessa kasvatetaan lähetyslaskuria jos vastaukseksi saadaan ACK. Kuvassa 10 on esitetty yksi kommunikaatiotapahtuma laitteiden välillä.




**Kuva 10** Yksinkertainen keskustelumalli yhdestä kommunikaatiotapahtumasta

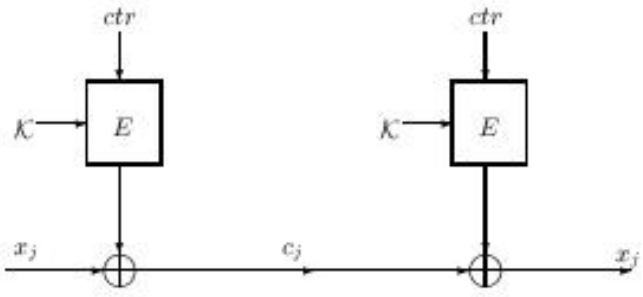
### 3.3.3 Protokollan heikkoudet

Protokollassa on haavoittuvaisuus häirinnälle, riippuen häirinnän hetkestä vaikutukset ovat eri luokkaa. Tarpeeksi voimakkaalla häirinnällä voidaan estää toiminta missä tahansa vaiheessa, mutta suurin haitta saadaan aikaan häiritsemällä PIN-sanoman jälkeistä ACK-sanomaa. Jos oviyksikön vastaanottama PIN-sanoma on oikea, laite suorittaa PIN-lukuun kytketyn toiminnon, kasvattaa lähetyslaskuria ja lähettää ACK-sanoman. Ennen tätä ACK-sanomaa suoritettava häirintä johtaa tilanteeseen, jossa oviyksikkö on kasvattanut lähetyslaskuria, mutta kauko-ohjain ei saa viestiä, jonka pohjalta se voisi kasvattaa omaa laskuriaan. Toinen mahdollinen toteutus voisi olla sellainen, jossa oviyksikkö kasvattaa lähetyslaskuriaan ja suorittaa PIN-lukua vastaavan toiminnon vasta kun se on saanut ACK-sanoman lähetettyä. Valitettavasti tämä-

kin toteutustapa on altis hyvin ajoitetulle häirinnälle, tällöin PIN-lukua vastaava toiminto ei tulisi suoritetuksi ollenkaan.

## 3.4 RC5-toimintatila

Symmetrisiä lohkosalaimia voidaan käyttää useissa eri tiloissa, joista kaikki eivät ole yhtä turvallisia /15/. Tätä projektia varten valittiin laskurimoodi eli RC5-CTR mode. Laskurimoodissa salausalgoritmiin syötetään sekä kauko-ohjaimessa että oviyksikössä olevan laskurin arvo, joka salauksen jälkeen XOR:taan varsinaisen selväkielisen tekstin kanssa. Kryptattu teksti voidaan muuttaa oviyksikössä selväkieliseen tekstiin toistamalla sama operaatio, mutta XOR:lla kryptattu teksti salatun laskurin kanssa. Laskurimoodin etuna on muuttuva kryptattu teksti, mikäli käytetyn laskurin luku on eri vaikka selväkielinen teksti ei muuttuisikaan. Kuvassa 11 on esitetty laskurimoodissa tapahtuva salaus ja purkaminen. Termi *ctr* tarkoittaa laskurin lukua, *K* salausavainta, *x* selväkielistä tekstiä ja *c* salattua tekstiä.




**Kuva 11** Laskurimoodin toiminta

## 3.5 Salausavainten vaihtaminen

Salausavainten vaihtaminen on tärkeä ominaisuus, jolla voidaan yrittää puolustautua mahdollista hyökkääjää vastaan jos salaus murretaan. Avainten vaihtoon ei voida käyttää järjestelmän normaalia radiotietä, koska tällöin uusi avain olisi kenen tahansa kuultavissa. Koska avainten vaihto haluttiin toteuttaa langattomasti, siirtotieksi valittiin infrapuna. Kun käyttäjän on näppäillyt oikean PIN-luvun kauko-ohjaimesta salausavainten vaihtoa varten, lähetetään kertaluonteinen numero oviyksikölle, joka

asettaa infrapunakomponentin valmiiksi vastaanottoa varten. Kauko-ohjain täytyy tuoda lähelle oviyksikköä, koska infrapunan kantama virrankulutusta rajoittavan vastuksen vuoksi on maksimissaan noin 40 cm. Rajoitettu kantama infrapunakommunikaatiossa tosin lisää tietoturvaa. Tietyn ajan kuluttua kauko-ohjain lähettää automaattisesti pulssijonon, jonka oviyksikkö ottaa vastaan ja asettaa uudeksi salausavaimen ytimeksi. Valitettavasti toteutus ei onnistunut täysin infrapunakomponentin vastaanotossa ilmenneiden ongelmien vuoksi.

# 4 MITTAUKSET

## 4.1 Mittausympäristö

Radiomoduulien taajuudet oli testattu jo aikaisemmin, mutta uudella testauksella varmistuttiin niiden toimivuudesta, joka olikin varsin hyvä. Muita taajuus- tai ajoitusmittauksia ei suoritettu, koska käytetyille radiomoduuleille oli tehty jo useita vastaavia mittauksia /9/. Käytetyt mittalaitteet on esitetty taulukossa 7.

**Taulukko 7** Mittauksissa käytetyt laitteet

| **Laite** | **Käyttötarkoitus** | **Käyttötarkoitus** |
|---|---|---|
| Agilent E3631A | Tasavirtalähde | Käyttöjännitteen tuottaminen prototyypeille |
| Agilent 34401A | Yleismittari | Jännitteen ja virrankulutuksen mittaus |
| Tektronix TDS3032 | Oskilloskooppi | Ajoitusten, keskeytysten ja prosessien keston mittaus |
| Hewlett Packard 8594E | Spektrianalysaattori | Radiomoduulien taajuusmittaus. |
| Agilent 54622D | Oskilloskooppi | Ajoitusten, keskeytysten ja prosessien keston mittaus |
| GW GDM 393A | Yleismittari | Jännitteen ja virrankulutuksen mittaus |

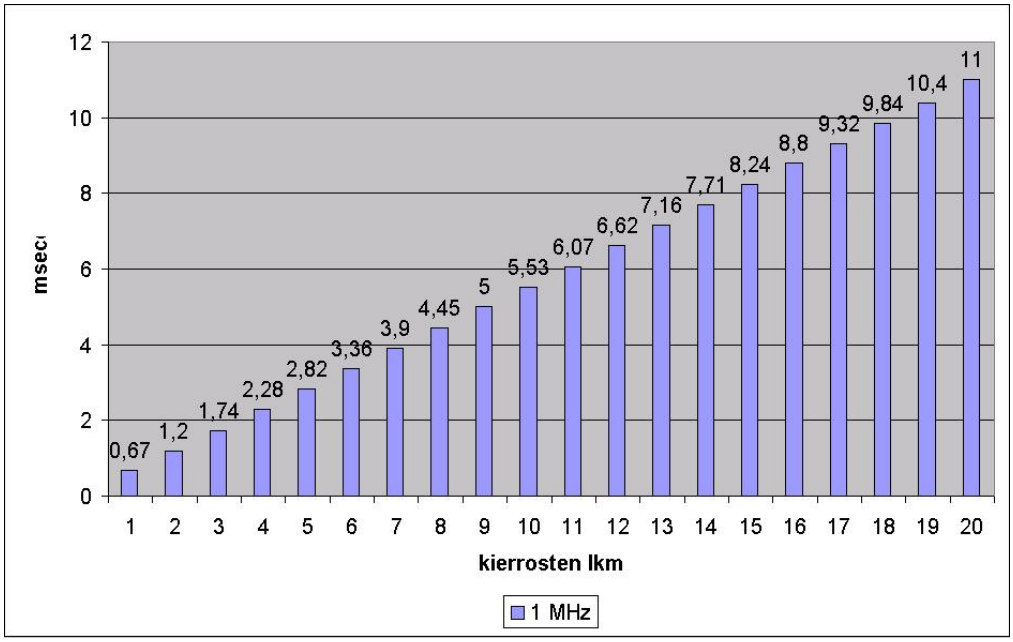
## 4.2 Salausmittaukset

**Mittausjärjestelyt**

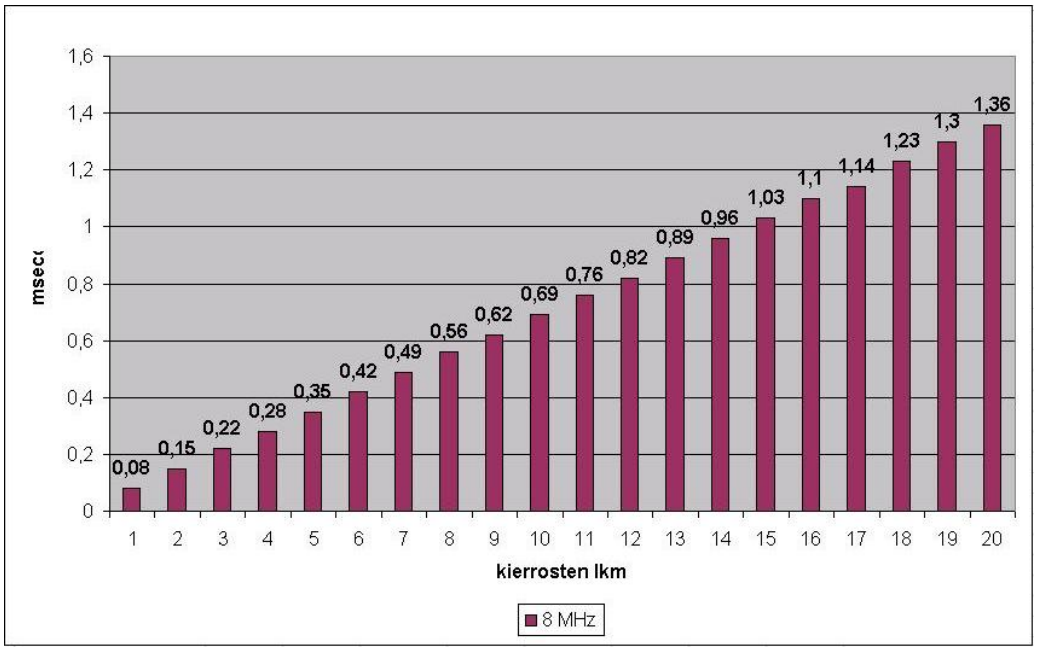
Salausmittauksissa mitattiin kryptauksen ja dekryptauksen kestoa sekä laajennetun salausavaimen luontiaikaa millisekunneissa 1 ja 8 MHz kellotaajuuksilla. RC5-salauksen parametrit testeissä olivat 32-bittinen sanan koko, 1-20 kierrosta sekä 16-tavuinen avain. Testausta varten kirjoitettiin oma pieni testiohjelma, jossa ajettiin ikuisessa silmukassa yllä mainittuja testitapauksia. Testiohjelma käännettiin luvussa 3 mainituilla ohjelmilla ja optimoinneilla. Varsinainen mittaus suoritettiin oskilloskoopilla mittaamalla yhtä I/O linjaa, joka ohjelmoitiin vaihtamaan tilaansa aina kun yksi testitapaus oli suoritettu. Kryptaus ja dekryptaus ovat kestoltaan samanpituisia, joten ne esitellään samoissa Excel kuvakaappauksissa.

**Mittaustulokset**

Kuvassa 12 on esitetty kryptauksen ja dekryptauksen kesto 1 MHz:n kellotaajuudella ja kuvassa 13 8 MHz:n kellotaajuudella. Esitetyt tulokset ovat millisekunteina.

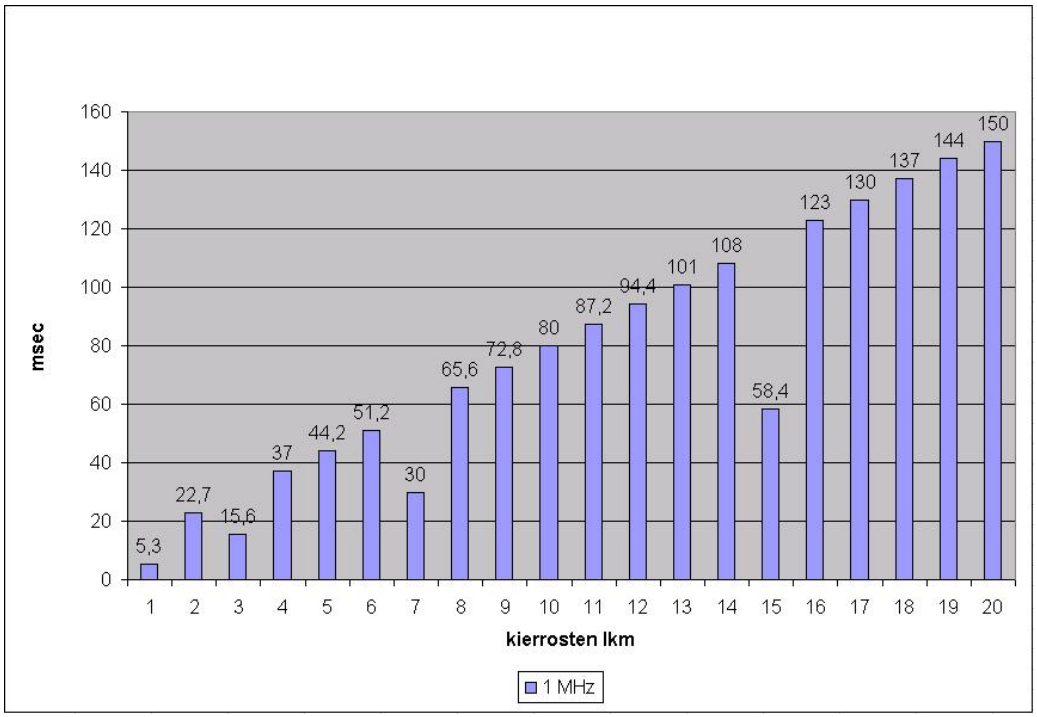



**Kuva 12** Kryptauksen ja dekryptauksen kesto kierroslukumäärän funktiona 1 MHz kellotaajuudella




**Kuva 13** Kryptauksen ja dekryptauksen kesto kierroslukumäärän funktiona 8 MHz kellotaajuudella

Kuvassa 14 on esitetty laajennetun salausavaimen luontiaika millisekunteina. Salauksen parametrit olivat 32/1-20/16 ja kellotaajuus 1 MHz.




**Kuva 14** Salausavaimen laajennuksen kesto kierroslukumäärän funktiona 1 MHz kellotaajuudella

## 4.3 Virrankulutusmittaukset

**Mittausjärjestelyt**

Mittauksen kohteita olivat virrankulutus sekä aktiivi- että unitilassa eri lisälaitteilla ja ilman. Mittaukset suoritettiin 1 MHz kellotaajuudella.

**Mittaustulokset**

Taulukossa 8 on esitetty virrankulutukset eri komponenteille.

**Taulukko 8** Mitattuja virrankulutuksia eri komponenteille eri tiloissa

| Komponentti | Tila | Mitattu virrankulutus | Virrankulutus datalehdestä | Huomioitavaa |
|---|---|---|---|---|
| ATmega644PV | Active | 0,94 mA | 0,75 mA | |
| ATmega644PV | Power Save | 0,5 µA | 0,61 µA | 32 kHz kide liitetty |
| MCP1824 | | 0,110 mA | 0,120 mA | |
| nRF905 | RX | 11,96 mA | 12,2 mA | Normal |
| nRF905 | RX | 10,26 mA | 10,5 mA | Reduced power |
| nRF905 | TX | 24,69 mA | 30 mA | +10 dbm |
| nRF905 | TX | 8,96 mA | 9 mA | -10 dbm |
| nRF905 | Standby | 40 µA | 32 µA | |
| nRF905 | Power Down | 7,5 µA | 2,5 µA | |

## 4.4 Radiokommunikaatiomittaukset

**Mittausjärjestelyt**

Mittauksen kohteita olivat paketin muodostuksen ja lähetyksen kesto eri dataosan pituuksilla, salatun sanoman muodostuksen aikajakauma ja yhden kommunikaatiotapahtuman kesto eri laitteilla. Mittaukset suoritettiin 1 MHz kellotaajuudella ja SPI-väylän kellotaajuus oli 1/16 MHz. Yhden salatun paketin lähettävä aliohjelma koostuu seuraavista osista: muuttujien alustus prosessointia varten, salattavan datan kryptaus, salatun datan pilkkominen tavun kokoisiin paloihin, siirto radiopiirille SPI-väylää pitkin ja varsinainen lähetystapahtuma, jonka kesto riippuu datatavujen määrästä. Lähetyksen keston voi laskea kaavasta 1, joka on todettu mittauksilla päteväk-

si. /11/ Alla esiintyvät arvot ovat mitattuja näillä parametreillä koska niitä käytetään laitteiden välisessä kommunikoinnissa.

**Kaava 1** Time On Air-kaava nRF905 datalehdestä

$$TOA = t_{startup} + t_{preamble} + \frac{N_{address} + N_{payload} + N_{CRC}}{50kbps}$$

**Mittaustulokset**

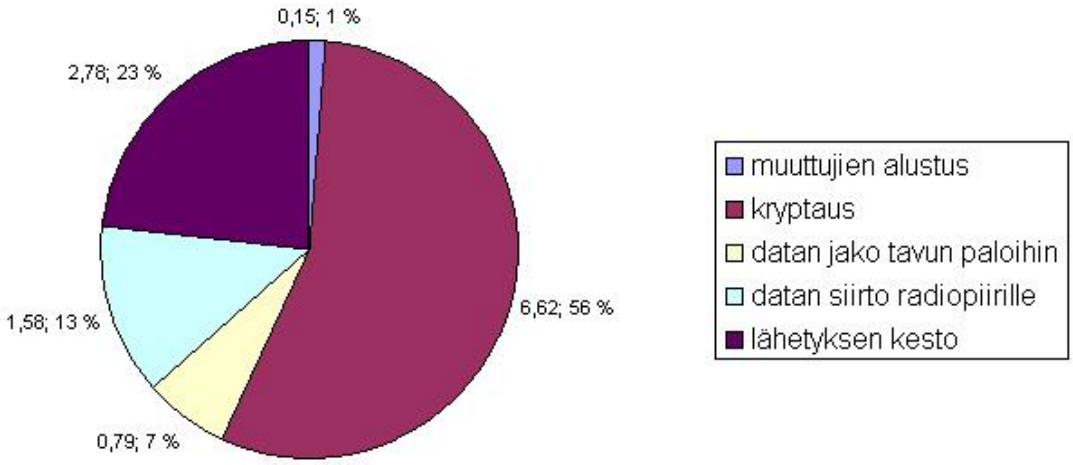
Taulukossa 9 on esitetty radiopaketin lähetyksen kesto eri datatavujen määrällä, taulukossa 10 yhden kommunikaatiotapahtuman kesto eri laitteilla ja kuvassa 15 9-tavuisen, salatun radiopaketin muodostuksen aikajakauma 1 MHz kellotaajuudella ja kuvassa 16 8 MHz kellotaajuudella. Kommunikaatiotapahtuma on määritelty tarkemmin luvussa 3.3.2.

**Taulukko 9** Radiopaketin lähetyksen kesto eri datatavujen määrällä

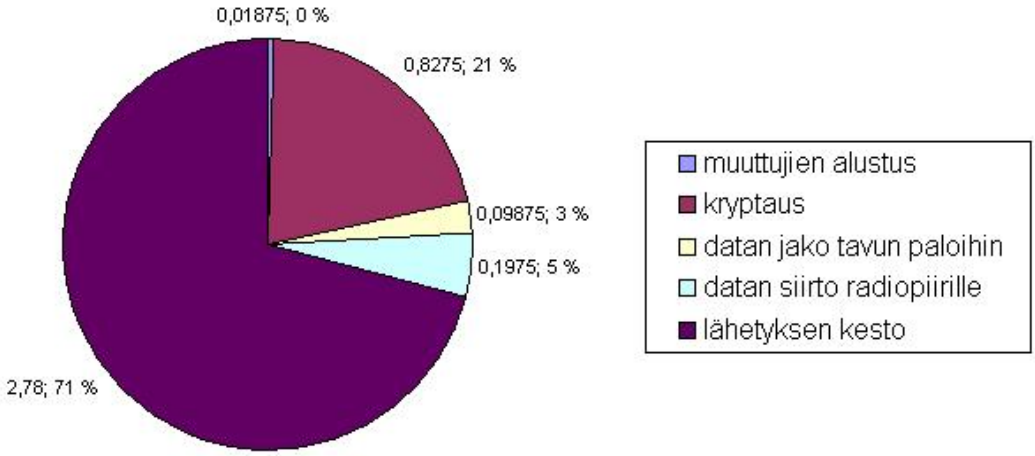
| Datatavujen määrä | Paketin lähetyksen kesto |
|---|---|
| 1 | 1,50 ms |
| 2 | 1,66 ms |
| 9 | 2,78 ms |

**Taulukko 10** Yhden kommunikaatiotapahtuman kesto eri laitteilla

| Laite | Kesto | Muuta huomioitavaa |
|---|---|---|
| Kauko-ohjain | 1028 ms | Alkaa siitä hetkestä kun ensimmäinen SYNC-sanoma on lähetetty |
| Oviyksikkö | 26–1023 ms | Alkaa siitä hetkestä kun SYNC-sanoma on luettu |




**Kuva 15** 9-tavuisen salatun radiopaketin muodostuksen ja lähetyksen aikajakauma 1 MHz kellotaajuudella, arvot millisekunteja**.**




**Kuva 16** 9-tavuisen salatun radiopaketin muodostuksen ja lähetyksen aikajakauma 8 MH kellotaajuudella, arvot millisekunteja.

# 5 ANALYSOINTI

## 5.1 Salausmittausten analyysi

### 5.1.1 Salausavaimen laajennus

Kuvassa 14 esitetyistä tuloksista on nähtävissä laskenta-ajan lineaarinen kehitys kierroslukumäärän funktiona. Tuloksissa on kuitenkin poikkeavuuksia, jotka johtuvat mikroprosessorin käyttämästä modulo-operaatiosta laajennettua salausavainta laskettaessa. Taulun koko tavuina lasketaan kaavasta 2*(r+1), jossa r on kierrosten lukumäärä. Jos taulun kooksi saadaan kahden potenssia oleva luku, modulo-operaatio x % (2*(r+1)) muuttuu summaksi x & (2*(r+1) - 1), joka on huomattavasti nopeampi laskea /14/. Mittauksissa poikkeavat tulokset ilmenivät kääntäjän tekemien automaattisten optimointien kautta.

### 5.1.2 Kryptaus

Kuvissa 12 ja 13 esitetyistä tuloksista on todettavissa salauksen lineaarinen laskenta-aika. Aliohjelma, jolla salaus on toteutettu, koostuu muuttujien alustuksesta ja sijoituksista ja varsinaisesta salauksesta, jonka toiminta on esitetty luvussa 2. Lineaarisuus mittaustuloksissa johtuu aliohjelman toteutuksesta, jossa yhden kierroksen lisäys kasvattaa kierroslaskuria yhdellä, jolloin laskenta-aika kasvaa aina yhden kierroksen laskemiseen kuluvalla ajalla. Yhden salauskierroksen laskenta-ajaksi mitattiin 1 MHz kellotaajuudella 536 µs. Kuvissa 12 ja 13 esitetyistä tuloksista voidaan laskea yhden kierroksen lisäyksen aiheuttama laskenta-ajan kasvu, taulukossa 11 on esitetty tämän kasvun keskiarvo ja keskihajonta. Tulokset tukevat huomiota laskenta-ajan lineaarisesta kasvusta kierroslukumäärän lisäyksen johdosta, RC5-salauksen lineaa-

rinen laskenta-aika helpottaa prosessien keston ja virrankulutuksen arvioimista ja analysointia.

**Taulukko 11** Salauskierroksen laskenta-ajan kasvun keskiarvo ja keskihajonta

| Kellotaajuus | Keskiarvo | Keskihajonta |
|---|---|---|
| 1 MHz | 0,54 µs | 0,02 µs |
| 8 MHz | 0,07 µs | 0,01 µs |

### 5.1.3 Kellotaajuuden vaikutus salauksen laskenta-aikaan

ATmega-mikrokontrollereilla on salauksen virrankulutuksen analysoinnin kannalta mielenkiintoinen ominaisuus, joka on lähes täydellinen 1 MIPS per MHz-suhde. MIPS eli million instructions per second tarkoittaa prosessorin suorittamien käskyjen lukumäärää per sekunti. Tämä ominaisuus johtuu AVR-arkkitehtuurin kyvystä käsitellä lähes kaikkia operaatioita prosessorin sisäisissä rekistereissä R0-R31 yhdessä kellojaksossa. Ominaisuus on tärkeä, koska sen avulla voidaan arvioida prosessorin kellotaajuuden muutoksen vaikutusta laskenta-aikaan ja virrankulutukseen.

### 5.1.4 Salauksen vaikutus virrankulutukseen

Salaus vaikuttaa virrankulutukseen kolmen eri toiminnon kautta, jotka ovat salausavaimen laajennus, kryptaus ja dekryptaus. Laskettaessa näiden toimintojen virrankulutusta, ainoa muuttuva tekijä on laskentaan käytetty aika. Prosessorin virrankulutus eri toimintoja laskettaessa on vakio, mikäli kellotaajuutta ei muuteta. Kryptaus ja dekryptaus vievät laskettaessa saman määrän aikaa, joten tässä luvussa puhuttaessa kryptauksen virrankulutuksesta voidaan sanan kryptaus tilalle sijoittaa myös dekryptaus. Kryptaukseen käytetty prosessoriaika on kuvassa 12 ja 13 esitettyjen tuloksien mukaan lineaarisesti kasvava, voidaan siis sanoa että vahvempi salaus kasvattaa virrankulutusta. Haastavampi analyysin kohde on salausavaimen laajennuksen poikkeamat, jotka ovat kuvassa 14 esitettyinä, syy poikkeamien esiintymiseen esitetään luvussa 5.1.1. Nämä poikkeamat ovat suuria, 15-kierroksisen salausavaimen laskeminen vie aikaa ja siten virtaa lähes puolet vähemmän kuin 14-kierroksisen sa-

lausavaimen laskenta. Poikkeamien vaikutusta virrankulutukseen voidaan havainnollistaan seuraavalla esimerkillä; tarkkaillaan kahden järjestelmän A ja B virrankulutusta.

Järjestelmässä A on käytössä 12-kierroksinen ja B 15-kierroksinen salaus, oletetaan myös että kummassakin järjestelmässä on MCU:n kellotaajuus 1 MHz ja virrankulutus sama kaikkina ajanhetkinä. Alkutilanteessa kummankin järjestelmän ensimmäinen toimenpide salaukseen liittyen on salausavaimen laajennus. Kuvassa 14 esitettyjen tulosten mukaisesti järjestelmä A käyttää laajennukseen 94,4 ms ja B 58,4 ms. Tässä vaiheessa järjestelmä B on kuluttanut lähes puolet vähemmän virtaa kuin A, vaikka sen käyttämä salaus on vahvempi. Kuvassa 12 esitetyistä tuloksista voidaan todeta, että suuremman kierrosluvun salaus kuluttaa enemmän aikaa ja siten virtaa laskentaan, kuin pienemmän kierrosluvun. Näin ollen voidaan päätellä, että jossakin vaiheessa järjestelmän B kokonaisvirrankulutus salauksesta johtuen (salausavaimen laajennukseen ja n salaustapahtuman laskentaan kuluvan virran summa) tulee olemaan suurempi kuin järjestelmän A. Kaava 2 esittää n toiminnon suorittamiseen kuluvaa keskimääräistä virtaa. Kaavaa on käytetty taulukoiden 12 ja 13 tulosten laskemisessa, joiden avulla havainnollistetaan kuinka vahvempi salaus on tiettyyn rajaan asti virrankulutuksen kannalta tehokkaampi kuin heikompi salaus. Analyysin kohteiksi on otettu 12-kierroksinen salaus, joka on järjestelmässä käytössä ja 15-kierroksinen salaus, joka tuottaa yhden kuvassa 14 nähdyistä poikkeavista arvoista.

**Kaava 2** N toiminnon suorittamiseen kuluva keskimääräinen virta voidaan laskea kaavalla:

$$I_{Avg} = \frac{I_1 * t_{1 + \ldots +} I_n * t_n}{t_{jakso}}$$

Taulukon 12 tuloksista on laskettavissa, että järjestelmässä B virtaa säästetään 0,03744 mA laskettaessa 15-kierroksinen laajennettu salausavain. Taulukossa 13 on laskettu salaukseen kuluva virta 12 ja 15 kierroksella.

**Taulukko 12** Laajennetun salausavaimen laskemiseen kuluva virta 12 ja 15 kierroksella

| Kierroslukumäärä | Laskentaan kuluva aika | Prosessorin ja regulaattorin virrankulutus | Kaavasta 2 laskettu virrankulutus |
|---|---|---|---|
| 12 | 94,4 ms | 1,04 mA | 0,098176 mA |
| 15 | 58,4 ms | 1,04 mA | 0,060736 mA |

**Taulukko 13** Salauksen laskemiseen kuluva virta 12 ja 15 kierroksella

| Kierroslukumäärä | Laskentaan kuluva aika | Prosessorin ja regulaattorin virrankulutus | Kaavasta 2 laskettu virrankulutus |
|---|---|---|---|
| 12 | 6,62 ms | 1,04 mA | 0,0068848 mA |
| 15 | 8,24 ms | 1,04 mA | 0,0085696 mA |

Taulukon 13 tuloksista on laskettavissa, että virtaa säästetään järjestelmässä A 0,0016848 mA laskettaessa 12-kierroksinen salaus verrattuna 15-kierroksiseen salaukseen. Jakamalla laajennetun salausavaimen laskennassa saatava virran säästö salauksesta saatavalla virran säästöllä saadaan tulokseksi 23. Näin ollen 12-kierroksinen salaus on virrankulutuksen kannalta tehokkaampi kuin 15-kierroksinen salaus, jos salaustapahtumia on 23 tai enemmän salausavainten vaihtamisten välillä. Luvun 3 radioprotokollaa käsittelevästä osasta on luettavissa, että yksi kommunikaatiotapahtuma järjestelmässä sisältää 2 salaustapahtumaa parhaimmassa tapauksessa. Tarvittaisiin siis vähintään 12 kommunikaatiotapahtumaa ennen salausavaimen vaihtamista, jotta yllä mainittu tehokkuus saavutettaisiin järjestelmään A valitussa 12-kierroksisessa salauksessa.

Vielä yleisemmällä tasolla asiaa voidaan tutkia muodostamalla lineaarinen funktio, joka kuvaa salausavaimen laajennuksen ja n salauskerran laskemiseen kuluvaa aikaa salauskertojen funktiona. Kaavassa 3 on esitetty funktio $f(x) = t_s*x+t_a$, jossa $t_s$ on yhden salauskerran laskentaan kuluva aika, x salauskertojen lukumäärä ja vakiotermi $t_a$ salausavaimen laajennukseen kuluva aika. Tätä funktiota voidaan hyödyntää, jos halutaan verrata kierroslukumäärältään erilaisten salausten suoritusaikoja. Haluttaessa esimerkiksi laskea kuinka monta salauskertaa tarvitaan ennen kuin 14 kierroksen salaus on kuluttanut enemmän virtaa kuin 15 kierroksen salaus, muodostetaan funktiosta f(x) yhtälöpari, josta ratkaistaan x eli salauskertojen lukumäärä. Kaavassa 3 ei

esiinny virtakomponenttia, koska virrankulutus oletetaan vertailtavissa järjestelmissä olevan vakio kaikkina ajanhetkinä salaukseen liittyvää laskentaa suoritettaessa.

**Kaava 3** Lineaarinen funktio salausavaimen laajennuksen ja n salauskerran ajan laskemiseen salauskertojen lukumäärän funktiona.

$$f(x) = t_s x + t_a$$

Taulukossa 14 on esitetty kaavan 3 avulla laskettuja salauskertojen lukumääriä eri kierrosluvuilla verrattuna 15-kierroksiseen salaukseen.

**Taulukko 14** Kaavan 3 tuloksia eri kierrosluvuilla verrattuna 15-kierroksiseen salaukseen.

| **Kierrosluku** | **Vaadittu salaustapahtumien lukumäärä, jotta saavutettaisiin suurempi tehokkuus kuin 15 kierroksen salauksella.** |
|---|---|
| 12 | 23 |
| 13 | 40 |
| 14 | 94 |
| 15 | 0 |

## 5.2 Virrankulutusmittausten analyysi

### 5.2.1 Laitteiston elinikä

Taulukossa 15 on esitetty taulukon 8, 9 ja 10 tulosten perusteella laskettuja toiminta-aikoja järjestelmälle erilaisissa tilanteissa. Taulukossa on myös laskettu eri regulaattorien arvoilla elinaikoja, 50 ja 10 µA regulaattoreilla lasketut laitteiden eliniät ovat teoreettisia, eivätkä välttämättä vastaa todellisuutta. Tulokset on laskettu kaavasta 2 laajennetuilla versioilla. Laskuissa oletetaan 1500 mAh paristo energianlähteenä, jossa ei tapahdu jännitteen laskua ajan kuluessa. Pitkällä aikavälillä pariston energian pienenee ikääntymisen ja käytön vuoksi. Tällaisen ajan funktiona tapahtuvan energiahukan määräksi on arvioitu noin 10 % vuodessa. Radiomoduuleissa havaittua kasvavan virrankulutuksen ongelmaa ei ole otettu huomioon laskuissa. Tuloksista

tarkastellaan ensin kauko-ohjaimen ja oviyksikön virrankulutusta erikseen ja lopulta niiden yhteistoimintaa.

**Taulukko 15** Laitteiden elinaikoja eri tilanteissa

| Laite | Tila | Elinikä vuosina |
|---|---|---|
| Kauko-ohjain | Jatkuva unitila, regulaattori Iq = 110 µA | 1,5 |
| Kauko-ohjain | Jatkuva unitila, regulaattori Iq = 50 µA | 3,2 |
| Kauko-ohjain | Jatkuva unitila, regulaattori Iq = 10 µA | 13,2 |
| Kauko-ohjain | 10 kommunikaatiotapahtumaa päivässä, regulaattori Iq = 110 µA | 1,5 |
| Kauko-ohjain | 10 kommunikaatiotapahtumaa päivässä, regulaattori Iq = 50 µA | 3,2 |
| Kauko-ohjain | 10 kommunikaatiotapahtumaa päivässä, regulaattori Iq = 10 µA | 12,1 |
| Oviyksikkö | Jatkuva unitila, regulaattori Iq = 110 µA | 1,5 |
| Oviyksikkö | Jatkuva unitila, regulaattori Iq = 50 µA | 3,2 |
| Oviyksikkö | Jatkuva unitila, regulaattori Iq = 10 µA | 13,2 |
| Oviyksikkö | Normaali kuuntelu, regulaattori Iq = 110 µA | 0,8 |
| Oviyksikkö | Normaali kuuntelu, regulaattori Iq = 50 µA | 1,0 |
| Oviyksikkö | Normaali kuuntelu, regulaattori Iq = 10 µA | 1,4 |
| Oviyksikkö | 10 kommunikaatiotapahtumaa päivässä, regulaattori Iq = 110 µA | 0,8 |
| Oviyksikkö | 10 kommunikaatiotapahtumaa päivässä, regulaattori Iq = 50 µA | 1,0 |
| Oviyksikkö | 10 kommunikaatiotapahtumaa päivässä, regulaattori Iq = 10 µA | 1,3 |

### 5.2.2 Kauko-ohjaimen virrankulutus

Kauko-ohjaimen virrankulutus koostuu kahdesta eri tilasta, jotka ovat uni- ja kommunikaatiotila. Ensimmäiseksi analysoitiin virrankulutuksen jakautuminen unitilassa eri komponenttien välillä taulukon 8 tietojen perusteella. Taulukossa 16 on esitetty prosentuaalinen jakauma eri komponenttien virrankulutuksen välillä. Infrapunakomponenttia ei ole huomioitu laskuissa, koska sen virrankulutus sammutettuna on äärimmäisen pieni.

**Taulukko 16** Komponenttien virrankulutuksen jakautuminen unitilassa

| **Komponentti** | **Virrankulutus** | **Prosentuaalinen osuus** |
|---|---|---|
| Regulaattori Iq = 110 µA, järjestelmässä käytössä oleva komponentti | | |
| ATmega644PV | 0,5 µA | 0,6 % |
| nRF905 | 7,5 µA | 6,4 % |
| Regulaattori | 110 µA | 93 % |
| Regulaattori Iq = 50 µA | | |
| ATmega644PV | 0,5 µA | 0,9 % |
| nRF905 | 7,5 µA | 12,9 % |
| Regulaattori | 50 µA | 86,2 % |
| Regulaattori Iq = 10 µA | | |
| ATmega644PV | 0,5 µA | 2,7 % |
| nRF905 | 7,5 µA | 41,7 % |
| Regulaattori | 10 µA | 55,6 % |

Tuloksista voidaan todeta, että regulaattorin valinta ei ollut paras mahdollinen. Valittu regulaattori kuluttaa erittäin paljon virtaa verrattuna muihin komponentteihin, mikä johtaa tavallista korkeampaan virrankulutukseen unitilassa. Taulukossa 17 on esitetty virrankulutuksen jakautuminen eri käyttöasteille, jotka ovat käyttökertoja per päivä. Laskut suoritettiin taulukkojen 8, 9 ja 10 tietojen perusteella käyttämällä kaavaa 2, jossa jaksonpituus oli yksi päivä sekunteina. Tuloksista on nähtävissä, että jopa 100 käyttökerralla päivässä unitilan virrankulutuksen % -osuus on yli 90 %.

**Taulukko 17** Eri käyttöasteiden elinaika kauko-ohjaimelle

| **Käyttöaste** | **Aktiivisen tilan virrankulutuksen % -osuus** | **Unitilan virrankulutuksen % -osuus** | **Elinikä päivinä** |
|---|---|---|---|
| 0 | 0 | 100 | 553 |
| 20 | 1,6 | 98,4 | 541 |
| 50 | 5,0 | 95,0 | 525 |
| 80 | 7,8 | 92,2 | 510 |
| 100 | 9,5 | 90,5 | 500 |

### 5.2.3 Oviyksikön virrankulutus

Toisin kuin kauko-ohjaimen, oviyksikön toimintasykli on tunnettu. Luvun 3.3.2 määrittelyn mukaan oviyksikkö on 898 ms unitilassa ja herää 7,8 ms:ksi kuuntelemaan radiotietä. Seuraavissa laskuissa on oletettu, että synkronointipursketta kestää sen havaitsemisen jälkeen täydet 1000 millisekuntia. Virrankulutuksen jakautuma unitilassa, joka on esitetty taulukossa 16, on sama kuin kauko-ohjaimessa identtisen laitteiston vuoksi. Kuuntelun ja unitilan virrankulutuksen jakautuma on esitetty taulukossa 19, vertailu on yhtä 0,91 sekunnin jaksoa kohden. Taulukossa 18 on esitetty arvot kolmelle eri regulaattorille, 110 µA arvot ovat järjestelmässä käytössä olevan regulaattorin jakautuma ja 50 ja 10 µA jakautumat ovat teoreettisia arvoja.

**Taulukko 18** Oviyksikön virrankulutuksen jakautuminen eri tilojen välillä normaalin kuuntelun aikana

| Tila | Virrankulutus | Kesto | Prosentuaalinen osuus |
|---|---|---|---|
| Regulaattori Iq = 110 µA | | | |
| Uni | 0,113 mA | 0,898 s | 50,02 % |
| Aktiivinen | 13 mA | 0,0078 s | 49,98 % |
| Regulaattori Iq = 50 µA | | | |
| Uni | 0,053 mA | 0,898 s | 31,94 % |
| Aktiivinen | 13 mA | 0,0078 s | 68,06 % |
| Regulaattori Iq = 10 µA | | | |
| Uni | 0,013 mA | 0,898 s | 10,32 % |
| Aktiivinen | 13 mA | 0,0078 s | 89,68 % |

Aktiivisen tilan kuunteluun käytettävää aikaa testattiin pienemmillä arvoilla mutta tämä johti jatkuvasti menetettyihin paketteihin. Unitilan kesto on mitoitettu kauko-ohjaimen synkronointisanomaan, jonka pituutta kasvattamalla voidaan kasvattaa myös oviyksikön unitilan pituutta samalla määrällä. Oviyksikön virrankulutukseen vaikuttaa oleellisesti se, missä vaiheessa synkronointipursketta herätään kuuntelemaan siirtotietä. Synkronointipurske kestää sekunnin mutta riippuen vastaanotetusta ajastinarvosta ei mikrokontrolleria kannata välttämättä enää sammuttaa, jos synkronointi on jo loppumassa. Taulukossa 19 on esitetty elinaikoja oviyksikölle eri käyttöasteilla.

**Taulukko 19** Eri käyttöasteiden elinaika oviyksikölle

| Käyttöaste | Aktiivisen tilan virrankulutuksen % -osuus | Unitilan virrankulutuksen % -osuus | Elinikä päivinä |
|---|---|---|---|
| 0 | 0 | 100 | 279 |
| 20 | 4,7 | 95,3 | 266 |
| 50 | 11 | 89 | 248 |
| 80 | 16,5 | 83,5 | 233 |
| 100 | 19,9 | 80,1 | 224 |

## 5.3 Radiokommunikaatiomittausten analyysi

Luvun 4.4 taulukoissa 9 ja 10 ja kuvissa 15 ja 16 esitetyistä tuloksista on huomattavissa virrankulutuksen ja viestinnän käyttämän ajan kannalta tärkeitä seikkoja, jotka liittyvät radiotiellä tapahtuvaan kommunikointiin. Ensinnäkin yhden sanoman lähetys on kestoltaan riippuvainen vain ja ainoastaan dataosan pituudesta, koska muut muuttujat pysyvät samoina kaikissa tilanteissa tässä järjestelmässä. Sanoman muodostukseen vaikuttaa MCU:n kellotaajuus, jota nostamalla on mahdollista lyhentää sanoman muodostuksen ja lähetyksen yhteenlaskettua aikaa. Muiden parametrien pienentäminen ei ole mahdollista, osoite on jo pienin mahdollinen leveydeltään ja CRC-summan pienentäminen heikentäisi turvallisuutta. Toiseksi oviyksikön kommunikaatiotapahtuman pituus on vaihteleva riippuen siitä, missä vaiheessa se havaitsee kauko-ohjaimen synkronointipurskeen ja kuinka kauan purske kestää vielä sen jälkeen kun se on havaittu. Jos radiopiiri joutuu kuuntelemaan täydet 7,8 ms radiotietä havaitakseen purskeen, virrankulutus on luonnollisesti suurempi kuin jos purske havaittaisiin nopeammin. Oviyksikön virrankulutuksen kannalta on myönteistä, jos purske havaitaan kun se on vasta alkanut. Tässä tapauksessa MCU voidaan asettaa unitilaan purskeen ajaksi, jolloin koko järjestelmän unitilassa viettämä aika kasvaa.

# JOHTOPÄÄTÖKSET JA JATKOKEHITYSMAHDOLLISUUDET

Sulautettu tietotekniikka on kehittynyt vuosien varrella yhä pienemmäksi, nopeammaksi ja monipuolisemmaksi, mikä on sallinut langattomien sovellusten ja verkkojen nopean kehityksen. Vallitsevan taloustilanteen salliessa ja asiakkaiden tarpeiden ja vaatimusten mukaan julkisten verkkojen yleistyessä muodostuu tarve turvata nämä verkot. Tietoturvan ymmärtäminen ja toteuttaminen langattomassa, virrankulutukseltaan mahdollisimman vähäisessä ja sulautettua tietotekniikka sisältävässä laitteistossa oli mielenkiintoinen haaste.

Tämän opinnäytetyön tuloksena luotiin toimiva järjestelmä, jolla osoitettiin salauksen käyttökelpoisuus langattomissa sovelluksissa ja pyrittiin ymmärtämään, miten turvataan langaton kommunikointi prosessointikyvyltään rajoitetuissa laitteissa. Tämän työn tulokset osoittavat, että salattu ja langaton kommunikointi on mahdollista toteuttaa laitteistolla, jolla on kohtuullinen pariston elinikä.

Projekti oli haastava sekä laitteiston että ohjelmiston suunnittelun ja tuotannon osalta. Toteuttamatta jäi ainoastaan infrapunakommunikointi huonon komponenttivalinnan takia. Laitteiston laatua parantaisi, kuten analysointi paljastaa, virrankulutukseltaan pienemmän regulaattorin käyttö. Käyttäjälle mukavampaa olisi myös yhtenäinen piirilevy, joka olisi koteloitu. Mielenkiintoisia lisätutkimuksia projektin aihealueeseen liittyen olisivat erilaisten salausten ja matalan kantaman radiotien testaus salausavaimien vaihdossa. Radioliikenteen turvaaminen taajuushyppelyllä tai kohinanaamioinnilla ovat myös mielenkiintoisia mahdollisuuksia mutta vaativat laitteistolta enemmän suorituskykyä.

# LÄHTEET

1: ECOmfort Living sivut [verkkodokumentti]. [Viitattu 23.10.2008]. Saatavissa: http://www.ele.tut.fi/en/research-en/rauma/projects/ECOmfort.htm

2: WABS TTY Rauma sivut [verkkodokumentti]. [Viitattu 23.10.2008]. Saatavissa: http://www.ele.tut.fi/en/research-en/rauma/projects/WABS-en.htm

3: Anderson, R., Kuhn, M.: Tamper Resistance – a Cautionary Note. The Second USENIX Workshop on Electronic Commerce Proceedings. Oakland, California, Nov. 18-21, 1996. s 1-11. [Viitattu 23.10.2008]. Saatavissa: http://www.cl.cam.ac.uk/~rja14/tamper.html

4: Sikkilä, H.: Kiinteistön Langaton Viestintä. 2005. [Viitattu 27.10.2008]. Diplomityö. Tampereen Teknillinen Yliopisto, Tietotekniikan osasto. s 58.

5: Rivest, R., L.: The RC5 Encryption Algorithm [verkkodokumentti]. Mar. 20, 1997. [Viitattu 27.10.2008]. MIT Laboratory for Computer Science. Saatavissa: http://people.csail.mit.edu/rivest/Rivest-rc5rev.pdf

6: Distributed.net [verkkodokumentti]. [Viitattu 28.10.2008]. Saatavissa: http://www.distributed.net/rc5/

7: ITU:n ISM suositukset [verkkodokumentti]. [Viitattu 3.11.2008]. Saatavissa: http://www.itu.int/ITU-R/terrestrial/faq/index.html#g013

8: Viestintäviraston radiotaajuuksien käyttöön liittyvät määräykset 4 J/2007 ja 15 X/2007 M sekä taajuusjakotaulukko [verkkodokumentti]. [Viitattu 3.11.2008]. Saatavissa: http://www.ficora.fi/index/saadokset/maaraykset/radioliikenne.html

9: Vierikko, J.: Energian Sieppaus Langattomiin Sensoreihin. 2007. [Viitattu 3.11.2008]. Diplomityö. Tampereen Teknillinen Yliopisto, Sähkötekniikan koulutusohjelma. s. 22-27, 34, 40, 46.

10: Atmel Corporation, ATmega164P/324P/644P Preliminary datasheet [verkkodokumentti]. 2008. [Viitattu 3.11.2008]. Saatavissa: http://www.atmel.com/dyn/resources/prod_documents/doc8011.pdf

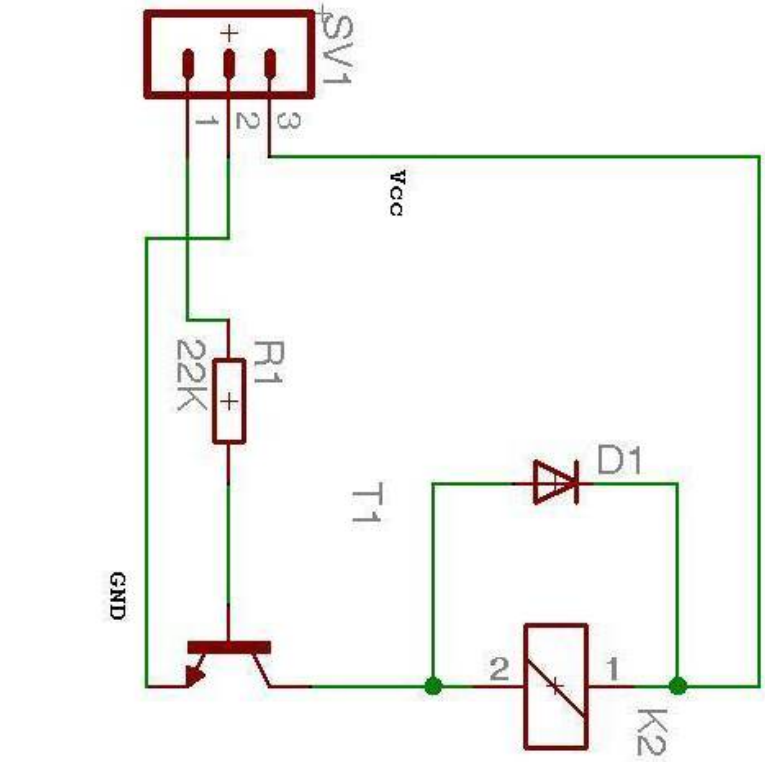
11: Nordic Semiconductor, nRF905 datasheet Revision 1.5 [verkkodokumentti]. 2008. [Viitattu 3.11.2008]. Saatavissa: http://www.nordicsemi.com/index.cfm?obj=product&act=display&pro=83#

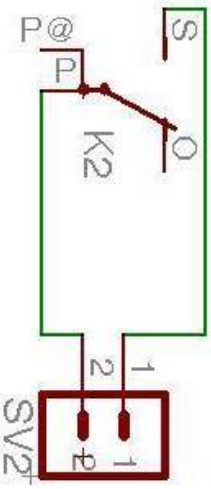
12: Vishay, TFBS4650 datasheet Revision 1.2 [verkkodokumentti]. May, 2008. [Viitattu 5.11.2008]. Saatavissa: http://www.vishay.com/docs/84672/tfbs4650.pdf

13: Energizer, 522 datasheet [verkkodokumentti]. [Viitattu 15.12.2008]. Saatavissa: http://data.energizer.com/PDFs/522.pdf

14: Leijen, D.: Division and Modulus for Computer Scientists [verkkodokumentti]. Dec. 20, 2001. s. 3. [Viitattu 30.11.2008]. University of Utrecht, Dept. of Computer Science. Saatavissa http://legacy.cs.uu.nl/daan/download/papers/divmodnote.pdf

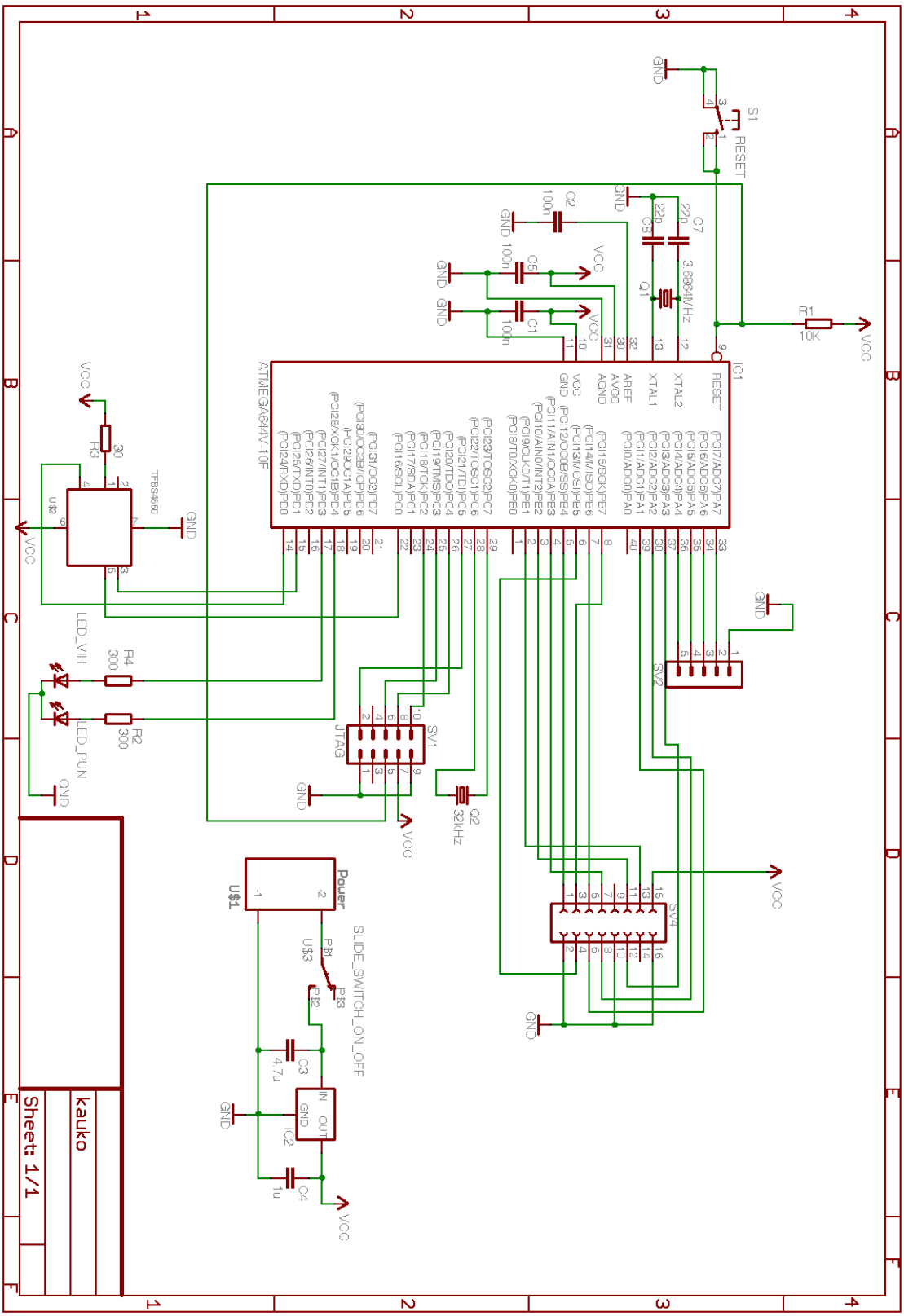
15: National Institute of Standards and Technology: Recommendation for Block Cipher Modes of Operation [verkkodokumentti]. 2001. [Viitattu 11.12.2008]. Saatavissa http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf


SV1
1
2
3
Vcc
R1
22K
D1
T1
GND
2
1
K2


P@
P
S
O
K2
2
1
SV2


ovipalikka
Sheet: 1/1

LIITE 2


ATMEGA644V-10P
IC1
RESET
XTAL2
XTAL1
AREF
AVCC
AGND
VCC
GND
S1
RESET
R1
10K
Q1
3.6864MHz
C1
C2
C5
C7
C8
100n
22p
R2
R3
R4
300
30
LED_VIH
LED_PUN
TFBS4650
JTAG
SV1
SV2
SV4
Q2
32kHz
U$1
Power
SLIDE_SWITCH_ON_OFF
C3
C4
4.7u
1u
IC2
IN
OUT
Sheet: 1/1
kauko