Antti Rantala

Differentiaalinen tehoanalyysihyökkäys AES-salausalgoritmia vastaan

Sähkötekniikan korkeakoulu

Diplomityö, joka on jätetty opinnäytteenä tarkastettavaksi diplomi-insinöörin tutkintoa varten Espoossa 31.10.2014.

Työn valvoja:

Prof. Jussi Ryynänen

Työn ohjaaja:

TkT Lauri Koskinen

Aalto-yliopisto
Sähkötekniikan korkeakoulu

AALTO-YLIOPISTO
SÄHKÖTEKNIIKAN KORKEAKOULU

DIPLOMITYÖN
TIIVISTELMÄ

Tekijä: Antti Rantala

Työn nimi: Differentiaalinen tehoanalyysihyökkäys AES-salausalgoritmia vastaan

Päivämäärä: 31.10.2014 Kieli: Suomi Sivumäärä: 7+55

Mikro- ja nanotekniikan laitos

Professuuri: Mikroelektroniikka Koodi: S-87

Valvoja: Prof. Jussi Ryynänen

Ohjaaja: TkT Lauri Koskinen

Tiedon joutuminen ulkopuolisten tahojen haltuun halutaan usein estää käyttämällä salausalgoritmeja. Symmetriset salauslalgoritmit ovat eräs tapa suorittaa salaus. Symmetriset salausalgoritmit käyttävät salaukseen ja salauksen purkamiseen samaa salausavainta.
Differentiaalinen tehoanalyysihyökkäys on sivukanavahyökkäys. Sivukanavahyökkäyksissä käytetään hyväksi sauslaitteen vuotamaa tietoa. Differentiaalisessa tehoanalyysihyökkäyksessä hyväksikäytetään elektronisen salauslaitteen tehonkulutuksen riippuvuutta laitteen käyttämästä salausavaimesta. Hyökkäyksellä on mahdollista selvittää salauslaitteen käyttämä salausavain.
Differentialiseen tehoanalyysihyökkäykseen tarvitaan salauslaitteen salaamaa salattua tietoa ja tehonkulutusmittauksia laitteesta. Hyökkäykseen tarvitaan oskilloskooppi ja tietokone, joiden avulla mitataan salauslaitteen tehonkulutus ja suoritetaan laskenta.
Salatun tiedon ja avainarvausten avulla lasketaan salauslaitteen mahdollisesti tuottamia välituloksia. Välitulosten avulla arvioidaan salauslaitteen tehonkulutusta. Korrelaatioanalyysillä tunnistetaan oikea avainarvaus.
Tässä työssä suoritettiin differentiaalinen tehoanalyysihyökkäys kahta AES-salauslaitetta vastaan. Salauslaitteen salausavain saatiin selville yhdellä kolmesta kokeillusta AES-toteutuksesta.

Avainsanat: Differentiaalinen tehoanalyysi, Sivukanavahyökkäys, AES, Tehonkulutuksen arviointi

AALTO UNIVERSITY
SCHOOL OF ELECTRICAL ENGINEERING

ABSTRACT OF THE
MASTER'S THESIS

Author: Antti Rantala

Title: Differential power analysis attack against Advanced Encryption Standard

Date: 31.10.2014 Language: Finnish Number of pages: 7+55

Micro- and Nano technology

Professorship: Microelectronics Code: S-87

Supervisor: Prof. Jussi Ryynänen

Advisor: D.Sc. (Tech.) Lauri Koskinen

It is often desirable that information is not readable by outsiders. To make information unreadable for outsiders an encryption algorithm is used. Symmetric encryption algorithms uses secred key for encryption and decryption.
Differential power analysis attack is a side-channel attack. The attack takes advantage of information about the secret key that leaks trough encryption device's power consumption. Goal of the attack is to find the secret key.
Encrypted information and power consumption measurements are needed for differential power analysis attack. An oscilloscope is used to measure the encryption device's power consumption. A computer is used to calculate results.
Possible intermediate values are calculated by encrypted information and key guesses. Intermediate values are used to approximate power consumption of the encryption device. Correlation analysis is used to distinguish the correct key guess.
In this work differential power analysis attack is performed against two different AES encryption devices. Secret key was found while using one of the three AES implementations that are investigated.

Keywords: Differential Power Analysis, Side-channel attack, AES, Approximation of power consumption

Esipuhe

Kiitos henkilöille ja organisaatioille, jotka ovat positiivis-sävytteisesti vaikuttanneet diplomityöni ja opintojeni valmistumiseen.

Otaniemi, 10.10.2014

Antti M. Rantala

Sisällysluettelo

Symbolit ja lyhenteet

Symbolit

P	Teho
U	Jännite
R	Vastus
I	Virta

Lyhenteet

FPGA	Kenttäohjelmoitava porttimatriisi (Field Programable Gate Array)
DPA	Differentiaalinen tehoanalyysi (Differential Power Analysis)
CPA	Korrelaatiotehoanalyysi (Correlation Power Analysis)
SNR	Signaali-kohinasuhde (Signal to Noise Ratio)
CMOS	Komplementtimetallioksidipuolijohde (Complementary Metal Oxide Semiconductor)
SMA	Pienoisliitin versio A (SubMiniature version A)
USB	Univeraali sarjaväylä (Universal Serial Bus)
UART	Univeraali epäsynkroninen lähetin vastaanotin (Universal Anynchronous Receiver Tran
NMOS	N-tyypin metallioksidipuolijohde (N-type Metal Oxide Semiconducto)
PMOS	P-tyypin metallioksidipuolijohde (P-type Metal Oxide Semiconductor)
XOR	Eksklusiivinen tai

1 Johdanto

Yrityksillä ja yksityisillä henkilöillä on tietoja joiden päätyminen ulkopuolisten tahojen haltuun halutaan estää. Arkaluontoista tietoa säilötään usein elektronisissa laitteissa, esimerkiksi älykorttien elektronisissa piireissä. Piirien sisällä tieto on yleensä turvassa sillä tiedon kerääminen suoraan piiriltä vaatii erikoislaitteita ja piirin koteloinnin fyysistä vahingoittamista. Menetelmien käyttäminen saattaa vahingoittaa myös piiriä ja tuhota tiedot.

Kun tietoa siirretään laitteesta toiseen tiedonsiirtokanavan kautta, altistuu tieto kanavan salakuuntelulle. Tiedot voidaan salata ennen tiedonsiirtokanavaan lähettämistä. Jos ulkopuoliset tahot saavat tiedon haltuunsa salattuna sitä ei voida purkaa ilman salausavainta. Salaus suoritetaan salausalgoritmilla elektronisen salauslaitteen avulla.

Symmetrinen salaus soveltuu hyvin tiedonsiirtokanavaan lähetettävän tiedon salaukseen. Symmetrisessä salauksessa samaa salausavainta käytetään tiedon salaamiseen ja salauksen purkamiseen. AES (Advanced Encryption Algorithm) on laajasti käytetty symmetrinen salausalgoritmi. Muita symmetrisiä salausalgoritmeja ovat muun muassa DES (Data Encryption Standard) ja DES:stä johdettu kolminkertainen DES.

Epäsymmetrisissä salausalgoritmeissa käytetään julkista ja yksityistä salausavainta. Esimerkkejä epäsymmetrisistä salausmenetelmistä ovat RSA (Rivest, Shamir, Adleman) ja Elliptiset käyrät. Käytössä on myös yksisuuntaisia tiivisteitä kuten SHA-1 (Secure Hash Algorithm) ja sähköisen allekirjoituksen menetelmiä kuten DSA (Digital Signature Algorithm).

Salauksen murtamisella tarkoitetaan salausavaimen selvittämistä. Salausalgoritmin käyttämä salausavain voidaan selvittää brute force-hyökkäyksellä eli järjestelmällisesti käymällä mahdollisia salausavaimia läpi. Salausalgoritmien tärkeimpiä ominaisuuksia on, että brute force-hyökkäyksen suoritus kestää kauan ja sitä ei voida nopeuttaa analysoimalla algoritmilla salattua tietoa. Salausavaimen selvittämisen nopeuttamista analysoimalla salattua tietoa kutsutaan kryptoanalyysiksi. Yleisiä kryptoanalyysimenetelmiä ovat lineaarinen ja differentiaalinen kryptoanalyysi. Brute force-hyökkäykseen kuluva aika riippuu lähinnä salausavaimen pituudesta.

DES oli pitkään käytetyin symmetrinen salausmenetelmä vaikka sen salausavainta pidettiin lyhyenä jo 1970-luvulla. Vuonna 1998 DES-salaus voitiin murtaa brute force-hyökkäyksellä muutamassa päivässä. Murtamiseen käytettiin erityisesti DES-salauksen murtamiseen suunniteltua tietokonetta. DES-avaimen pituus on 56 bittiä ja se on lyhyt verrattaessa esimerkiksi AES-algoritmin salausavaimeen. AES:n lyhimmän 128 bitin salausavaimen avainavaruuden läpikäymiseen kuluisi nykyaikaiselta tietokoneelta miljoonia vuosia.

DES:n elinikää pidennettiin ottamalla käyttöön kolminkertainen DES, joka toteutetaan suorittamalla DES-salaus kolme kertaa käyttäen eri salausavaimia. Salausavaimen pituus kolminkertaistui ja on nykyisten tietokoneiden laskentatehon saavuttamattomissa. Salausavaimen pituus kasvoi 56 bitistä 168 bittiin. Yhden bitin lisääminen salausavaimeen kaksinkertaistaa mahdollisten salausavaimien määrän, joten kolmikertainen DES on hyvin vastustuskykyinen brute force-hyökkäystä

vastaan.

AES on korvannut DES:n käytetyinpänä symmetrisena salauksena. Vaikka DES:n salausavaimen pituutta lisättiin kolminkertaisen DES:n avulla ja se on vastustuskykyinen useita tunnettuja hyökkäysmenetelmiä vastaan, tarve modernimmalle salaukselle oli olemassa. Salausavaimen lisäksi DES:n 64 bitin pituista lohkoa pidettiin liian lyhyenä. Symmetrinen salaus jakaa salattavan tiedon tietyn suuruisiin lohkoihin, joita käsitellään yksitellen.

Salauslaite, joka suorittaa salausta, saattaa vuotaa tietoa salausavaimesta niin kutsuttujen sivukanavien kautta. Sivukanavatiedot ovat salauslaitteen toiminnasta aiheutuvia ilmiöitä, joita voidaan mitata. Salauslaitteen suunnittelija ei ole tarkoittanut sivukanavia tiedonvälitykseen. Ulkopuolinen taho voi kuitenkin käyttää sivukanavatietoa saadakseen ylimääräistä tietoa laitteen toiminnasta ja helpottamaan salausavaimen selvittämistä. Salausavaimen selvittämistä sivukanavista saatavan tiedon avulla kutsutaan sivukanavahyökkäykseksi.

Salauslaitteen kuluttama teho on sivukanavatietoa, koska laitteen kuluttama teho riippuun salauslaitteen käsittelemästä tiedosta ja sen käyttämästä salausavaimesta. Muita esimerkkejä sivukanavista ovat viive, ääni ja sähkömagneettinen säteily.

Differentiaalinen tehoanalyysi (differential power analysis, DPA) on sivukanavahyökkäys, jonka avulla hyökkääjä voi saada selville elektronisen salauslaitteen käyttämän salausavaimen. Hyökkäys esiteltiin vuonna 1999 Paul Kocherin, Joshua Jaffen ja Benjamin Junin julkaisussa Differential Power Analysis [1]. Julkaisussa esitellään miten differentiaalisella tehoanalyysillä voidaan pienellä vaivalla saada selville elektronisella laitteella toteutetun DES-salauksen (Data Encryption Standard) käyttämä salausavain.

Salauavaimen pituuden kasvattaminen vaikeuttaa brute force-hyökkäystä eksponentiaalisesti. Differentiaalinen tehoanalyysi kohdistetaan kerrallaan yhteen bittiin tai pieneen bittijoukkoon salausavaimesta. Salausavaimen pituuden kasvattaminen vaikeuttaa differentiaalista tehoanalyysiä vain lineaarisesti. Jos yhden bitin pituisen salausavaimen murtamiseen kuluu brute force-menetelmällä ja differentiaalisella tehoanalyysillä yksi yksikkö aikaa, niin kuuden bitin pituisen salausavaimen murtamiseen kuluu brute force-menetelmällä 64 yksikköä aikaa, mutta differentiaalisella tehoanalyysillä vain 6 yksikköä. Salausavaimen pituuden lisääminen ei merkittävästi vaikeuta differentiaalista tehoanalyysihyökkäystä.

AES-standardi otettiin käyttöön vuonna 2001. Koska differentiaalinen tehoanalyysi julkaistiin vuonna 1999 ja AES valintaprosessi aloitettiin vuonna 1997 ei AES-salaukselta vaadittu erityistä suojausta sivukanavahyökkäystä vastaan.

AES-salausta ei käytännössä voida murtaa brute force-menetelmällä, eikä merkittäviä kryptoanalyysimenetelmiä AES-salausta vastaan tunneta. Differentiaalinen tehoanalyysi toimii AES-algoritmia vastaan ja hyökkäystä vastaan suojaamaton AES-toteutus voidaan murtaa differentiaalisella tehoanalyysillä muutamassa tunnissa. Differentiaalisen tehoanalyysihyökkäyksen nopeus riippuu salauslaitteen ominaisuuksista, mittausjärjestelyistä, käytettävissä olevasta laskentatehosta ja salausalgoritmin toteutuksesta.

Kocher esitteli myös menetelmiä joilla uutta hyökkäystä voidaan hidastaa. Nykyisin hänen perustamansa yritys Cryptography Research on maailman johtava puo-

lijohdeturvallisuuden tutkija [2]. Suuri osa salausta suorittavista elektronisista laitteista kuten pankki- ja älykorteista on erikseen suojattu differentiaaliselta tehoanalyysihyökkäykseltä. Suojaukset ovat tehokkaita ja suojatun laitteen murtamiseen kuluva aika lähestyy brute force-hyökkäykseen vaadittavaa aikaa. Suojauksia voidaan toteuttaa erityisillä ohjelmointi- ja suunnittelutekniikoilla. Suojaukset tekevät laitteista kalliimpia ja hitaampia koska niiden vuoksi joudutaan suorittamaan ylimääräistä laskentaa. Suojauksien tarve täytyy arvioida tarvittavan turvallisuustason mukaan.

Tässä työssä on tarkoituksena osoittaa, että turvallisuuskriittisissä laitteissa on tarpeellista käyttää erityisiä suojausmenetelmiä sivukanavahyökkäyksiä vastaan. Vaikka tieto on salattu kryptoanalyysille vastustuskykyisellä salausmenetelmällä, salauslaite saattaa vuotaa tietoa käytetystä salausavaimesta. Mikäli salausavain saadaan selville voidaan sen avulla purkaa kaikki kyseisellä avaimella salattu tieto.

Luvussa 2 esitetään DPA-hyökkäyksen kannalta oleellisia taustatietoja. Ensimmäisessä alaluvussa käydään läpi AES-salausalgoritmi. Toisessa alaluvussa käsitellään integroitujen piirien tehonkulutusta. Kolmannessa alaluvussa esitellään korrelaatio, joka on tilastollinen menetelmä näytejoukkojen lineaarisen yhteyden havaitsemiseksi. DPA-hyökkäyksessä korrelaatiolla arvioidaan mitatun tehonkulutuksen ja arvioidun tehonkulutuksen lineaarista yhteyttä.

Luvussa 3 esitellään differentiaalinen tehoanalyysihyökkäys. Toisessa alaluvussa esitellään menetelmä jonka avulla todelliseen tehonkulutukseen verrannollinen jännite voidaan mitata. Kolmannessa alaluvussa esitetään miten salausalgoritmin tuottamien väliarvojen perusteella voidaan arvioida salauslaitteen tehonkulutusta. Neljännessä alaluvussa käydään läpi miten korrelaatioanalyysillä voidaan tunnistaa osa salausavaimesta. Toistamalla hyökkäys kaikkia avaimen osia vastaan saadaan selville koko salausavain.

Luvussa 4 esitetään suoritetut differentiaaliset tehoanalyysihyökkäykset. Ensimmäisessä alaluvussa esitellään käytetyt salauslaitteet ja AES-toteutukset. Toisessa alaluvussa esitetään mittausten suoritustapa ja mittaustulokset. Kolmannessa alaluvussa käydään läpi tehonkulutuksen arviointi. Neljännessä alaluvussa esitellään korrelaatioanalyysillä saatuja tuloksia. Havainnot mittaus ja korrelaatioanalyysituloksista kerrotaan viidennessä alaluvussa.

2 Taustatietoja

AES-salausalgoritmia käytetään differentiaalisessa tehoanalyysihyökkäyksessä salauslaitteen tuottamien välitulosten laskemiseksi, joten salausalgoritmin toiminta täytyy tuntea. Hyökkäys perustuu olettamukseen, että salauslaitteen tehonkulutusta voidaan jossain määrin arvioida jos tiedetään millaisia operaatioita laite suorittaa tunnetulla datalla. Integroitujen piirien tehonkulutusta voidaan arvioida jos tiedetään mistä tehonkulutus aiheutuu ja miten käsitelty data vaikuttaa siihen. Korrelaatio on tilastollinen menetelmä, jonka avulla voidaan tunnistaa lineaarinen yhteys salauslaitteen todellisen tehonkulutuksen ja arvioidun tehonkulutuksen välillä.

2.1 Advanced Encryption Standard

2.1.1 Historiaa

AES on laajasti käytetty salausmenetelmä. AES kehitettiin DES-salauksen seuraajaksi, kun DES-salauksen turvallisuuden todettiin heikentyneen tietokoneiden kasvaneen laskentatehon seurauksena. DES-salauksen salausavaimen pituus on 56 bittiä, mikä on vähän esimerkiksi AES-salauksen salausavaimenpituuksiin verrattuna. Lyhyen salausavaimen vuoksi DES-salaus on mahdollista murtaa suhteellisen nopeasti brute force-hyökkäyksellä. Vuonna 1998 valmistettiin DES Cracker niminen tietokone, joka kykeni suorittamaan brute force-hyökkäyksen DES-salausta vastaan 56 tunnissa. AES-salauksen murtamiseen brute force-menetelmällä kuluisi miljoonia vuosia. Taulukkoon 1 on koottu DES-salauksen ja AES-salauksen eroja. [4]

Taulukko 1: AES ja DES salausalgoritmien eroja.

Algoritmi	**DES**	**AES**
Avaimen pituus	56	128, 192 tai 256
Lohkon pituus	64	128
Kierrosten määrä	16	10, 12 tai 14
Standardointivuosi	1977	2001

Yhdysvaltojen kansallinen standardointi-instituutti (National Institute of Standards and Technology, NIST) nimesi Rijndael-salausalgoritmin AES-salausalgoritmiksi vuonna 2001. Valitsemisprosessi toteutettiin kilpailunomaisesti useiden salausalgoritmien välillä. Ehdokasalgoritmit lähetettiin arvioitavaksi vuonna 1997 ja valintaprosessi kesti vuoteen 2000, jolloin Rijndael julistettiin kilpailun voittajaksi. [4]

Kilpailevia algoritmejä vertailtiin kolmessa kategoriassa: turvallisuus, hinta ja algoritmin toteutuksien ominaisuudet. Tärkeimpänä kriteerinä oli vastustuskyky tunnettuja hyökkäysmuotoja vastaan. Algoritmin vaadittiin myös olevan ilmainen ja vapaasti kaikkien halukkaiden käytettävissä mahdollisen valinnan jälkeen. AES-salauksen haluttiin olevan laskennallisesti tehokas toteuttaa erilaisilla alustoilla.[4]

2.1.2 Salauksen käyttötarkoitukset ja turvallisuus

AES on symmetrinen salausmenetelmä. Symmetrinen salausmenetelmä käyttää samaa salausavainta tiedon salaamiseen ja salatun tiedon purkamiseen takaisin salaamattomaksi.

Symmetristä salausta voidaan käyttää esimerkiksi FPGA-piireissä (Field Programable Gate Array) tietoliikenteen salaamiseen. FPGA:t ovat uudelleenohjelmoitavia integroituja piirejä. Jos salausta ei käytettäisi, voisivat ulkopuoliset tahot saada FPGA:n lähettämän ja vastaanottaman tiedon haltuunsa yksinkertaisesti salakuuntelemalla FPGA:n tietoliikennettä. FPGA -piirien uudelleenohjelmointi vaatii usein laitteelle asetetun salausavaimen tuntemisen. Tällä pyritään estämään laitteen uudelleenohjelmointi ulkopuolisten tahojen toimesta.

AES-salausavaimen pituus voi olla 128, 192 tai 256 bittiä. Avaimen pituudesta riippuen salaus suorittaa 10, 12 tai 14 salauskierrosta. Salauskierrokset koostuvat neljästä operaatiosta. Avaimen pituudella on merkittävä vaikutus salauksen turvallisuuteen. Erityisesti brute force-hyökkäystä voidaan vaikeuttaa kasvattamalla avaimen pituutta eli kasvattamalla mahdollisten salausavaimien määrää. Pidemmän salausavaimen käyttäminen vaatii enemmän resursseja ja on hitaampaa kuin lyhyemmän salausavaimen käyttäminen.

Brute force-hyökkäys perustuu kaikkien avainmahdollisuuksien kokeilemiseen. Oletuksena on, että oikean arvauksen löytyminen voidaan havaita. DES-salauksen 56 bittiä pitkä salausavain oli riittävä, kun salaus otettiin käyttöön vuonna 1977. Koko avainavaruuden läpikäyminen olisi vienyt satoja vuosia tehokkaimmilla tietokoneilla. Tietokoneiden laskentatehon kasvettua DES-salaus on mahdollista murtaa merkittävästi lyhyemmässä ajassa. Brute force-hyökkäykset saattavat tulevaisuudessa uhata myös AES-salauksen turvallisuutta jos käytettävissä oleva laskentateho kasvaa merkittävästi. Nykyinen käytettävissä oleva laskentatehokkuus ei mahdollista tehokkaita brute force-hyökkäyksiä AES-salausta vastaan.

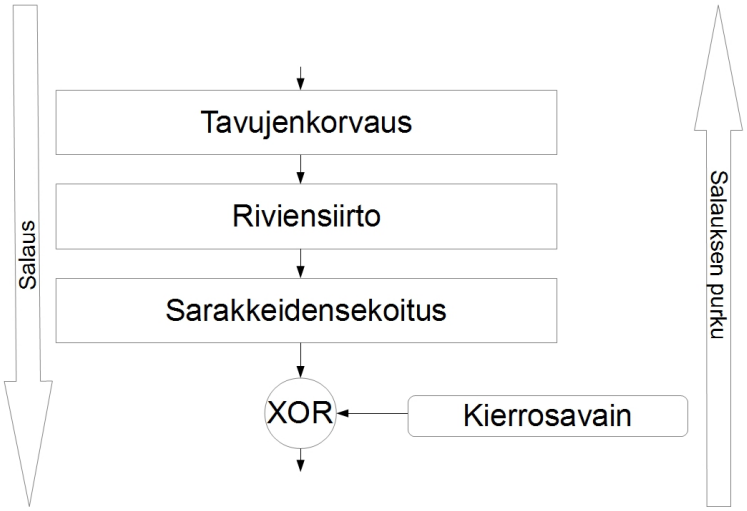
Kryptoanalyysi on hyökkäysmenetelmä jolla pyritään heikentämään salausalgoritmin turvallisuutta. Hyökkäys on onnistunut, jos sen avulla saadaan salausavain selville lyhemmässä ajassa kuin brute force-hyökkäyksellä. Yksi AES-salauksen valintakriteereistä oli, että mitkään tunnetut hyökkäysmenetelmät eivät toimi sitä vastaan. Yleisimmät kryptoanalyysimenetelmät ovat lineaarinen ja differentiaalinen kryptoanalyysi. Näillä hyökkäyksillä ei olla onnistuttu heikentämään AES-salauksen turvallisuutta merkittävästi.

2.1.3 Algoritmin kuvaus

Liitteessä A on esimerkki AES-algoritmin käytöstä. Differentiaalisen tehoanalyysihyökkäyksen suorittamiseen tarvitaan salausalgoritmin tuottamia välituloksia. Välituloksia käytetään salauslaitteen kuluttaman tehon arviointiin.

AES on lohkosalausmenetelmä, joka käsittelee tietoa vakiokokoisina lohkoina. AES-lohkon koko on 128 bittiä. Salaus ottaa alkuarvokseen 128 bittiä salaamatonta tietoa ja muuntaa sen 128:ksi bitiksi salattua tietoa. AES-operaatioiden tuottamat AES-välitulokset ovat 128 bitin kokoisia kuten salattava lohko. AES-välitulosten

bitit on jaettu tavuihin ja tavuista on muodostettu matriisi, jolla on neljä riviä ja neljä saraketta.



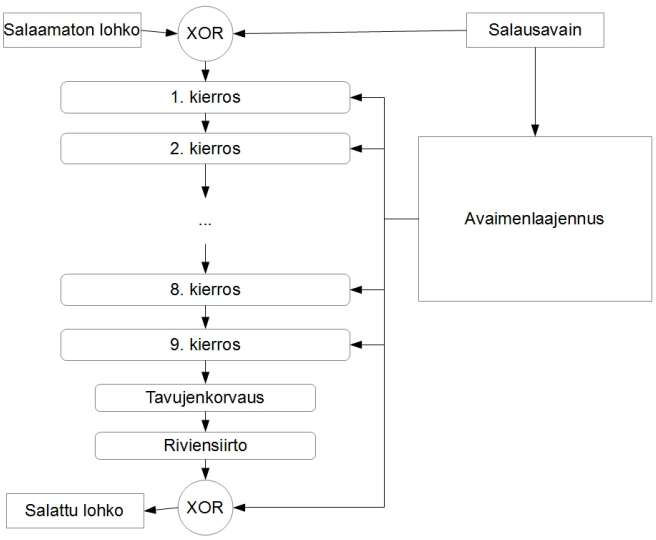
Kuva 1: AES-kierros

Salaus suoritetaan käsittelemällä lohkoa eri operaatioilla. Operaatiot, joista AES koostuu, ovat riviensiirto, sarakkeidensekoitus, kierrosavaimensummaus ja tavujenkorvaus. Lisäksi salausalgoritmi laskee jokaiselle kierrokselle oman kierrosavaimen, joka perustuu varsinaiseen salausavaimeen. Tätä operaatiota kutsutaan avaimenlaajennukseksi. Salattu lohko saadaan purettua salaamattomaksi käyttämällä käänteisiä versioita salaukseen käytetyistä operaatioista ja suorittamalla ne käänteisessä järjestyksessä. Kuvassa 1 nähdään kierroksen operaatioiden järjestys salauksen ja salauksen purkamisen yhteydessä.

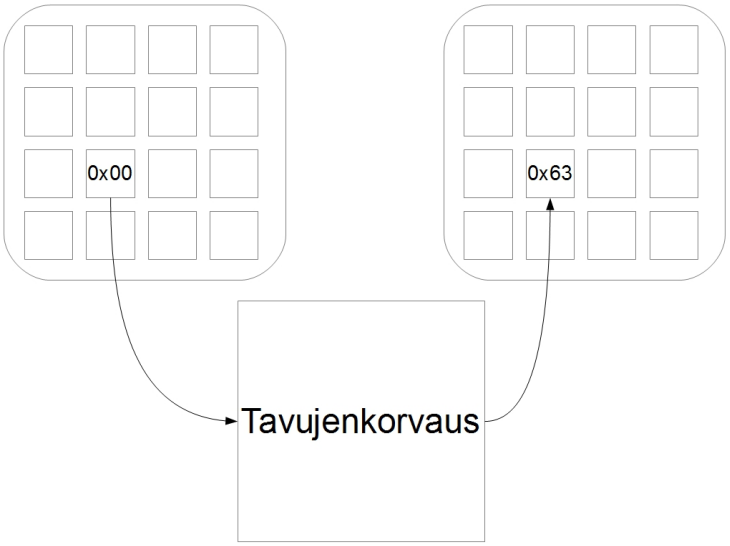
AES-salausalgoritmi alkaa kierrosavaimensummaus-operaatiolla. AES-operaatiot suoritetaan $GF(2^8)$ kentässä. GF, eli Galois Field, on äärellinen kenttä, jonka elemettien määrä on p^n, missä p on kantaluku ja n on kantalukujen määrä. Kenttä on joukko elementtejä, joille on määritetty summaus- ja tulo-operaatiot tietyillä ominaisuuksilla. Käytetyssä kentässä kierrosavaimensummaus on eksklusiivinen tai-operaatio, eli XOR-operaatio. Kierrosavaimensummaus-operaatio suoritetaan ensimmäisellä kerralla lohkon ja salausavaimen välillä. Myöhemmin operaatio tehdään AES-välituloksen ja kierrosavaimen välillä. [7]

Ensimmäisen kierrosavaimensummaus-operaation jälkeen suoritetaan neljästä operaatiosta koostuvia salauskierroksia. Suoritettavien kierrosten määrä määräytyy avaimen pituuden mukaan. Poikkeuksena viimeisellä kierroksella sarakkeidensekoitusoperaatiota ei käytetä. Muuten viimeinen kierros on saman lainen kuin muut kierrokset. Normaalin kierroksen aikana operaatioiden järjestys on seuraava: tavujenkorvaus, riviensiirto, sarakkeidensekoitus ja kierrosavaimensummaus. Kuvassa 2 nähdään koko AES käytettäessä 128 bitin pituista avainta.

Tavujenkorvausoperaatio korvaa AES-välituloksen jokaisen tavun toisella tavulla. Korvaavat tavut on määritetty standardissa ja ne on valittu siten, että ne vaikeut-



Kuva 2: AES:n toiminta.

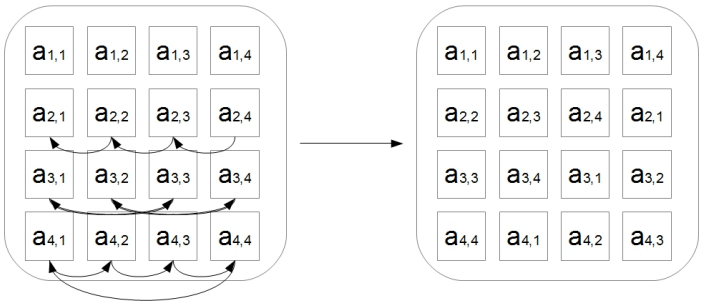


Kuva 3: Tavujenkorvaus-operaatio.

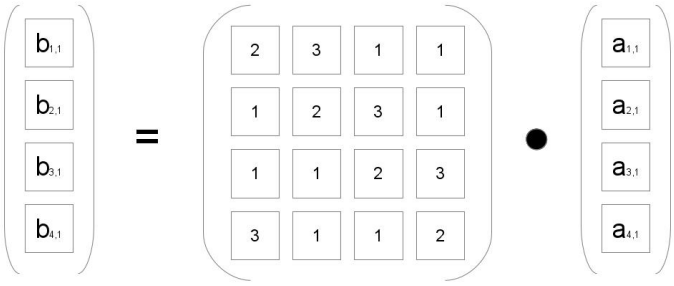
tavat kryptoanalyysin suorittamista salausalgoritmia vastaan [4]. Kuvassa 3 nähdään operaation toiminta yhden tavun osalta.

Riviensiirto-operaatiossa rivien tavuja siirretään vasemmalle. Ensimmäistä riviä ei siirretä. Toisen rivin jokaista tavua siirretään yhden paikan eli tavun verran vasemmalle. Kolmannen rivin tavuja siirretään kaksi paikkaa ja neljännen rivin tavuja kolme paikkaa. Operaation toiminta nähdään kuvassa 4.

Sarakkeidensekoitusoperaatio voidaan toteuttaa matriisikertolaskuna AES-välituloksen ja vakiomatriisin välillä. Operaation seurauksena jokainen sarakkeen tavu vaikuttaa muihin saman sarakkeen tavuihin painotettuna ennakkoon määrätyllä vakiolla. Operaatio yhdelle sarakkeelle nähdään kuvassa 5.



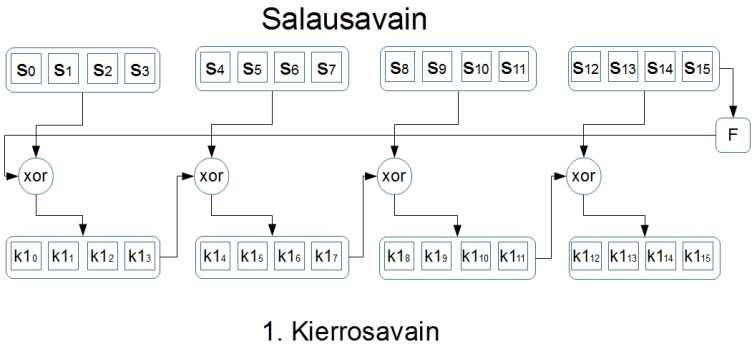
Kuva 4: Riviensiirto-operaatio.



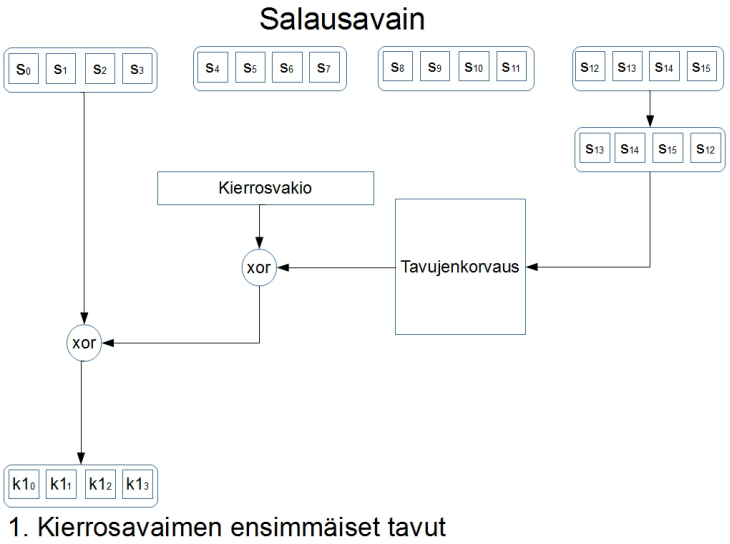
Kuva 5: Sarakkeidensekoitusoperaatio

Kierrosavaimet luodaan avaimenlaajennusoperaatiolla. Kuvassa 6 nähdään ensimmäisen kierrosavaimen luominen salausavaimella. Kierrosavaimen ensimmäinen sana, eli neljän tavun suuruinen osa, luodaan XOR-operaatiolla salausavaimen ensimmäisen ja viimeisen sanan avulla. Viimeistä sanaa käsitellään kuvassa 7 nähtävällä tavalla ennen XOR-operaatiota ensimmäisen sanan kanssa. Toinen kierrosavain luodaan samalla tavalla ensimmäisellä kierrosavaimella. Avaimenlaajennusoperaation ainoa salainen tieto on salausavain.

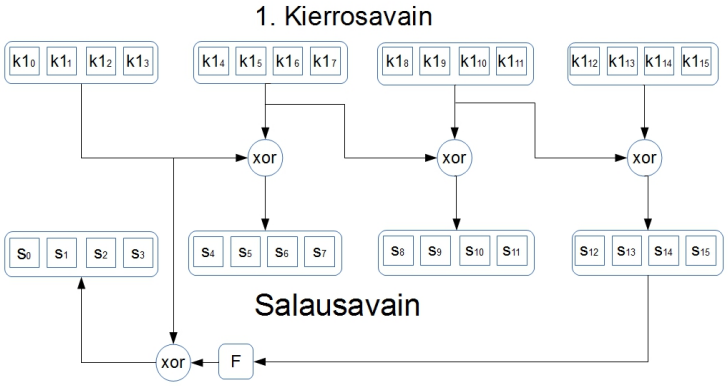
Jos tunnetaan viimeisen kierroksen kierrosavain, voidaan salausavain laskea käänteisellä avaimenlaajennuksella [10]. Kuvasta 8 nähdään, että kolme neljästä salausavaimen sanasta voidaan laskea XOR-operaatioilla kierrosavaimen sanojen välillä. Sa-



Kuva 6: Avaimenlaajennusoperaatio.



Kuva 7: Kierrosavaimen ensimmäisten tavujen laskenta.



Kuva 8: Käänteinen avaimenlaajennus.

lausavaimen ensimmäinen sana voidaan laskea kun ollaan selvitetty salausavaimen viimeinen sana. Viimeisen kierroksen kierrosavaimella voidaan laskea toiseksi viimeisen kierroksen kierrosavain. Samalla tavalla voidaan laskea kaikki kierrosavaimet ja salausavain.

Liitteessä A esitetään AES-operaatioiden, avaimenlaajennuksen ja käytettävän kentän kertolaskun toimintaa esimerkkien avulla.

2.2 Integroitujen piirien tehonkulutus

Tehonkulutusta muodostuu digitaalisissa integroiduissa piireissä neljällä tavalla. Tehonkulutus on verrannollinen virrankulutukseen, joten tehonkulutuksen muodostumista voidaan tutkia virrankulutuksen avulla. Virrankulutus muodostuu kytkentävirrasta, oikosulkuvirrasta, vuotovirrasta ja staattisesta virrasta. Differentiaalisessa tehoanalyysihyökkäyksessä tutkitaan kytkentävirran aiheuttamaa tehonkulutusta. [9]

Kytkentävirralla on kaksi komponenttia. Komponentit ovat logiikan kytkentävirta ja signaalin siirtämiseen kuluva virta. Kytkentävirran tehonkulutus voidaan laskea kaavalla 1. Siirtymäaktiivisuus riippuu piirin rakenteesta, logiikasta ja signaalin tilastollisista ominaisuuksista. [9]

$$P = \beta C_L V_{VDD}^2 f, \tag{1}$$

missä β on siirtymäaktiivisuus, C_L on kuormakapasitanssi, V_{VDD} on käyttöjännite ja f on taajuus.

Oikosulkuvirta syntyy kun maa ja käyttöjännite ovat suoraan yhteydessä toisiinsa. CMOS-tekniikassa tilanvaihdoksen puolivälissä NMOS ja PMOS transistorit ovat molemmat hetkellisesti auki. [9]

Vuotovirta syntyy transistorien lävitse vuotavasta virrasta niiden ollessa suljettuna. Staattista virrankulutusta ei muodostu CMOS-tekniikassa. [9]

2.3 Korrelaatio

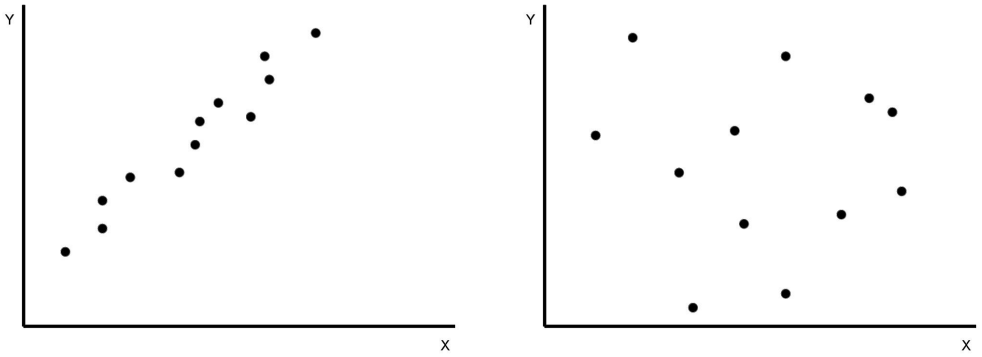
Korrelaatio on tilastollinen menetelmä jonka avulla tutkitaan satunnaismuuttujien lineaarisia yhteyksiä [5]. Differentiaalisessa tehoanalyysihyökkäyksessä korrelaatiota käytetään havaitsemaan mitatun tehon ja arvioidun tehon välisiä lineaarisia yhteyksiä [6]. Korrelaatio voidaan laskea Pearssonin korrelaatiokertoimella kaavalla 2.

$$p_{XY} = \frac{Cov(X,Y)}{\sqrt{(VarX)(VarY)}}, \tag{2}$$

missä X ja Y ovat tutkittavat muuttujat, Var on Varianssi ja Cov on Kovarianssi.

Korrelaatiokerroin on lukuarvo väliltä [-1,1]. Jos korrelaatiokertoimen itseisarvo on yksi, on muuttujien välillä täydellinen lineaarinen yhteys eli täydellinen korrelaatio. Kuvassa 9a nähdään muuttujajoukko, jolla on lähes täydellinen positiivinen korrelaatio.

Jos korrelaatiokerroin on nolla ei muuttujien välillä ole lineaarista yhteyttä. Kuvassa 9b nähdään muuttujajoukko, jolla ei ole merkittävää lineaarista yhteyttä.



(a) Positiivinen korrelaatio.

(b) Ei korrelaatiota.

(c) Ei lineaarista yhteyttä.

Kuva 9: Korrelaatioesimerkkejä.

Jos korrelaatiokerroin on lähellä nollaa satunnaismuuttujien välillä ei ole lineaarista yhteyttä. Muuttujilla voi olla epälineaarisia yhteyksiä, mutta korrelaatio tarkastelee vain lineaarisia yhteyksiä. Kuvassa 9c nähdään muuttujajoukko, jonka muuttujien välillä on yhteys, mutta se ei ole lineaarinen.

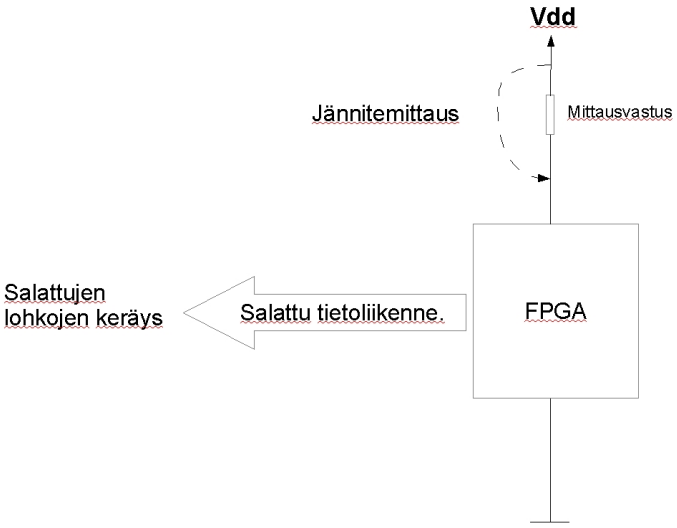
3 Differentiaalinen tehoanalyysihyökkäys

Differentiaalinen tehoanalyysihyökkäys koostuu kolmesta osasta: tehonkulutuksen mittaus, tehonkulutuksen arviointi avainarvausten sekä salattujen lohkojen avulla ja oikean avainarvauksen tunnistaminen korrelaatioanalyysillä.

3.1 Hyökkäyksen kuvaus

Differentiaalinen tehoanalyysihyökkäys on sivukanavahyökkäysmenetelmä, jonka avulla voidaan selvittää elektronisen salauslaitteen salausavain. Hyökkäykseen tarvitaan tehonkulutusmittauksia ja tietoliikenteen tarkkailua [6]. Jos salausavain saadaan selville, voidaan sen avulla purkaa kaikki salausavaimella salatut tiedot.

Hyökkäykseen tarvittavat tehonkulutusmittaukset voidaan suorittaa oskilloskoopilla tehonkulutukseen verrannollisina jännitemittauksina. Tässä työssä tutkituissa salauslaitteissa on mittausvastukset, joiden avulla tehonkulutukseen verrannollinen jännite voidaan mitata. Mittausvastuksen läpi kulkee kaikki salauslaitteen kuluttama virta. Virran muutokset aiheutuvat salauslaitteen transistorien tilojen vaihtumisesta ja virran muutokset muuttavat jännitettä mittausvastuksen yli. Kuvassa 10 nähdään mistä hyökkäykseen tarvittava data kerätään.



Kuva 10: Tarvittavan datan keräys.

Salauslaitteen tietoliikennettä tarkkailemalla saadaan selville salattuja lohkoja. Käytännöllisessä hyökkäyksessä on pääsy vain salattuun tietoliikenteeseen. Differentiaalinen tehoanalyysihyökkäys toimii myös salaamattomia lohkoja käyttämällä, mutta salaamattomiin lohkoihin perustuvan hyökkäyksen hyödyllisyys on kyseenalainen jos voidaan suoraan kerätä salaamatonta tietoa. Tässä työssä hyökkäys suoritetaan salattujen lohkojen avulla.

Hyökkäyksessä salauslaitteille lähetetään tiedonsiirtokanavan kautta satunnaisia salaamattomia lohkoja. Salauslaite salaa lohkot AES-salauksella, joka käyttää

128 bittiä pitkää salausavainta. Salauslaitteet lähettävät salatut lohkot takaisin tiedonsiirtokanavaan ja ne kerätään tiedostoon. Tietoliikennekanavan salakuuntelu on aiheena rajattu tämän työn ulkopuolelle.

AES-salausalgoritmia käyttämällä voidaan salattujen lohkojen ja avainarvausten avulla laskea salauksen aikana mahdollisesti tuotettuja välituloksia. Koska viimeisen kierroksen aikana AES ei käytä sarakkeidensekoitusoperaatiota, voidaan arvaamalla tavun kokoinen osa viimeisen AES-kierroksen kierrosavaimesta laskea saman kokoinen osa jokaisesta viimeisen kierroksen AES-välituloksesta. Oikeaa avainta ei tunneta, joten kokeillaan kaikkia mahdollisia vaihtoehtoja.

Laskettujen välitulosten perusteella arvioidaan FPGA-piirin kuluttama teho hetkellä, jolloin AES-välitulos muodostuu. Tehonkulutuksen arviointiin käytetään Hammingin etäisyys ja Hammingin paino menetelmiä alaluvussa 3.3.1 esitettävällä tavalla.

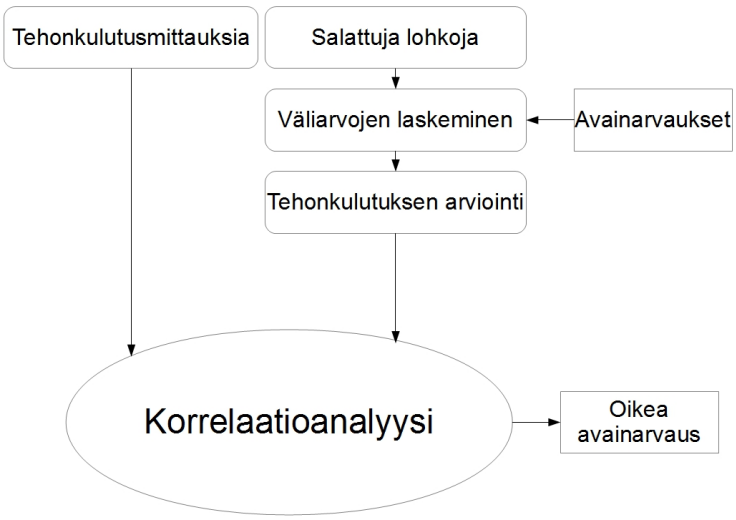
Mitattujen ja arvioitujen tehonkulutusten lineaarista yhteyttä arvioidaan korrelaation avulla. Kun avainarvaus on oikea ja riittävä määrä mittaustuloksia on käytettävissä oikea avainarvaus voidaan erottaa vääristä arvauksista sen aiheuttaman lineaarisen yhteyden ansiosta. Väärillä avainarvauksilla saadut välitulokset voidaan ajatella satunnaisiksi, eikä merkittävää lineaarista yhteyttä ole.

Kaikki mahdolliset tavun arvot käydään läpi eli yhtä tavua kohden tehdään 256 avainarvausta. Oikea avainarvaus tunnistetaan korrelaatioanalyysillä. Hyökkäys toistetaan jokaista kierrosavaimen tavua vastaan. Tämän työn differentiaalisessa tehoanalyysihyökkäyksessä AES-salausta vastaan tehdään $16 * 256$ avainarvausta. Jos AES-toteutus käsittelee tavuja rinnakkain voidaan tehoa arvioida useamman tavun suuruisella avainarvauksella, mikä parantaa korrelaatiota mutta kasvattaa tarvittavien avainarvausten määrää. Kun viimeisen AES-kierroksen kierrosavain on selvitetty, voidaan varsinainen salausavain selvittää käänteisellä avaimenlaajennuksella.

Differentiaaliseen tehoanalyysihyökkäykseen tarvittavien avainarvausten määrä on pienempi kuin brute force-hyökkäykseen vaadittava avainarvausmäärä 2^{128}. Differentiaalisen tehoanalyysihyökkäyksen jokaisella avainarvauksella lasketaan AES-välitulokset kaikille kerätyille salatuille lohkoille, joten DPA-hyökkäys käyttää enemmän aikaa yhden avainarvauksen käsittelyyn kuin brute force-hyökkäys. Tässä työssä esitetty differentiaalinen tehoanalyysihyökkäys on nopeampi kuin brute force-hyökkäys jos salattujen lohkojen määrä on pienempi kuin $10^3 3$.

Alkuperäisessä DPA-hyökkäyksessä oikean avainarvauksen tunnistamiseksi käytettiin keskiarvojenerotusmenetelmää [1]. Korrelaatiotehoanalyysihyökkäys (Correlation Power Analysis) eli CPA-hyökkäys eroaa alkuperäisestä hyökkäyksestä oikean avainarvauksen tunnistamiseen käytetyn matemaattisen menetelmän osalta. CPA-hyökkäyksessä käytetään oikean avaimen erottamiseen korrelaatioanalyysiä keskiarvojenerotuksen sijaan. Alan kirjallisuudessa DPA ja CPA erotetaan joskus erillisiksi hyökkäysmenetelmiksi. CPA ajatellaan tässä työssä kehittyneeksi DPA-hyökkäykseksi.

Tässä työssä oletetaan, että on tiedossa laitteen käyttävän AES-salausta. Muita oletuksia ei tehdä esimerkiksi AES:n toteutuksesta. Tehonkulutusta arvioidaan AES-algoritmilla laskettujen välitulosten perusteella. Kuvassa 11 nähdään algoritmi differentiaalisen tehoanalyysin suorittamiseen.



Kuva 11: Algoritmi differentiaalisen tehoanalyysihyökkäyksen suorittamiseen.

3.2 Tehonkulutuksen mittaaminen

FPGA-piirin tehonkulutukseen verrattavissa oleva jännitteen vaihtelu voidaan mitata piirin käyttöjännitteen tai maan puolelta. Tässä työssä mittaukset on tehty käyttöjännitteen puolelta, sillä Sakura-G laitteessa on mittausvastus vain käyttöjännitteen puolella. Salauslaitteen käyttöjännitteen ja FPGA:n välille on asetettu mittausvastus, jonka yli muuttuvaa jännitettä mitataan oskilloskoopilla. Vastuksen läpi kulkevan virran muutokset aiheuttavat jännitteen muutoksia vastuksen yli. Jännitteen muutos on verrannollinen FPGA:n kuluttamaan tehoon, sillä virran muutokset aiheutuvat tilaansa vaihtavista transistoreista.

Differentiaalinen tehoanalyysihyökkäys ei tarvitse tietoa tehon absoluuttisesta arvosta. Tehonkulutuksen suhteellisten muutosten tunteminen riittää. Kun tehonkulutusta arvioidaan Hammingin etäisyydellä tai Hammingin painolla ovat tehonkulutusarviot suhteellisia. Tehonkulutuksen suhteellisiin muutoksiin verrattavissa olevan jännitteen ja arvioidun tehonkulutuksen välinen linearinen yhteys voidaan laskea korrelaation avulla.

Hyökkäyksen onnistumiseksi tarvitaan tehonkulutusmittauksia hetkeltä, jolloin salauslaite suorittaa hyökkäyksen kohteena olevia operaatioita. Yksi näyte jokaista salattua lohkoa kohti riittää hyökkäyksen suorittamiseen. Oikeaa hetkeä ei välttämättä tunneta tarkasti ja näytteitä joudutaan keräämään pitkältä ajalta. Oikea hetki on kellonreuna, jonka seurauksena hyökkäyksen kohteena oleva tilanvaihdos tapahtuu.

Mittausvastuksen valinnassa tulee huomioida, että mikäli mittausvastus on liian suuri, se saattaa haitata FPGA:n normaalia toimintaa alentamalla FPGA:n käyttöjännitettä. Mikäli mittausvastus on pieni voivat jännitteen muutokset olla pieniä ja niitä on vaikea havaita oskilloskoopin resoluutiolla. Sopiva mittausvastus on suuruudeltaan 1-100 Ohmia.

3.3 Tehonkulutuksen arvioiminen

3.3.1 Hammingin etäisyys ja Hammingin paino tehonkulutusmalleina

Tehonkulutusmallilla arvioidaan elektronisen laitteen tehonkulutusta. Jos laitteen toiminta ja sen käsittelemä tieto tunnetaan, voidaan tehonkulutus arvioida tarkasti. Ulkopuolisilla tahoilla ei ole tarkkaa tietoa laitteen toiminnasta tai sen käsittelemästä tiedosta. Laitteen toiminnasta voidaan tehdä oletuksia, joiden perusteella tehonkulutusta voidaan arvioida.

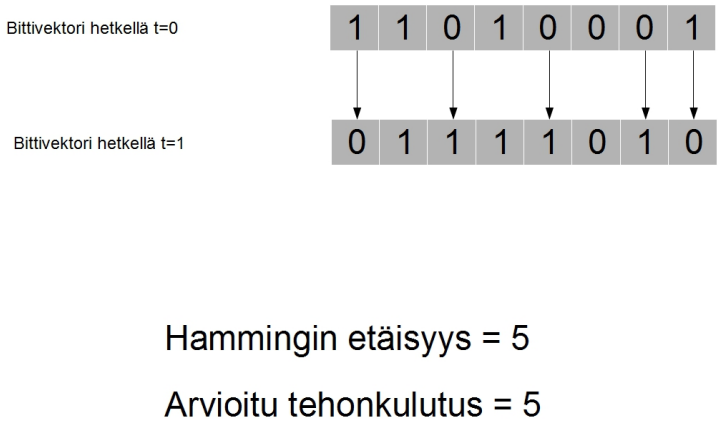
Differentiaalisessa tehoanalyysihyökkäyksessä käytetään tehonkulutusmallina Hammingin etäisyyttä tai Hammingin painoa [6]. Hammingin etäisyys kertoo eri tiloissa olevien bittien määrän kahdessa bittivektorissa. Jos on tiedossa millaisia bittivektoreita elektronisessa salauslaitteessa muodostuu, bittivektorien alkioiden voidaan ajatellaan kuvaavan salauslaitteen transistoreja, jotka liittyvät kyseisen alkion tilan vaihtumiseen.

Hammingin paino kertoo kuinka moni bitti bittivektorissa on tilassa 1. Hammingin paino vastaa Hammingin etäisyyttä, jos toisen Hammingin etäisyydellä verrattavan bittivektorin kaikki bitit ovat nollia. Joissain tilanteissa tällainen tehonkulutusmalli on realistinen ja Hammingin paino toimii yhtä hyvin kuin Hammingin etäisyys. Yleensä Hammingin etäisyys kuvaa elektronisen laitteen tehonkulutusta paremmin kuin Hammingin paino. [6]

Transistorien tilojen vaihtuminen kuluttaa elektronisissa laitteissa tehoa. Arvioitaessa tehonkulutusta Hammingin etäisyydellä tai Hammingin painolla yhden bitin tilan vaihtuminen aiheuttaa yhden yksikön suuruisen tehonkulutuksen riippumatta siitä kuinka usea transistori salauslaitteessa vaihtaa tilaansa. Arvioitu tehonkulutus ei anna tietoa absoluuttisesta tehonkulutuksesta. Tietoa saadaan erilaisten tilojen vaihtumisten suhteellisista tehonkulutuksista. Kuvassa 12 on esimerkki Hammingin etäisyyden käytöstä tehonkulutuksen arviointiin. Hammingin etäisyyttä voidaan käyttää integroidun piirin rekisterien ja tiedonsiirtokanavien tilojen vaihtumisen tehonkulutuksen suhteelliseen arviointiin [6].

Jos voidaan laskea kaksi bittivektoria joiden mukaiset tilat muodostuvat peräkkäin FPGA:ssa, voidaan käyttää Hammingin etäisyyttä tilanvaihdoksen tehonkulutuksen arviointiin. Hammingin etäisyys arvioi yhden bitin aiheuttaman arvioidun tehonkulutuksen olevan riippumaton muutoksen suunnasta. Tilan vaihtumisen nollasta yhteen ja yhdestä nollaan arvioidaan kuluttavan yhtä paljon tehoa. Elektronisessa laitteessa tilan vaihtuminen matalasta korkeaan voidaan erottaa vaihtumisesta korkeasta matalaan. [6]

Hammingin painoa voidaan käyttää tehonkulutuksen arviointiin, jos salauslaitteen tuottamia bittivektoreita peräkkäisillä hetkillä ei ole tiedossa. Hammingin etäisyys toimii vain jos on tiedossa peräkkäisiä bittivektoreita. Hammingin painoa voidaan käyttää koska bittien tilojen vaihtuminen eri suuntiin aiheuttaa hieman erilaisen tehonkulutuksen. Jos edeltävällä hetkellä bittivektorin arvo on satunnainen, niin riittävällä määrällä jälkimmäisen bittivektorin arvoja edeltävän bittivektorin arvojen vaikutus lähestyy nollaa. [6]



Kuva 12: Hammingin etäisyyden käyttö tehonkulutuksen arviointiin.

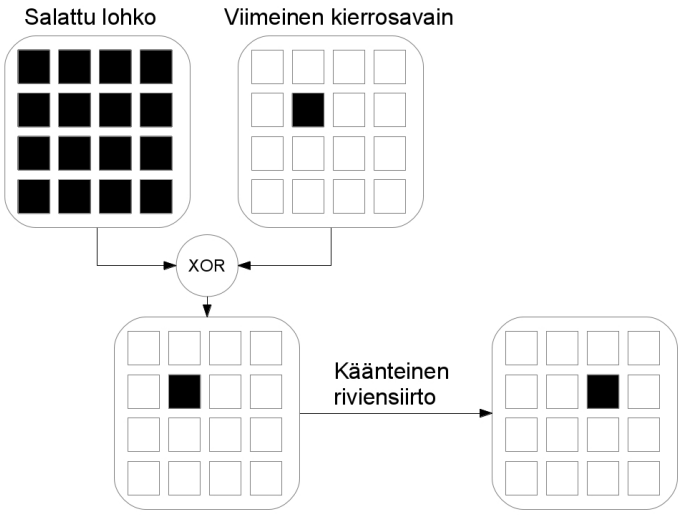
3.3.2 Väliarvojen laskeminen

Hammingin etäisyyttä voidaan käyttää tehonkulutusmallina, jos on tiedossa kaksi peräkkäistä salauslaitteen tuottamaa bittivektoria. Hammingin painoa käytettäessä tehonkulutusmallina yhden välituloksen tunteminen salattua lohkoa kohti riittää. Koska AES-salauksen toteutuksesta FPGA:ssa ei ole tarkkaa tietoa, voidaan käyttää ainoastaan salausalgoritmin perusteella laskettuja välituloksia.

Salattuja lohkoja kerätään mittausten aikana. Salausvaimen avulla voidaan laskea käänteisiä operaatioita käyttäen salauksen aikana tuotetut AES-välitulokset ja alkuperäinen salaamaton lohko. Salausavainta ei ole käytettävissä mutta se voidaan yrittää arvata. Brute force-hyökkäys perustuu kaikkien mahdollisten avaimien systemaattiseen kokeiluun. Hammingin tehonkulutusmallit toimivat kaiken pituisilla bittivektoreilla joten laskettavat välitulokset voivat olla minkä tahansa pituisia. AES-algoritmin viimeisen kierroksen välituloksista voidaan laskea tavun kokoinen osa, jos tunnetaan tavun kokoinen osa viimeisen kierroksen kierrosavaimesta.

Jonojensekoitusoperaatiossa jokainen tavu vaikuttaa neljään tavuun operaation tuloksessa. Muissa operaatioissa jokainen tavu vaikuttaa vain yhteen tavuun. Viimeisellä AES-kierroksella ei käytetä sarakkeidensekoitusoperaatiota, joten yhden tavun kokoisella avainarvauksella voidaan laskea tavun kokoinen bittivektori jokaisesta välituloksesta ennen toiseksi viimeistä kierrosavaimen lisäystä.

Toiseksi viimeisellä AES-kierroksella käytetään sarakkeidensekoitusoperaatiota. Laskettaessa välituloksia toiseksi viimeiseltä kierrokselta tarvitaan tietoa neljästä kierrosavaimen tavusta viimeiseltä ja toiseksi viimeiseltä kierrokselta. Hyökkäyksen laskennallinen vaiva kasvaa merkittävästi jos tarvitaan muita kuin viimeisen AES-kierroksen välituloksia. Toiseksi viimeisen AES-kierroksen välituloksia voidaan tarvita jos hyökkäys ei onnistu viimeisen AES-kierroksen välituloksilla. Taulukossa 2 esitetään avainarvausten lisääntyminen, kun välituloksia lasketaan useammilta



Kuva 13: Tunnetun tavun sijainti välituloksissa.

AES-kierroksilta tai jos käytetään useampaa tavua. Tässä työssä sarakkeidensekoitusoperaatiota ei käytetä AES-välitulosten lakemiseen.

Taulukko 2: Avainarvausten määrä erilaisilla AES-välitulosten laskutavoilla.

AES-kierros	**Tavuja**	**Avainarvaukset**
10. kierros	1	$16 * 2^8$
10. kierros	4	$4 * 2^{32}$
9. kierros	1	DPA ei onnistu
9. kierros	4	$4 * 2 * 2^{32}$
8. kierros	1	DPA ei onnistu
8. kierros	4	$4 * 2 * 2^{32}$

Kuvassa 13 on merkitty mustalla tunnetut ja laskettavissa olevat tavut, kun tunnetaan viimeisen kierrosavaimen kuudes tavu. Käänteinen riviensiirto on ainoa operaatio joka siirtää tavun sijaintia. Laskettavissa olevan tavun sijainti tavujenkorvausoperaation jälkeen on sama kuin käänteisen riviensiirron jälkeen. Tunnetun tavun sijainnin siirtyminen täytyy ottaa huomioon vertaillessa laitteen tuottamia peräkkäisiä tavuja.

3.4 Korrelaatioanalyysi

Korrelaatiolla saadaan selville onko näytejoukkojen välillä lineaarista yhteyttä. Korrelaatioanalyysillä voidaan arvioida vastaako arvioitu tehonkulutus mitattua tehonkulutukseen verrannollista jännitettä ja tunnistaa oikea avainarvaus.

Jos korrelaatiokerroin on lähellä nollaa, näytejoukot ovat toisistaan lineaarisesti

riippumattomia. Jos korrelaatio selvästi poikkeaa nollasta, on mitatulla ja arvioidulla tehonkulutuksella lineaarinen yhteys.

Differentiaalisessa tehoanalyysihyökkäyksessä korrelaatioanalyysiä käytetään oikean avainarvauksen erottamiseen vääristä. Mitattua tehonkulutukseen verrannollista jännitettä verrataan eri avainarvauksilla laskettuihin arvioituihin tehonkulutuksiin. Väärällä arvauksella korrelaatio on lähellä nollaa. Oikealla arvauksella korrelaatio on havaittavasti erilainen kuin muilla avainarvauksilla ajanhetkellä, jolloin laite on suorittanut operaatioita joihin hyökkäys on kohdistettu. Muilla ajanhetkillä myös oikealla arvauksella korrelaatiokerroin on lähellä nollaa. Tehonkulutuksen arvointi ollaan tehty vain yhdelle ajanhetkelle ja tätä arviota verrataan kaikkien mittausten kaikkia näytteitä vastaan.

Mittaustuloksia ja niitä vastaavia salattuja lohkoja tarvitaan paljon sillä mittaustuloksissa on mukana kohinaa ja tehonkulutuksen arviointiin käytetty tehonkulutusmalli ei välttämättä kuvaa laitteen todellista tehonkulutusta hyvin. Kohina vaikeuttaa korrelaatiopiikin havaitsemista, mutta keskiarvoistamalla kohina lähestyy nollaa. Kun kohina on riittävän pientä, voidaan avainarvauksen nollasta poikkeava raja-arvo havaita.

Hyökkäystä voidaan pitää onnistuneena, kun voidaan riittävän luotettavasti erottaa oikea arvaus vääristä. Käytännössä korrelaatiopiikin tulee olla selvästi suurempi kuin seuraavaksi suurin korrelaatiopiikki. Korrelaatiopiikkejä voi syntyä kohinan seurauksena. Kohinan vuoksi mitatun ja arvioidun tehonkulutuksen välillä voi olla yksittäisten vertailujen aikana keskimääräistä lineaarisempi yhteys. Kohinan aiheuttamia korrelaatiopiikkejä voi muodostua, mutta suurilla mittaustulosmäärillä niiden todennäköisyys pienenee. Korrelaatiopiikkejä voi muodostua myös jos laitteessa suoritetaan salaukseen liittymättömiä operaatioita, jotka korreloivat laskettujen välitulosten kanssa. Korrelaatiopiikkejä esitetään luvussa 4.4.

4 Tehoanalyysihyökkäyksen suorittaminen

Differentiaalisen tehoanalyysihyökkäykseen tarvitaan oskilloskooppi ja tietokone. Oskilloskoopin avulla mitataan salauslaittteen tehonkulutukseen verrannollista jännitettä useiden salausoperaatioiden ajalta. Tietokoneella kerätään salauslaitteen salaamaa tietoa ja lasketaan hyökkäystulokset.

4.1 Hyökättävien kohteiden kuvaukset

4.1.1 Sakura-G

Differentiaalisen tehoanalyysihyökkäyksen toimivuutta tutkittiin kahdella eri salauslaitteella. Ensimmäinen tutkittava kohde oli Sakura-G. Sakura-G on sivukanavahyökkäyksien tutkimiseen suunniteltu salauslaite [11]. Laitteen on valmistanut Morita tech.

Tutkittavaa salaustoteutusta suoritetaan laitteen Spartan6 FPGA-piirillä. Alustan toinen Spartan6 FPGA välittää tietoa salausta suorittavan FPGA:n ja USB-tiedonsiirtoväylän (Universal Serial Bus) välillä. USB-väylä siirtää tietoa Sakura-G:n ja tietokoneen välillä. Tietokone lähettää salauslaitteelle satunnaisia lohkoja ja vastaanottaa salatut lohkot.

Sakura-G ottaa käyttöjännitteensä USB-liitännästä. USB-liitännästä saadaan viiden Voltin jännite. Jännite muutetaan regulaattorien avulla sopiviksi jännitteiksi Sakura-G:n komponenteille. Salausta suorittavan FPGA:n käyttöjännite on 1,2 volttia. FPGA toimii 48 MHz:n kellotaajuudella. Kellosignaali luodaan erillisellä oskillaattorilla. [11]

Tehonkulutukseen verrannolliset jännitemittaukset suoritetaan Sakura-G:n mittausvastuksen avulla. Mittausvastus on FPGA:n ja käyttöjännitteen välissä. Mittausvastuksen suuruus on yksi Ohmi. Mittausvastuksen molemmilla puolilla on SMA-liittimet (SubMiniature version A), joiden kautta mittauspisteen jännite voidaan mitata. Sakura-G:n lohkokuva nähdään kuvassa 14.

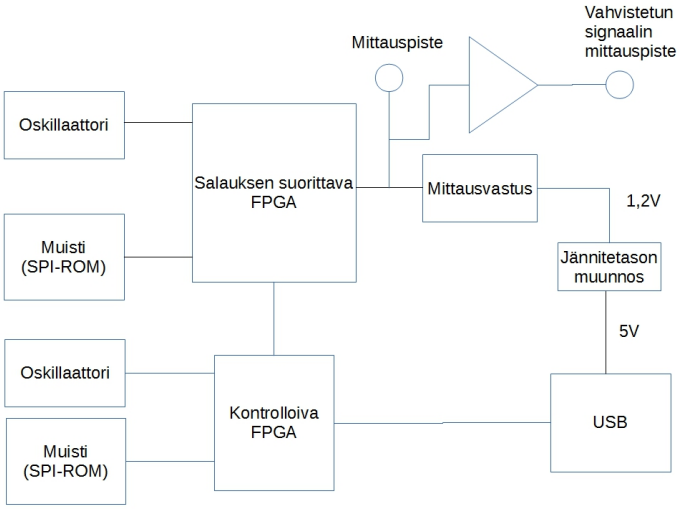
Mittaukset suoritettiin FPGA:n puoleisesta mittauspisteestä. FPGA:n puoleisen mittauspisteen jännite voidaan mitata vahvistettuna kolmannen SMA-liittimen kautta. Vahvistettua jännitettä ei mitattu, koska hyökkäys onnistui vahvistamattomalla signaalilla. [11]

Laitteessa on yleiskäyttöisiä liitäntöjä, joiden avulla voidaan välittää tietoa laitteeseen tai laitteesta. Esimerkiksi liipaisusignaali, jota voidaan käyttää mittauksen ajoittamiseksi salausoperaation alkuun on johdettu yhteen liitäntään. Kuvassa 15 nähdään Sakura-G.

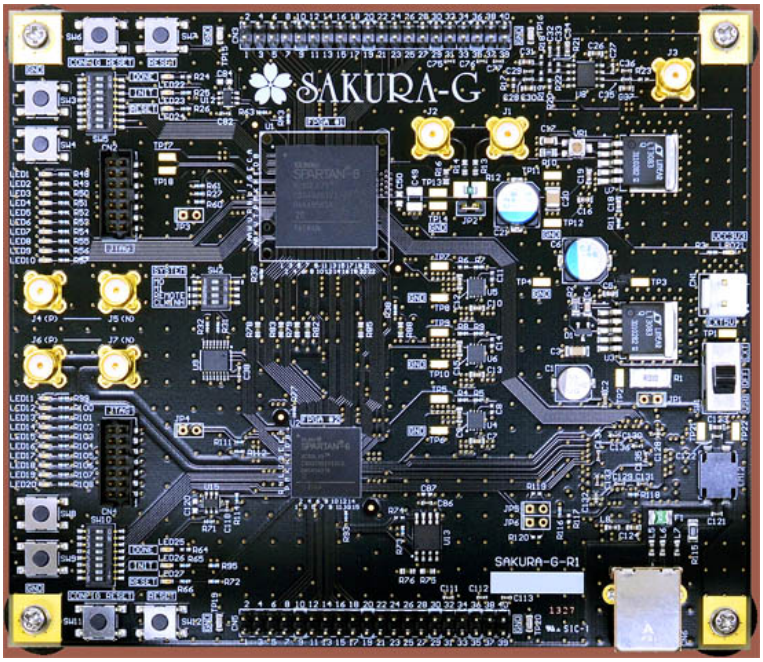
4.1.2 Toteutettu salauslaite

Toinen salauslaite jolla differentiaalista tehoanalyysihyökkäystä tutkittiin toteutettiin Spartan6 FPGA-piirillä. Salauslaitteen piirilevy suunniteltiin tätä työtä varten. Salauslaite nähdään kuvassa 16.

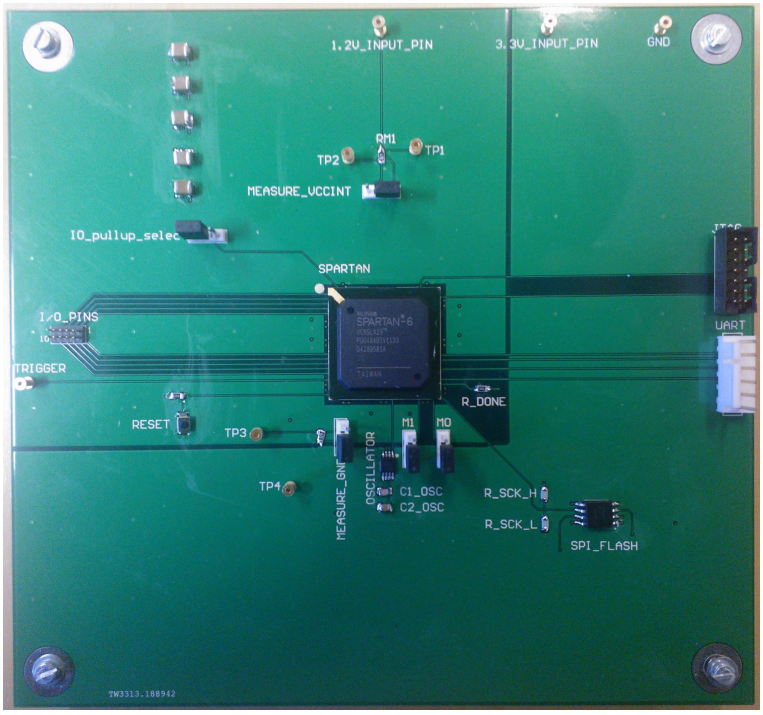
Salauslaite käyttää tiedonsiirtoon UART-sarjaliikenneporttia (Universal Asynchronous Receiver Transmitter). Laitteessa on DS1088LU-10 oskillaattori joka välittää



Kuva 14: Sakura-G:n lohkokuva.



Kuva 15: Sakura-G

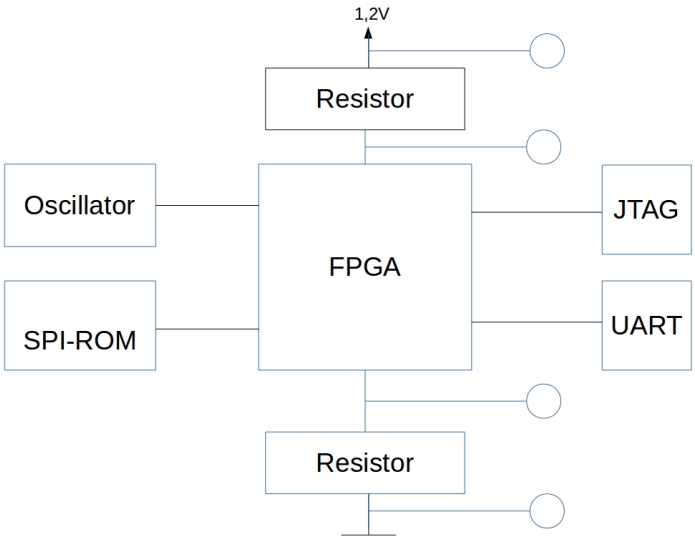


Kuva 16: Tähän työhön suunniteltu FPGA-salauslaite.

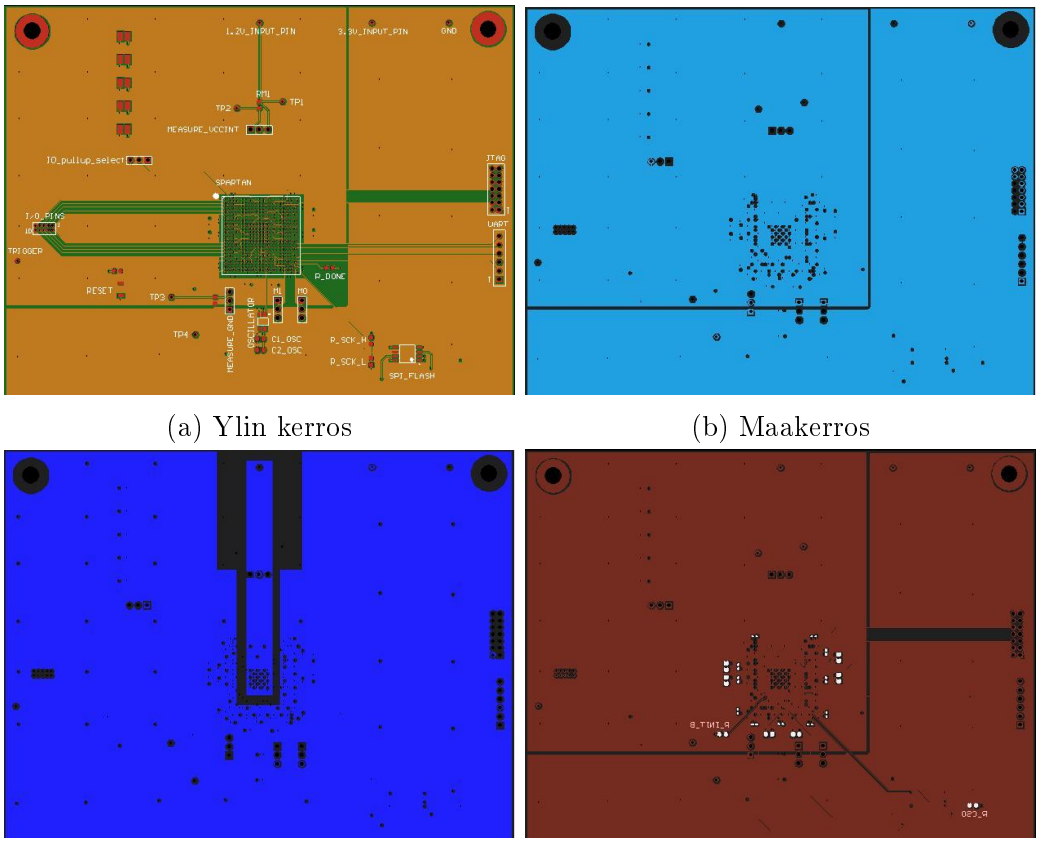
FPGA:lle 10 MHz:n kellosignaalin. Oskillaattori valittiin koska sen tuottaman taajuuden lämpötilariippuvuus 25 Celsiusasteen ympäristössä on pieni [12].

Laitteessa on kaksi mittausvastusta. Mittausvastukset voidaan ohittaa hyppylangan avulla. Mittausvastuksien suuruus on 50 Ohmia. Ensimmäinen mittausvastus on sijoitettu FPGA:n ytimen käyttöjännitteen ja piirilevylle tulevan positiivisen jännitteen välille. Toinen mittausvastus on sijoitettu FPGA:n maan ja piirilevyn maan välille. Toista mittausvastusta ei käytetty, koska Sakura-G:ssä ei ollut vastaavaa mittausmahdollisuutta ja haluttiin hyökkäysten olevan vertailukelpoisia laitteiden välillä. Liipaisusignaalille on erillinen mittauspiste, mihin lähetettään pulssi jokaisen AES-kierroksen alkaessa. Levyllä on kymmenen yleiskäyttöistä liitäntää, joita käytettiin laitteen oikean toiminnan varmistamiseen kokoamisen jälkeen. Laitteen lohkokuva näkyy kuvassa 17.

Toteutetun salauslaitteen piirilevy on nelikerroksinen. Komponentit on sijoitettu ylimpään ja alimpaan kerrokseen. Toiseksi ylin kerros on varattu kahdelle maatasolle. FPGA:lle on erillinen maataso ja muille komponenteille toinen maataso. Maatasot yhdistyvät jos maapuolen mittauspiiri on ohitettu hyppylangalla. Kolmas kerros sisältää 1,2 Voltin ja 3,3 Voltin jännitetasot. FPGA:n ydin, joka suorittaa salausoperaatiot, käyttää 1,2 Voltin jännitettä. FPGA:n liitännät ja laitteen muut komponentit käyttävät 3,3 Voltin jännitettä. Ytimen jännitetaso on pyritty suojaamaan kohinan vähentämiseksi eristämällä se toisesta jännitetasosta. Salauslaitteen piirilevyn kerrokset nähdään kuvassa 18.



Kuva 17: Toteutetun salauslaitteen lohkokuva.



(a) Ylin kerros

(b) Maakerros

(c) Käyttöjännitekerros

(d) Alin kerros

Kuva 18: Suunnitellun piirilevyn kerrokset.

Taulukko 3: AES-toteutuksien eroja.

Toteutus	**Katashita**	**De La Piedra**	**Usselmann**
Kierroksen kesto [sykliä]	1	2	1
Syklin kesto [kellojaksoa]	16	1	1
Ylimääräistä laskentaa	Ei	Kyllä	Ei
FPGA:n rekisterit [prosenttia]	2	1	2
FPGA:n Etsintätaulukot [prosenttia]	20	6	5

4.1.3 Salausalgoritmin toteutukset ja FPGA-piirien ohjelmointi

AES-salaus voidaan toteuttaa erilaisilla tavoilla FPGA-piirillä. Toteutustapojen suorituskyvyissä ja niiden käyttämien resurssien määrissä on eroja. Nopeat toteutukset kuluttavat yleensä enemmän resursseja kuin hitaammat. Esimerkiksi tavujenkorvausoperaation toteutustapa vaikuttaa merkittävästi käytettyihin resursseihin ja nopeuteen. Tavujenkorvausperaatio voidaan toteuttaa käyttämällä jokaiselle lohkon 16 tavulle omaa 256 tavusta koostuvaa etsintätaulukkoa. Tällainen toteutus on nopea, mutta kuluttaa paljon resursseja [3]. Vaihtoehtoisesti voidaan käyttää yhtä etsintätaulukkoa, josta korvattavat tavut haetaan vuorotellen kullekin tavulle.

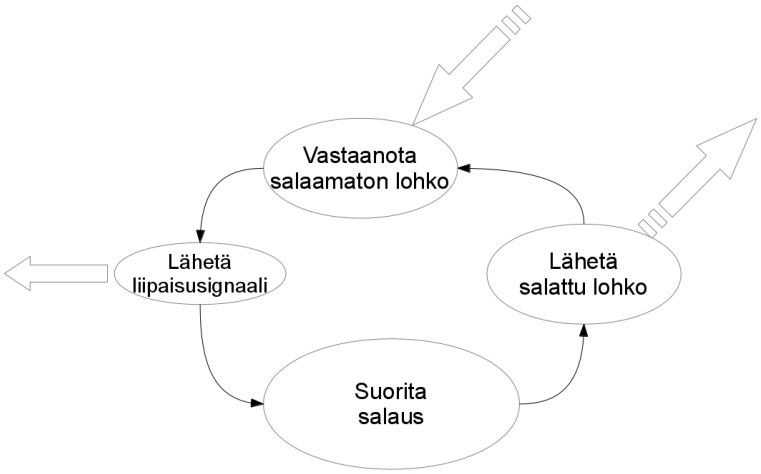
Differentiaalisen tehoanalyysihyökkäyksen vaarallisuus perustuu osittain siihen, että hyökkäyksen onnistumiseksi ei tarvita tarkkaa tietoa salauksen toteutuksesta. Laitteen käyttämää salausalgoritmia ei tarvitse tietää. Jos salausalgoritmia ei tiedetä, voidaan kokeilla kaikia algoritmeja joiden osittaisia välituloksia voidaan laskea. Jos joudutaan kokeilemaan erilaisia algoritmeja, hyökkäys kestää kauemmin.

Ensimmäisen tutkittavan AES-toteutuksen on suunnitellut Toshihiro Katashita. Toteutus on suunniteltu käytettäväksi Sakura-G laitteessa. Sivustolta http://satoh.cs.uec.ac.jp/SAKURA/hardware/SAKURA-G.html ladattiin ohjelmointitiedostot Sakura-G laitteen FPGA-piireille. AES-toteutus sisältyy salausta suorittavan FPGA:n ohjelmointitiedostoon. Ohjelmointitiedostot välitettiin FPGA-piireille JTAG-yhteyden kautta Xilinxin ISEimpact-sovelluksella.

Toteutetulla salauslaitteella tutkittiin differentiaalisen tehoanalyysihyökkäyksen toimivuutta Sakura-G:n AES-toteutusta ja kahta opencores.org sivustolta ladattua AES-toteutusta vastaan. AES-toteutusten oikea toiminta varmistettiin laitteistonkuvauskielisimuloinnein. Ensimmäisen opencores.org-sivustolta ladatun toteutuksen on ohjelmoinut Antonio De La Piedra [14]. Toisen opencores.org-sivuston AES-toteutuksen on ohjelmoinut Rudolf Usselmann [15]. Taulukkoon 3 on koottu AES-toteutusten eroja.

AES-toteutuksen lisäksi FPGA:lle ohjelmoitiin UART-tiedonsiirto ja tilakone. Ensimmäisessä tilassa tilakone vastaanottaa salattavan lohkon tietokoneelta. Kun lohko on vastaanotettu siirrytään seuraavaan tilaan. Toisessa tilassa FPGA lähettää liipaisusignaalin oskilloskoopille. Kolmannessa tilassa suoritetaan salaus vastaanotetulle lohkolle. Viimeisessä tilassa salattu lohko lähetetään tietokoneelle. Kuvassa 19 havainnollistetaan käytetyn tilakoneen toimintaa.

AES-toteutuksia tutkittiin mahdollisten hyökkäyskohtien löytämiseksi. Tukimuk-



Kuva 19: Salauslaitteen toiminta

```
//================================================ AES_Core
module AES_Core (din, dout, kin, sel);

   //------------------------------------------------
   input  [127:0] din, kin;
   input          sel;
   output [127:0] dout;

   //------------------------------------------------
   wire [31:0] st0, st1, st2, st3, // state
               sb0, sb1, sb2, sb3, // SubBytes
               sr0, sr1, sr2, sr3, // ShiftRows
               sc0, sc1, sc2, sc3, // MixColumns
               sk0, sk1, sk2, sk3; // AddRoundKey

   //------------------------------------------------
   // din -> state
   assign st0 = din[127:96];
   assign st1 = din[ 95:64];
   assign st2 = din[ 63:32];
   assign st3 = din[ 31: 0];
```

Kuva 20: Osa Katashitan AES-toteutuksesta.

sissa keskityttiin valittujen signaalien tilojen vaihdoksiin. Signaalit valittiin laitteistokuvauskielellä kirjoitettuja toteutuksia tutkimalla. Toteutuksista etsittiin signaaleja joihin AES-operaatioiden tulokset tallennetaan. Kuvassa 20 nähdään osa Katashitan AES-toteutuksesta, missä kaikkien operaatioiden tuloksille on oma signaalinsa.

Käytännöllisessä hyökkäyksessä hyökkääjä ei voi tutkia salausalgoritmin toteutusta. AES-algorimi ja FPGA-piirien ominaisuudet rajoittavat mahdollisia toteutustapoja. Katashitan ja Usselmanin toteutuksissa AES-kierrosten operaatioiden välitulokset tallennetaan peräkkäin samaan rekisteriin. Edeltävän kierroksen ope-

raation tulos korvataan uuden kierroksen operaation tuloksella. Tällaista toteutusta vastaan voidaan hyökätä laskemalla jonkin viimeisen kierroksen operaation tuloksen Hammingin etäisyys saman operaation toiseksi viimeisen kierroksen tulokseen.

De La Piedran toteutus on monimutkaisempi. Salattavan lohkon salauksen lisäksi toteutus suorittaa salausta toiselle lohkolle. Toista lohkoa ei tunneta eikä sen käyttämiselle havaittu syytä. Salauksen suorittaminen toiselle lohkolle vaikuttaa tarpeettomalta. Yhden AES-kierroksen suoritus kestää kaksi sykliä. Muissa tutkituissa AES-toteutuksissa kierros suoritetaan yhdessä syklissä. Salattavan lohkon välitulokset tallennetaan samaan signaaliin, mutta vain ensimmäisen syklin aikana. Toisen syklin aikana signaaliin tallennetaan tuntemattoman lohkon välitulokset. Koska toista lohkoa ei tunneteta, sen välituloksia ei voida laskea.

Katashitan AES-toteutuksessa yksi sykli kestää 16 kellojaksoa. Muissa toteutuksissa sykli kestää yhden kellojakson.

4.2 Mittaukset

4.2.1 Oskilloskooppi ja Labview

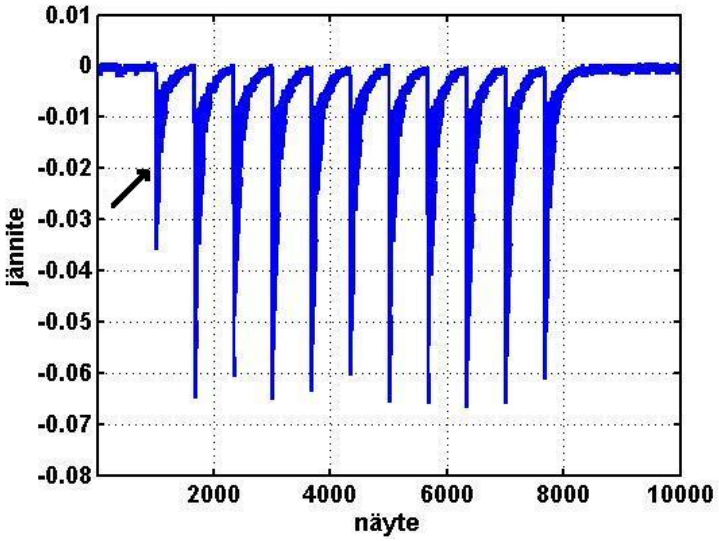
Jännitemittaukset suoritettiin Lecroyn Wavesurffer 44MXS-A oskilloskoopilla. Oskilloskooppia ohjattiin Labview-ohjelmistolla. Labview-ohjelmistolla mittaustulokset tallennettiin tietokoneelle.

Differentiaalisessa tehoanalyysihyökkäyksessä mitattujen tehonkulutukseen verrannollisten jännitemittausten ja vastaanotettujen salattujen lohkojen täytyy vastata toisiaan. Mittauksen väliin jääminen tai virheellinen liipaisu aiheuttaa sen, että mittaukset ja salattujen lohkojen avulla arvioidut tehonkulutukset eivät vastaa toisiaan.

Automaattisella kalibroinnilla parannetaan mittaustuloksia ympäristön lämpötilan muuttuessa. Automaattinen kalibrointi käynnistyy jos oskilloskoopin lämpötila muuttuu riittävästi. Automaattisen kalibroinnin aikana oskilloskooppi ei suorita mittauksia, mutta salauslaite suorittaa salausta mittalaitteesta riippumatta. Oskilloskoopin automaattista kalibrointia ei käytetä, koska automaattinen kalibrointi saattaa aiheuttaa tarpeellisten mittaustulosten menetyksen. Kalibroinnin tarkoituksena on parantaa mittaustuloksia, mutta differentiaalisen tehoanalyysihyökkäyksen kannalta on oleellisempaa saada kaikki mittaustulokset kerättyä oikeassa järjestyksessä.

Katashitan AES-toteutusta käytettäessä tehonkulutusta mitattiin koko salausoperaation ajalta. Muiden AES-toteutusten tehonkulutusta mitattiin viimeisten AES-kierrosten ajalta. Salauslaitteen lähettämän liipaisusignaalin avulla oskilloskoopin liipaisu ajoitettiin hetkeen, jolloin salausoperaatio alkaa.

Oskilloskoopin mittauspäät ovat herkkiä ulkopuolisille häiriöille ja saattavat aiheuttaa vääriä liipaisuja. Väärien liipaisujen välttämiseksi laitteiden maatasot kytkettiin yhteen ja mittauspäät maadoitettiin kytkemällä maadoitusjohdin yhteiseen maatasoon.



Kuva 21: Sakura-G -salauslaitteen tehonkulutukseen verrattavissa oleva jännite yhden 128 bitin salausoperaation ajalta.

4.2.2 Sakura-G

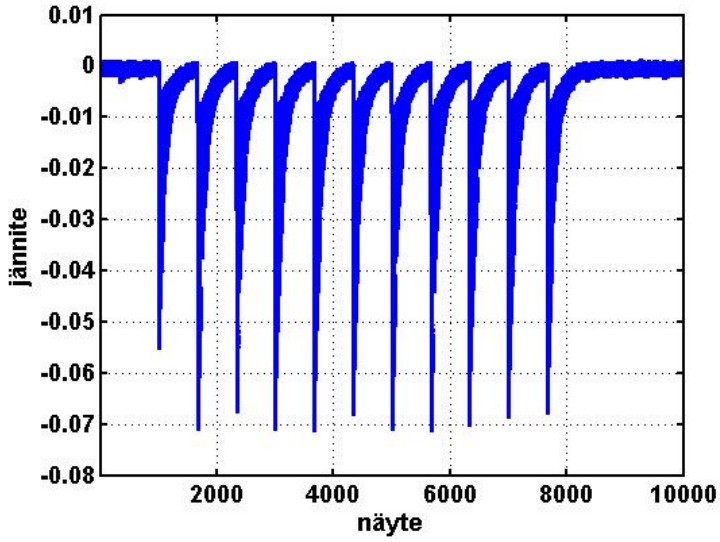
Sivustolta http://satoh.cs.uec.ac.jp/SAKURA/hardware/SAKURA-G.html ladattiin ohjelmisto satunnaisen datan lähettämiseksi ja salatun datan vastaanottamiseksi. Ohjelmiston avulla tietokone voi kommunikoida Sakura-G:n kanssa USB-liitännän kautta. Ohjelmisto tarkastaa vastaanotetut salatut lohkot ja keskeyttää toiminnan jos Sakura-G:ltä vastaanotettu salattu lohko ei vastaa ohjelman laskemaa salattua lohkoa.

Ohjelmistoa muokattiin tallentamaan vastaanotetut salatut lohkot. Salatut lohkot tallennetaan tiedostoon omalle rivilleen saapumisjärjestyksessä heksadesimaalilukuina. Ohjelmiston suoritukseen lisättiin viivettä mittaustulosten oikeellisuuden varmistamiseksi. Viive lisättiin lähetettävien satunnaisten lohkojen välille.

Sakura-G:n mittauspisteessä on SMA-liitäntä jonka kautta mittauspiste yhdistetään oskilloskooppiin johtimella. Liipaisusignaali voidaan viedä oskilloskoopille mittapään avulla. Oskilloskoopin mittapäät ovat herkkiä häiriöille. Häiriöt saattavat aiheuttaa vääriä liipaisuja. Sakura-G:ssä ei ole liitäntää mittauspään maadoitusjohtimelle.

Väärien liipaisujen aiheuttamat mittaustulokset voidaan tunnistaa, sillä niiden muoto eroaa selvästi oikealla liipaisulla saadun mittaustuloksen muodosta. Ylimääräiset mittaustulokset voidaan poistaa myöhemmin, jolloin mittaustulosten järjestys palautuu oikeaksi. Virheellisten mittausten poistaminen vaatii ylimääräistä laskentaa.

Ylimääräisen laskennan välttämiseksi liipaisu suoritettiin Sakura-G:tä käytettäessä suoraan tehonkulutukseen verrannollisesta jännitesignaalista. Kuvassa 21 nähdään Sakura-G:ltä mitattu jännitesignaali, jossa liipaisutaso on merkitty nuolella. Liipaisu asetettiin puoliväliin ensimmäistä laskevaa jännitepiikin reunaa. Laite ei suorita salauksen aikana muita tehtäviä.



Kuva 22: 5000 tehonkulutukseen verrannollista jännitemittausta päällekkäin.

Tehonkulutukseen verrannolliset jännitepiikit osoittavat alaspäin. Mittausvastuksen läpikulkevan virran kasvaessa mittauspisteen jännite pienenee maatason jännitteeseen verrattuna.

Jännitepiikkejä on 11. Ensimmäinen jännitepiikki on muita pienempi. Suuremmat piikit ovat seurausta AES-kierrosten kuluttamasta tehosta. Käytettäessä 128 bittiä pitkää avainta, AES suorittaa 10 kierrosta. Ensimmäinen piikki aiheutuu ensimmäisestä kierrosavaimensummausoperaatiosta, joka ei varsinaisesti kuulu mihinkään kierrokseen.

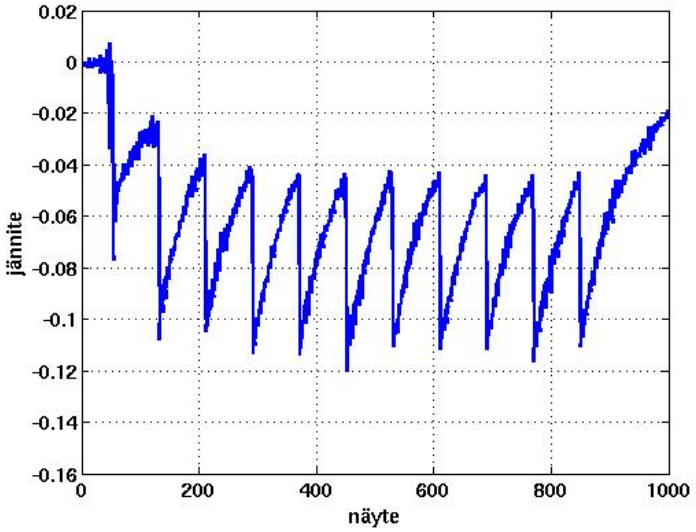
Satunnaisia lohkoja lähetettiin laitteelle 50000. Kuvassa 22 osa tehonkulutukseen verrannollisista jännitemittauksista on piirretty päällekkäin. Mittaustulosten yleinen muoto on samankaltainen. Mittaustuloksissa on kohinaa ja erilaisen datan käsittelystä aiheutunutta vaihtelua.

4.2.3 Toteutettu salauslaite

Toteutetulle FPGA-salauslaitteelle lähetettiin satunnaisia lohkoja. Satunnaiset lohkot luotiin Matlab-ohjelmistolla. UART-yhteys salauslaitteen ja tietokoneen välille muodostettiin Realterm-ohjelman avulla. Realterm-ohjelman avulla lähetettiin tavun suuruinen osa satunnaisesta lohkosta lähetysnopeudella 9600 symbolia sekunnissa UART-tiedonsiirtokanavaan. Tavun lähetyksen jälkeen odotetaan 150 millisekuntia ennen seuraavan tavun lähetystä. Viive lisättiin mittausten oikeellisuuden varmistamiseksi.

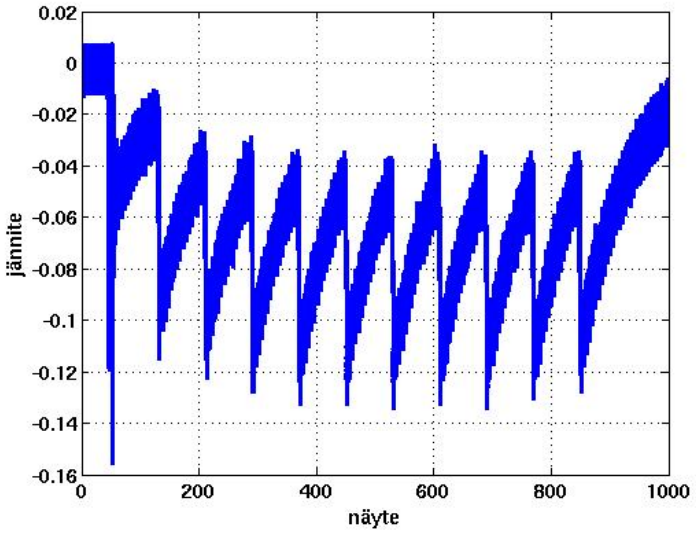
Toteutetulla salauslaitteella liipaisu suoritettiin salauslaitteen lähettämällä liipaisusignaalilla. Katashitan AES-toteutuksella liipaisu voidaan suorittaa myös tehonkulutussignaalista. Muilla AES-toteutuksilla liipaisua ei voida helposti suorittaa suoraan tehonkulutussignaalista, sillä jännitesignaalista ei voida selvästi erottaa AES-operaation alkamishetkeä.

Kuvassa 23 nähdään tehonkulutukseen verrannollinen jännite yhden salausoperaation ajalta käytettäessä Katashitan AES-toteutusta. AES-kierrokset ovat selkeästi havaittavissa. Kierrosten välillä jännite ei ehdi laskeutua alkutilaan. Tämä johtuu laitteen kapasitanssin, vastuksen ja laitteen kellosignaalin suhteista.



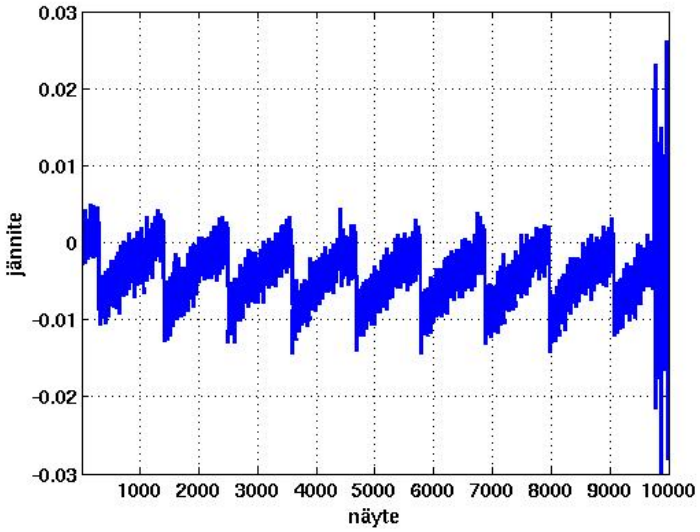
Kuva 23: FPGA -salauslaitteen tehonkulutukseen verrannollinen jännite salausoperaation aikana käytettäessä Katashitan AES-toteutusta.

Kuvassa 24 10000 jännitemittausta on piirretty päällekkäin. Yleinen muoto on yhtenäinen. Kohinasta johtuen mittauksissa on vaihtelua. Vaihtelu johtuu osittain käsitellystä tiedosta. Käsitelty tieto on erilainen jokaisen mittauksen aikana.



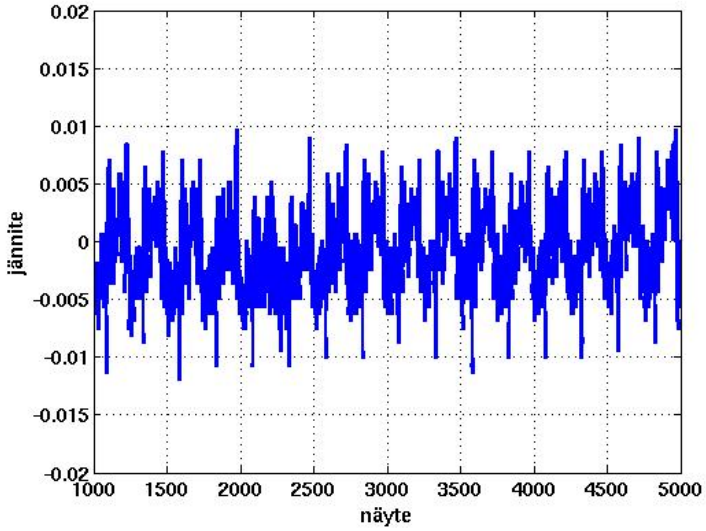
Kuva 24: 10000 tehonkulutukseen verrannollista jännitemittausta piirrettynä päällekkäin.

De La Piedran AES-toteutuksella AES-kierrokset voidaan erottaa toisistaan. AES:n aiheuttamat piikit ovat matalampia kuin Katashitan AES-toteutuksessa. Kuvassa 25 nähdään jännitemittaus toisella AES-toteutuksella.



Kuva 25: Tehonkulutukseen verrannollinen jännite De La Piedran AES-toteutuksella.

Usselmannin AES-toteutuksella AES-kierroksia ei havaita selvästi. Tehonkulutus aiheuttaa matalan ja nopean piikin. Tehonkulutukseen verrannollinen jännitemittaus kolmannella AES-toteutuksella nähdään kuvassa 26.

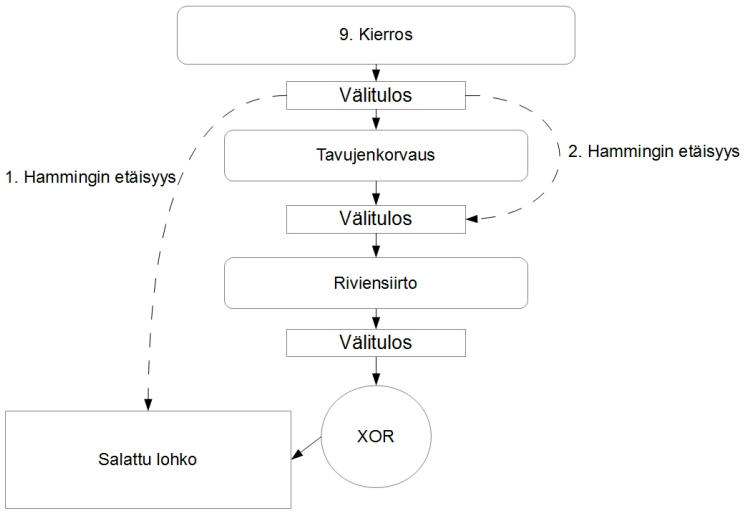


Kuva 26: Tehonkulutukseen verrannollinen jännite Usselmannin AES-toteutuksella.

4.3 Arvioidun tehonkulutuksen laskeminen

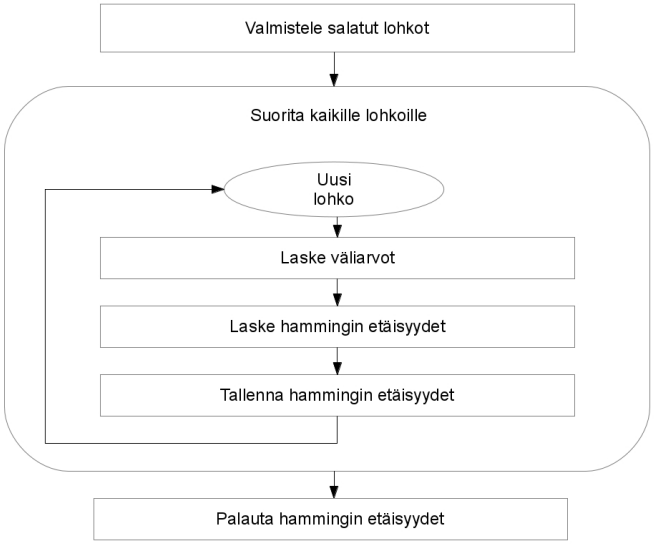
Salauslaitteen tehonkulutusta voidaan arvioida Hammingin etäisyydellä. Hammingin etäisyys lasketaan kahden AES-välituloksen välillä. AES-toteutuksesta riippuu miten välitulokset tallennetaan FPGA:ssa. AES-toteutuksia tutkimalla havaittiin tietyn operaation tuloksen tallentuvan samaan rekisteriin. Hammingin etäisyys voidaan laskea jonkin operaation viimeisen ja toiseksi viimeisen kierroksen tulosten välillä. Toisen kierroksen välitulosten laskeminen on työlästä, joten lasketaan vain viimeisen kierroksen välitulokset.

Viimeisen kierroksen välitulosten kahdeksan bittiä leveiden osien avulla lasketaan Hammingin etäisyyksiä. Ensimmäisessä hyökkäyksessä lasketaan Hammingin etäisyydet salatun lohkon ja toiseksi viimeisen kierrosavaimensummausoperaation tuloksen välillä. Toisessa hyökkäyksessä lasketaan Hammingin etäisyydet toiseksi viimeisen kierrosavaimensummausoperaation tuloksen ja viimeisen tavujenkorvausoperaation tuloksen välillä. Hammingin painolla voidaan arvioida salauslaitteen tehonkulutusta jos hyökkäykset Hammingin etäisyyksillä eivät toimi. Kolmannessa hyökkäyksessä lasketaan viimeisen tavujenkorvausoperaation tulosten Hammingin painot. Kuvassa 27 nähdään välitulokset, joiden Hammingin etäisyydet laskettiin.

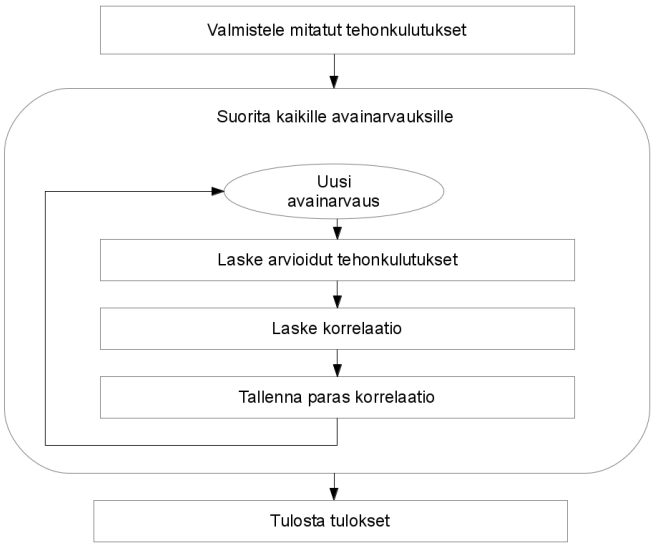


Kuva 27: Hyökkäyksissä käytetyt välitulokset

Kuvassa 28 nähdään algoritmi jolla arvioidut tehonkulutukset laskettiin. Laskenta suoritettiin Matlab-ohjelmalla. Matlab-funktio laskee salattua tekstiä vastaavat tehonkulutusarviot eri avainarvauksilla ja tallentaa ne. Tehonkulutusarviot lasketaan kaikilla avainarvauksilla jokaiselle salatulle lohkolle.



Kuva 28: Arvioidun tehonkulutuksen laskeminen



Kuva 29: Hyökkäystulosten laskenta.

4.4 Korrelaatioanalyysi

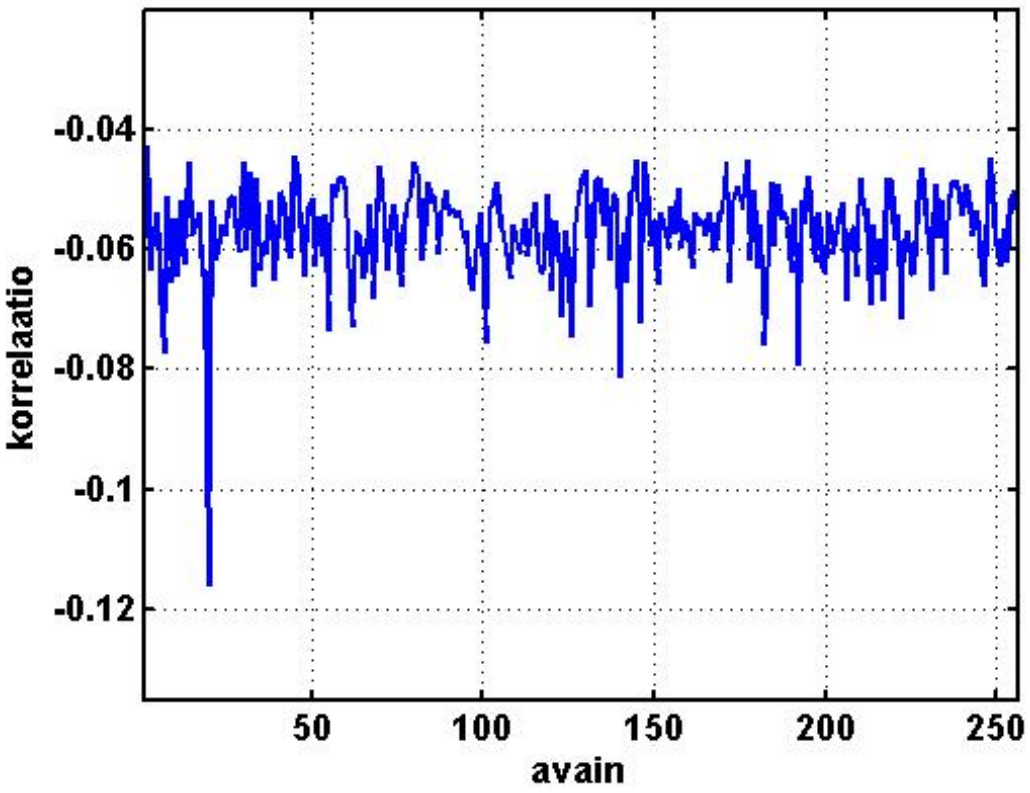
4.4.1 Sakura-G

Korrelaatio laskettiin Matlabin corr-funktiolla. Corr -funktiolle annettavilla matriiseilla tulee sama määrä rivejä. Sarakkeiden määrä voi vaihdella. Arvioituja tehonkulutuksia täytyy olla yhtä paljon kuin tehonkulutukseen verrannollisia jännitemittauksia. Jokaista arvioitua tehonkulutusarvoa verrataan samalla tavalla jokaisen mittaustuloksen kaikkiin näytteisiin. Kuvassa 29 nähdään hyökkäystulosten laskentaan käytetty algoritmi.

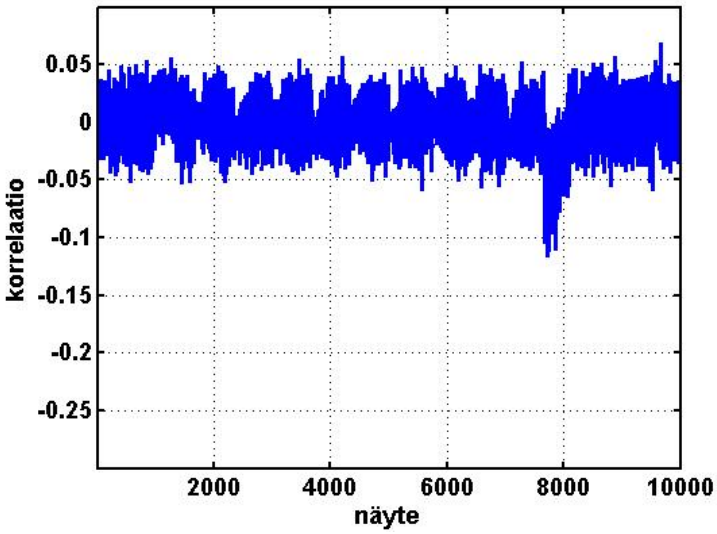
Ensimmäinen hyökkäys suoritettiin laskemalla salatun lohkon tavun ja viimeistä tavujenkorvausoperaatiota edeltävän väliarvon välinen Hammingin etäisyys. Kuvassa 30 nähdään hyökkäystulos Sakura-G:n viimeisen kierroksen kierrosavaimen ensimmäistä tavua vastaan 4000 salattulla lohkolla ja niitä vastaavilla tehonkulutukseen verrannollisina jännitemittaustuloksilla. Käytetty salausavain heksadesimaalimuodossa on 00 01 02 03 04 05 06 07 08 0A 0B 0C 0D 0E 0F. Viimeisen kierroksen kierrosavain on 13 11 1D 7F E3 94 4A 17 F3 07 A7 8B 4D 2B 30 C5. Neljä bittiä voidaan esittää heksadesimaalilukuna. Oikea avainarvaus on heksadesimaalimuodossa 13 ja desimaalimuodossa 19. Hyökkäystuloksesta nähdään itseisarvoltaan suurimman piikin sijaitsevan paikalla 20. Matlabissa indeksointi alkaa luvusta 1 joten suurin korrelaatiopiikki on muodostunut oikealla avainarvauksella lasketulla arvioidulla tehonkulutuksella.

Jokainen viimeisen kierrosavaimen tavu voidaan tunnistaa samalla tavalla. Tunnistukseen tarvittava mittaustulosmäärä vaihtelee. Tässä hyökkäyksessä kaikkien tavujen oikea avainarvaus aiheutti suurimman piikin 3400 mittaukstuloksella. Suurin osa tavuista saatiin tunnistettua alle 3000 mittaustuloksella.

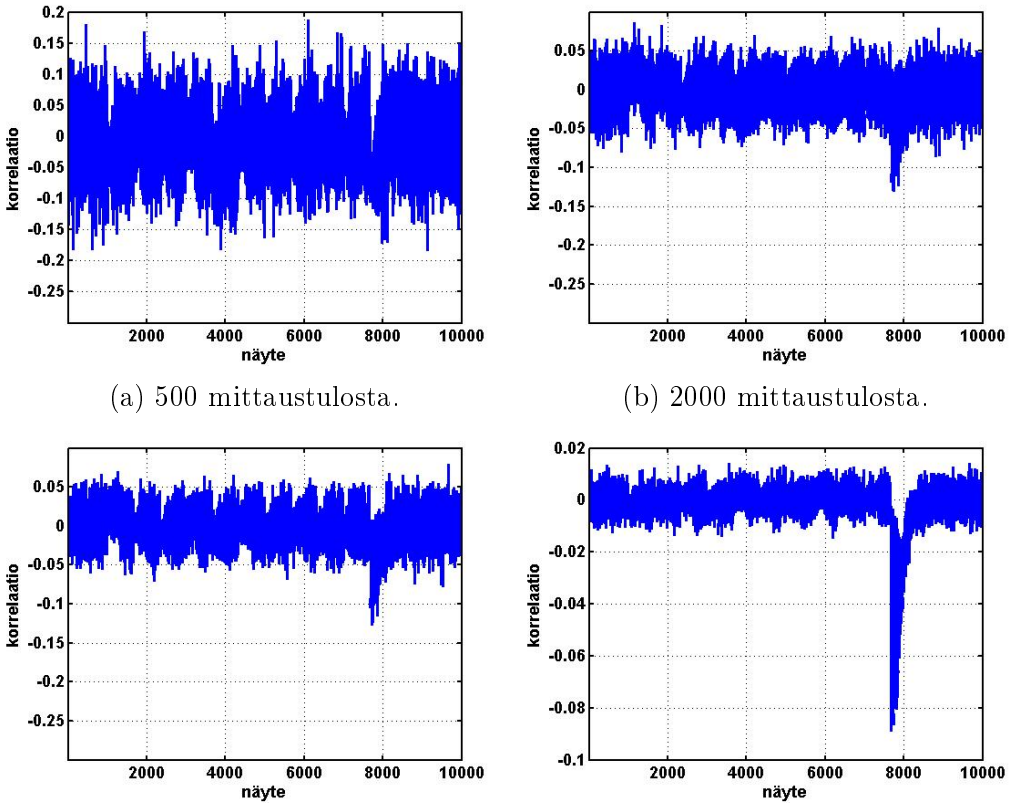
Kuvista 21 ja 31 nähdään korrelaatiopiikin muodostuvan hetkellä jolloin suoritetaan viimeistä AES-kierrosta. Piikki on AES-kierrokseen kuluvan ajan levyinen.



Kuva 30: Paras korrelaatio jokaisella avainarvauksella käytettäessä ensimmäistä Hammingin etäisyyttä 4000 mittaustuloksella.



Kuva 31: Korrelaatio ajan suhteen 4000 mittaustuloksella.



(a) 500 mittaustulosta.

(b) 2000 mittaustulosta.

(c) 3000 mittaustulosta.

(d) 50000 mittaustulosta.

Kuva 32: Korrellaatio ajan suhteen oikealla avainarvauksella ensimmäisellä hammingin etäisyydellä.

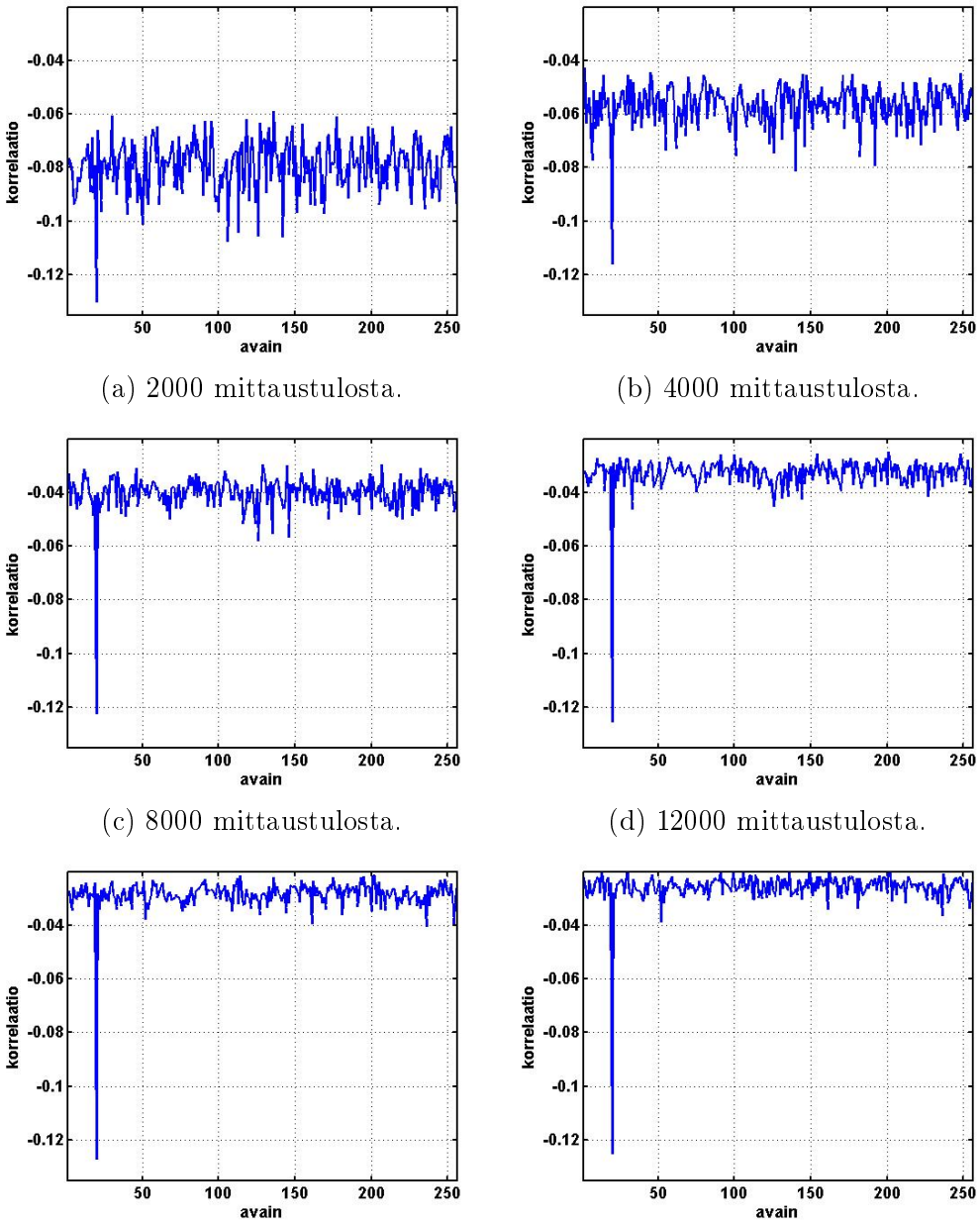
Kuvassa 32 nähdään miten mittaustulosten lisääminen vaikuttaa korrelaatioon. Kuvan 32a perusteella oikeaa avainta ei voida tunnistaa, sillä korrelaatiopiikki ei erotu kohinasta.

Lisäämällä mittaustuloksia oikea avainarvaus saadaan erottumaan. Kuvassa 32b nähdään korrelaatioanalyysin tulos 2000 mittaustuloksella. Korrelaatiopiikki alkaa muodostumaan mutta on edelleen vaikeasti havaittava ja kohinaa pienempi.

3000 mittaustuloksella oikean avainarvauksen aiheuttama korrelaatiopiikki nähdään kuvassa 32c. 50000 mittauksella kohina on pientä suhteessa oikean avainarvauksen korrelaatiopiikkiin 32d.

Korrelaatiopiikki muodostuu oikealla avainarvauksella, jos käytetään sopivaa tehonkulutusmallia. Muillakin avainarvauksilla saattaa muodostua korrelaatiopiikkejä. Väärillä avainarvauksilla muodostuneita korrelaatiopiikkejä kutsutaan haamupiikeiksi (ghost peaks) [13].

Haamupiikkejä muodostu jos väärillä avainarvauksilla lasketut arvioidut tehonkulutukset korreloivat mitatun tehonkulutukseen verrannollisen jännitteen kanssa. Korrelointi voi johtua kohinasta tai tehonkulutusmallista. Kohinasta aiheutuvat haamupiikit vaimenevat suurilla tehonkulutusmittaus määrillä. Salauslaite saattaa suorittaa hyökkäykseen liittymättömiä operaatioita jotka korreloivat tehonkulutusmal-



(a) 2000 mittaustulosta.

(b) 4000 mittaustulosta.

(c) 8000 mittaustulosta.

(d) 12000 mittaustulosta.

(e) 16000 mittaustulosta.

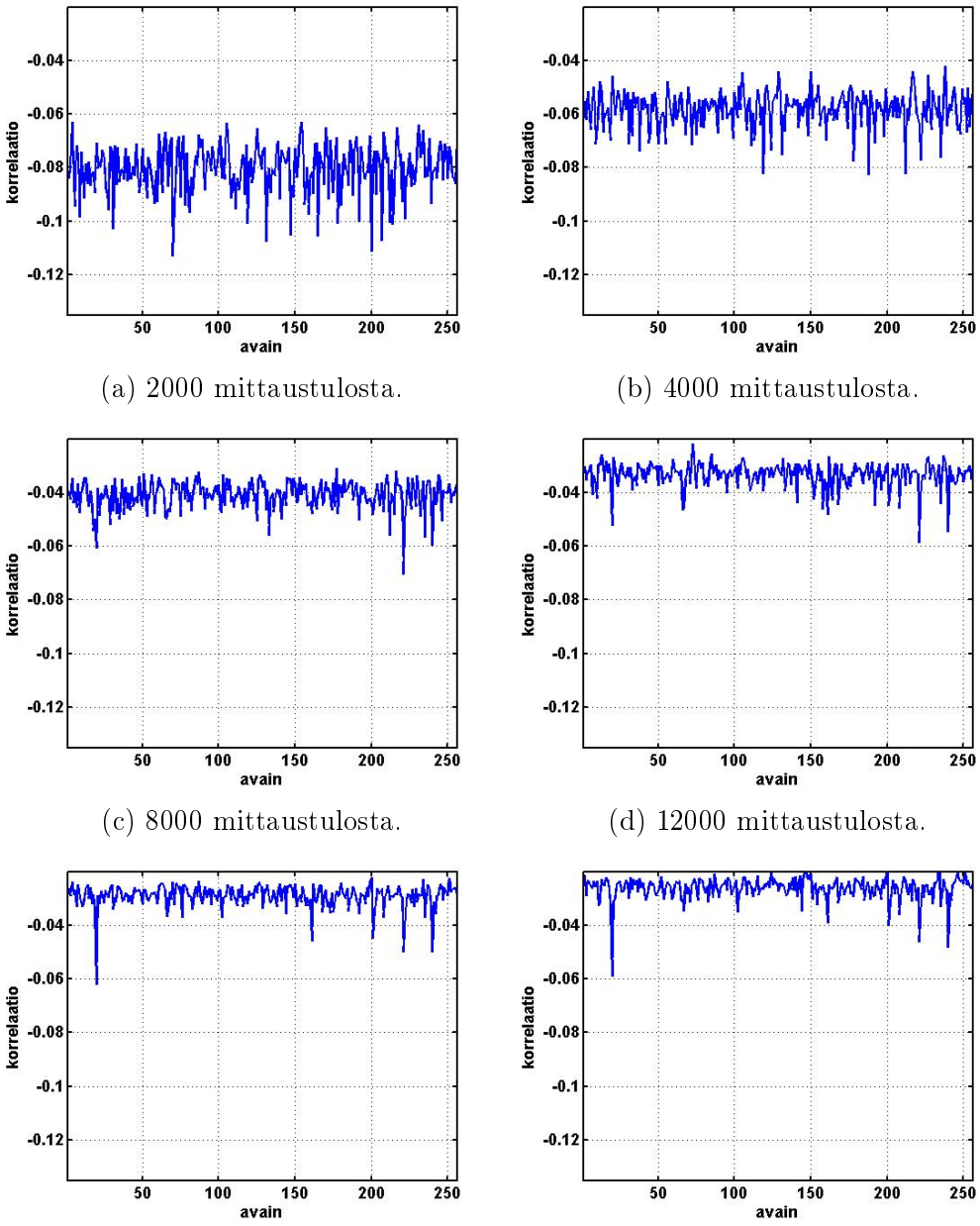
(f) 20000 mittaustulosta.

Kuva 33: Korrellaatio oikealla avainarvauksella ensimmäisellä Hammingin etäisyydellä.

lin tuottamien tehonkulutusarvioiden kanssa.

Oikean avainarvauksen löytämiseksi kaikkien avainarvausten korrelaatioita verrataan toisiinsa. Jokaisella avainarvauksella lasketusta korrelaatiotuloksesta valitaan itseisarvoltaan suurin korrelaatiokerroin. Avainarvausten tuottamat suurimmat itseisarvot eri mittausmäärillä nähdään kuvassa 33.

Toinen hyökkäys Sakura-G:tä vastaan suoritettiin laskemalla Hammingin etäisyys väliarvosta ennen viimeistä tavujenkorvausoperaatiota väliarvoon sen jälkeen.



(a) 2000 mittaustulosta.

(b) 4000 mittaustulosta.

(c) 8000 mittaustulosta.

(d) 12000 mittaustulosta.

(e) 16000 mittaustulosta.

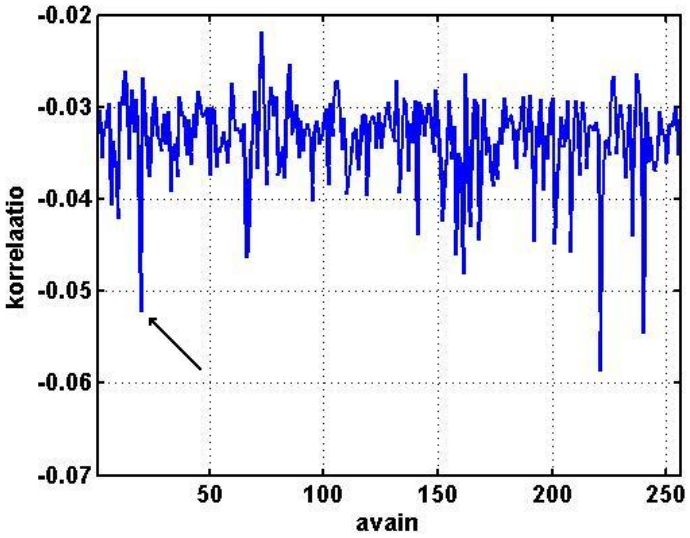
(f) 20000 mittaustulosta.

Kuva 34: Parhaat korrelaatiot jokaisella avainarvauksella Hammingin etäisyydellä tavujenkorvausoperaation yli.

Tällaista tilanvaihtoa ei havaittu laitteistonkuvauskielisten toteutuksien simulointien aikana mutta sen arvioitiin olevan potentiaalinen hyökkäyskohde. Kuvassa 34 nähdään avainarvausten itseisarvoltaan suurimmat korrelaatiokertoimet eri mittaustulosmäärillä.

Kuvassa 35 kuvan 34d näkyvää korrelaatioakselia on supistettu. Kuvasta 35 nähdään, että nuolella merkityn oikean avainarvauksen aiheuttama piikki ei ole suurin.

Kuvasta 34e nähdään suurimman korrelaatiopiikin muodostuvan oikealla avai-



Kuva 35: Parhaat korrelaatiot jokaisella avainarvauksella toisella Hammingin etäisyydellä 12000 mittaustuloksella.

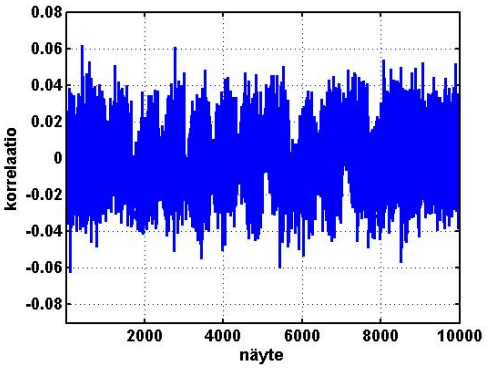
narvauksella kun käytetään 16000 tehonkulutusmittausta. Tarvittava määrä mittaustuloksia oikean avainarvauksen tunnistamiseen on suurempi kuin ensimmäisellä Hammingin etäisyydellä.

Kuvassa 36 nähdään oikealla avainarvauksella lasketut korrelaatiot ajan suhteen eri mittaustulosmäärillä kun ollaan käytetty Hammingin etäisyyttä tavujenkorvausoperaation yli. Korrelaatiopiikki on nähtävissä 8000 mittaustuloksella.

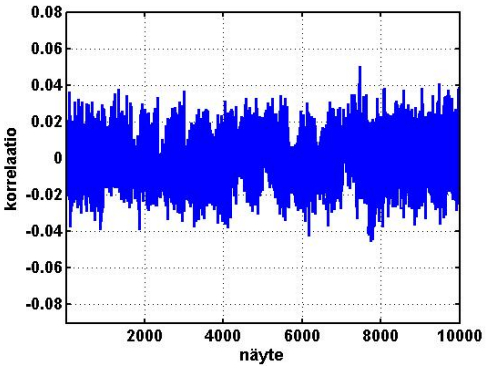
Kuvassa 37 nähdään väärällä avainarvauksella muodostunut korrelaatio ajan suhteen kahdella mittaustulosmäärällä. Korrelaatiopiikki vaimenee käytettäessä enemmän mittauksia. Kuvassa 34c nähdään väärän arvauksen aiheuttama suurin korrelaatiopiikki käytettäessä 8000 mittaustulosta. Kuvassa 34f väärän arvauksen aiheuttama piikki on pienentynyt suhteessa oikean arvauksen piikkiin, eikä se ole suurin. Kuvia 37a, 37b, 36c ja 36d vertailemalla nähdään, että lisättäessä mittaustulosten määrää väärän avainarvauksen piikki vaimenee, mutta oikean arvauksen piikki säilyy ennallaan.

Kolmas hyökkäys Sakura-G:tä vastaan tehtiin Hammingin painolla laskettuja arvioituja tehonkulutuksia käyttäen. Hammingin paino laskettiin viimeisen tavujenkorvausoperaation tuloksesta. Kuvassa 38 nähdään korrelaatio ajan suhteen oikealla avainarvauksella eri mittaustulosmäärillä. Korrelaatiopiikki muodostuu ajanhetkellä jolloin viimeistä AES-kierrosta suoritetaan. Korrelaatiopiikki voidaan havaita kun käytetään 20000 mittausta. 30000 mittaustuloksella korrelaatiopiikki erottuu hyvin. 50000 mittaustuloksella oikealla avainarvauksella muodostunut korrelaatiopiikki on vaimentunut.

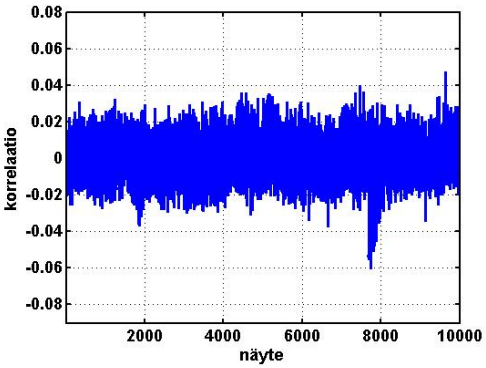
Hammingin painoa käytettäessä kerätyllä mittaustulosmäärällä oikean avainarvauksen korrelaatiopiikki ei ole suurin. Haamupiikkejä muodostui useilla väärillä avainarvauksilla. Muista piikeistä erottuvaa korrelaatiopiikkiä ei havaittu.



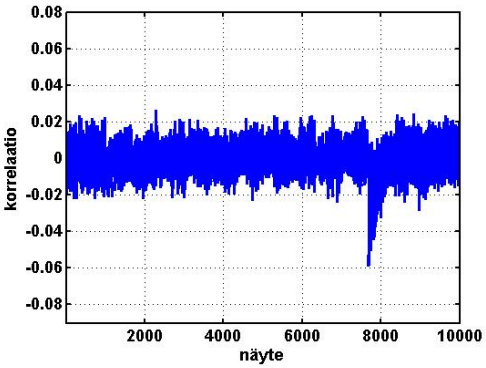
(a) 3000 mittaustulosta.



(b) 5000 mittaustulosta

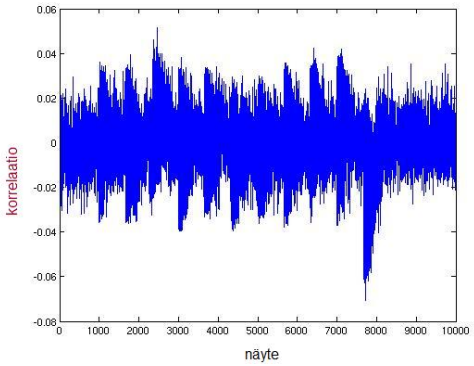


(c) 8000 mittaustulosta.

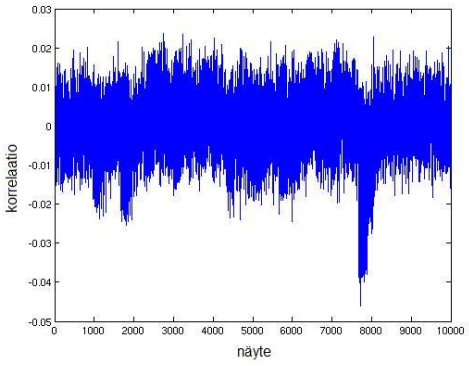


(d) 20000 mittaustulosta.

Kuva 36: Korrelaatio ajan suhteen oikealla avainarvauksella toisella Hammingin etäisyydellä.

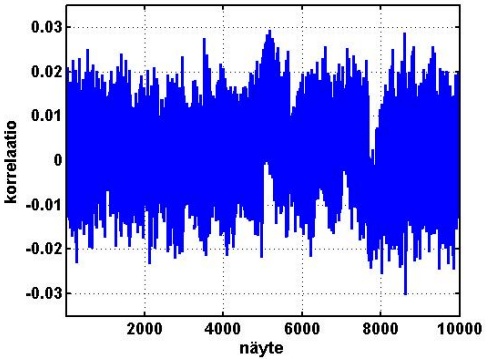


(a) 8000 mittaustulosta.

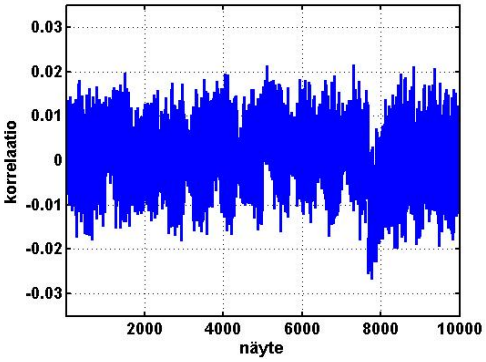


(b) 20000 mittaustulosta.

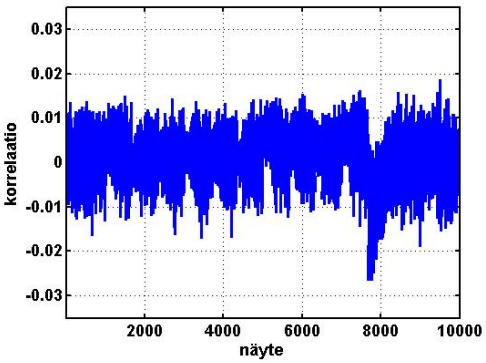
Kuva 37: Korrelaatiopiikki väärällä avainarvauksella.



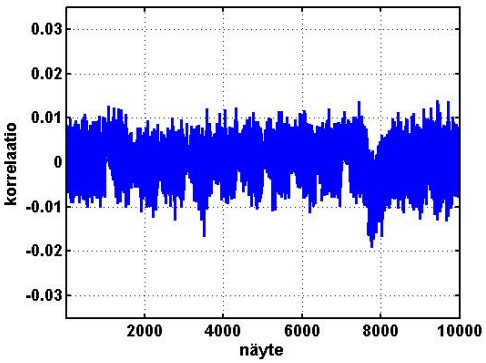
(a) 15000 mittaustulosta.



(b) 20000 mittaustulosta.

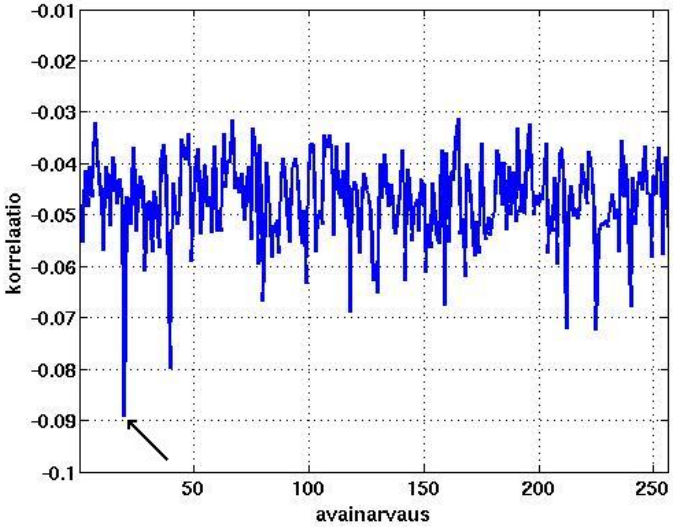


(c) 30000 mittaustulosta.



(d) 50000 mittaustulosta.

Kuva 38: Korrelaatio ajan suhteen oikealla avainarvauksella käytettäessä Hammingin painoa.



Kuva 39: Paras korrelaatio kaikilla avainarvauksilla 4000 mittaustuloksella käytettäessä ensimmäistä Hammingin etäisyyttä tehonkulutusmallina.

4.4.2 Toteutettu salauslaite

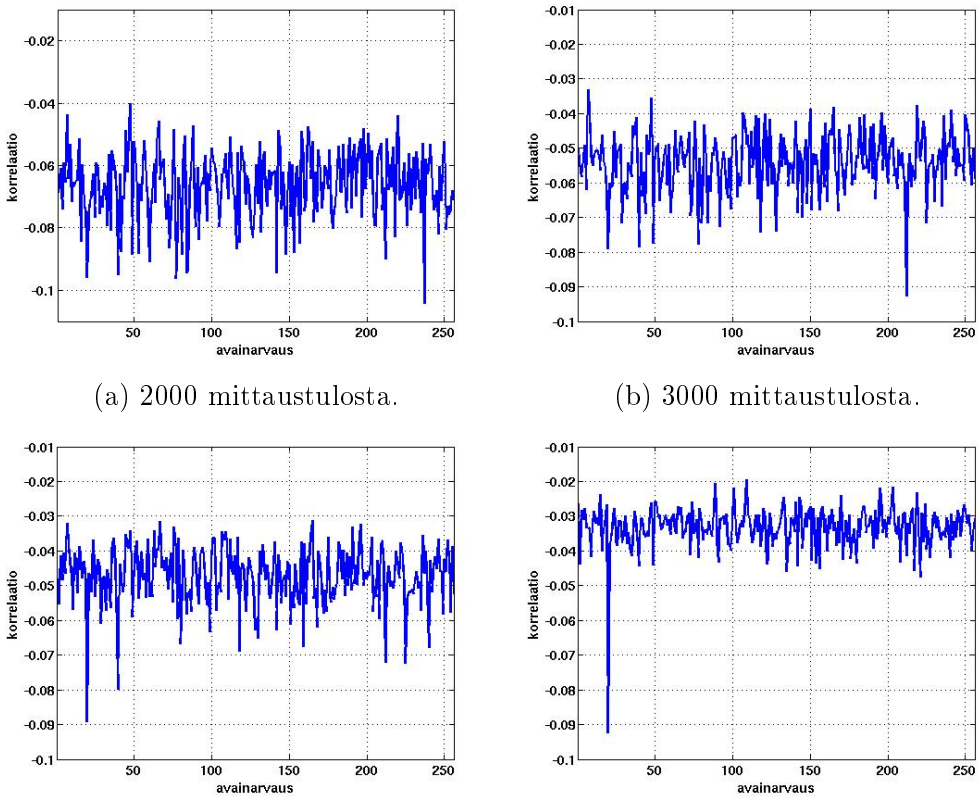
Toteutetussa FPGA-salauslaitteessa käytettiin kolmea AES-toteutusta. Salauslaitteen salausavaimeksi asetettiin 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F. Viimeisen AES-kierroksen kierrosavain on 13 11 1D 7F E3 94 4A 17 F3 07 A7 8B 4D 2B 30 C5. Toteutetun salauslaitteen AES-toteutuksia vastaan suoritettiin samat hyökkäykset kuin Sakura-G:tä vastaan. Hyökkäys suoritettiin viimeisen kierrosavaimen ensimmäistä tavua vastaan. Hyökkäys voidaan toistaa salausavaimen muita tavuja vastaan koko kierrosavaimen selvittämiseksi.

Katashitan AES-toteutusta vastaan hyökättiin ensimmäiseksi. Tehonkulutusmittauksia kerättiin 10000. Ensimmäisessä hyökkäyksessä tehonkulutusmallina käytetään kuvan 27 ensimmäistä Hammingin etäisyyttä. Kuvassa 39 nähdään suurimman korrelaatiopiikin muodostuvan oikealla avainarvauksella. Oikea avainarvaus on merkitty nuolella. Kuvasta 40 nähdään mittaustulosten määrän lisäämisen vaikutus kaikkien avainarvausten itseisarvoltaan suurimpaan korrelaatioketoimeen.

Kuvassa 40b nähdään väärällä avainarvauksella muodostunut korrelaatiopiikki. Haamupiikki vaimenee mittaustuloksia lisäämällä.

Kuvista 23 ja 41d nähdään korrelaatiopiikin muodostuvan viimeistä AES-kierrosta suoritettaessa. Kuvassa 41 nähdään korrelaatio ajan suhteen oikealla avainarvauksella eri mittausmäärillä.

Toteutettua salauslaitetta Katashitan AES-toteutuksella vastaan hyökättiin myös toista kuvan 27 Hammingin etäisyyttä ja viimeisen tavujenkorvausoperaation tuloksen Hammingin painoa käyttäen. Toisella Hammingin etäisyydellä korrelaatiopiikki muodostui käytettäessä oikeaa avainarvausta. Kerätyllä mittaustulosmäärällä oikean avainarvauksen korrelaatiopiikki ei ole suurin verrattuna muihin avainarvauksiin. Hammingin painoa tehonkulutusmallina käytettäessä korrelaatiopiikkiä ei havaittu



(a) 2000 mittaustulosta.

(b) 3000 mittaustulosta.

(c) 4000 mittaustulosta.

(d) 8000 mittaustulosta.

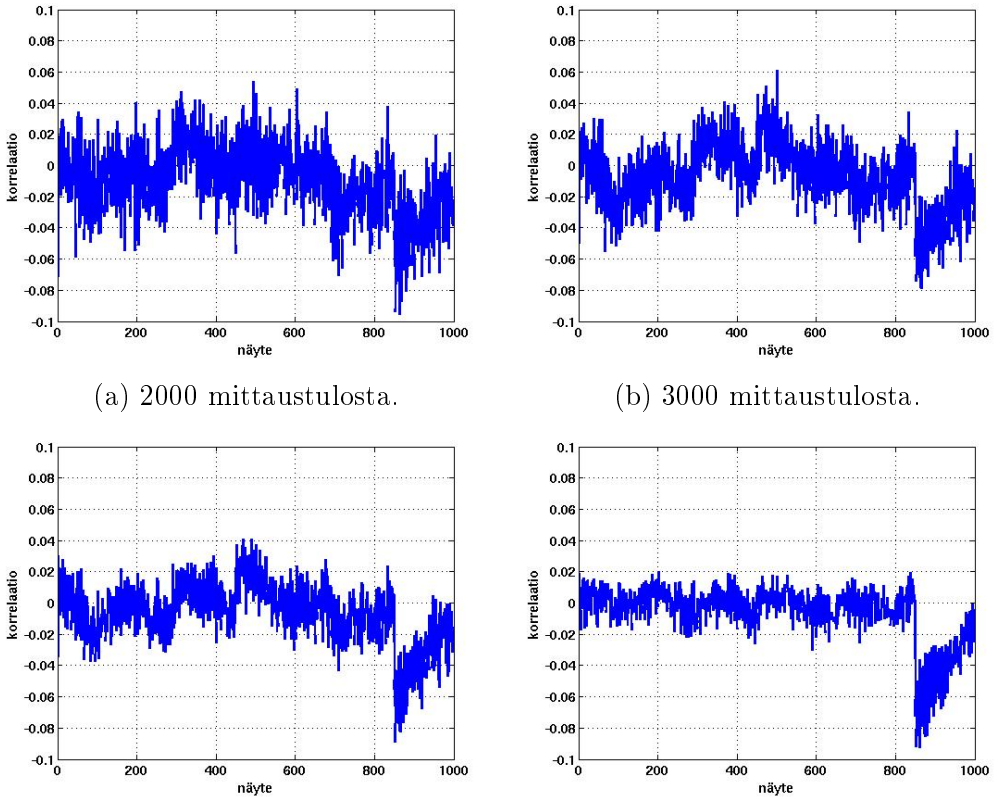
Kuva 40: Paras korrelaatio kaikilla avainarvauksilla käytettäessä ensimmäistä Hammingin etäisyyttä tehonkulutusmallina.

oikealla avainarvauksella.

Kaikkia hyökkäyksiä kokeiltiin molempia opencores.com sivustolta ladattuja AES-toteutuksia vastaan. Korrelaatiopiikkejä ei havaittu kerätyillä mittaustulosmäärillä. De La Piedran AES-toteutusta vastaan hyökättiin 100000 mittaustuloksella. Usselmannin AES-toteutusta vastaan hyökättiin 10000 mittaustuloksella. Taulukkoon 4 on koottu kerätyt mittausmäärät ja oikealla avainarvauksella havaittu korrelaatio.

Taulukko 4: Korrelaatio oikealla avainarvauksella. Suuri tarkoittaa onnistunutta hyökkäystä. Pieni tarkoittaa, että korrelaatiota oli havaittavissa oikealla avainarvauksella mutta hyökkäys ei onnistunut. Ei tarkoittaa, että millään avainarvauksella ei muodostunut havaittavaa korrelaatiopiikkiä.

	Sakura-G	**Katashita**	**De La Piedra**	**Usselmann**
Mittaustuloksia	50000	10000	100000	10000
1. hammingin etäisyys	Suuri	Suuri	Ei	Ei
2. hammingin etäisyys	Suuri	Pieni	Ei	Ei
Hammingin paino	Pieni	Ei	Ei	Ei



(a) 2000 mittaustulosta.

(b) 3000 mittaustulosta.

(c) 4000 mittaustulosta.

(d) 8000 mittaustulosta.

Kuva 41: Korrelaatio ajan suhteen oikealla avainarvauksella käytettäessä ensimmäistä Hammingin etäisyyttä tehonkulutusmallina.

4.5 Havainnot mittaus- ja analyysituloksista

Alaluvussa 4.4 esitettyjen korrelaatioanalyysitulosten perusteella voidaan todeta, että oikealla avainarvauksella lasketulla arvioiduilla tehonkulutuksilla on lineaarinen yhteys mitattujen tehonkulutukseen verrannollisten jännitteiden kanssa. Salauslaitteen on AES-algoritmin mukaan tuotettava oikealla avainarvauksella lasketut välitulokset. Salauslaite ei tuota väärillä avainarvauksilla laskettuja välituloksia, joten väärillä avainarvauksilla lasketuilla arvioiduilla tehonkulutuksilla ja mitatuilla tehonkulutuksilla ei ole lineaarista yhteyttä.

Alaluvussa 4.4 esitettyistä kuvista nähdään, että mitä enemmän mittauksia ja salattuja lohkoja käytetään, sitä selkeämmin oikea avainarvaus erottuu vääristä avainarvauksista. Oikean arvauksen aiheuttama korrelaatiopiikki lähestyy nollasta poikkeavaa raja-arvoa ja väärien avainarvausten aiheuttama korrelaatio lähestyy nollaa käytettävän mittausmäärän kasvaessa. Hyökkääjän täytyy valita luottamustaso, jonka perusteella oikea avainarvaus tulkitaan tunnistetuksi.

Oikean avainarvauksen aiheuttaman korrelaatiopiikin lisäksi väärillä avainarvauksilla voi syntyä haamupiikkejä. Haamupiikit ovat korrelaatiopiikkejä jotka ovat syntyneet kohinan tai epätarkan tehonkulutusmallin seurauksena. Haamupiikkejä ei voida erottaa oikealla avainarvauksella syntyneestä korrelaatiopiikistä. Suuril-

la mittausmäärillä kohinasta aiheutuneet haamupiikit vaimenevat. Riippuen AES-toteutuksesta, salauslaitteesta, mittausjärjestelyistä ja analyysimenetelmistä mittaustulosmäärä joka vaaditaan haamupiikkien vaimenemiseen voi olla kymmeniä miljoonia. Epätarkan tehonkulutusmallin seurauksena syntyneet haamupiikit eivät välttämättä vaimene. Jos itseisarvoltaan suuria korrelaatiopiikkejä muodostuu useita, oikeaa avainarvausta ei voida yksiselitteisesti tunnistaa.

Jos kerätyllä mittausmäärällä syntyy useita korrelaatiopiikkejä, ei salausavainta saada suoraan selville. Voidaan kuitenkin suorittaa brute force-hyökkäys supistetulla salausavainjoukolla. Supistettuun salausavainjoukkoon valitaan ne salausavaimet jotka voidaan muodostaa suurimpien korrelaatiopiikkien perusteella.

Katashitan AES-toteutuksessa yhden AES-kierroksen suorittaminen kestää 16 kellojaksoa. Kierros voitaisiin suorittaa yhdessä kellojaksossa, mutta viiveen lisääminen parantaa tehonkulutussignaalin ja kohinan suhdetta. Viive on mahdollisesti lisätty toteutukseen haavoittuvuuden esittelemiseksi. Toisissa AES-toteutuksissa viivettä ei ole lisätty ja signaalin ja kohinan suhde on pienempi kuin Katashitan AES-toteutuksessa. Katashitan AES-toteutus on erityisen haavoittuvainen DPA-hyökkäykselle.

Esitettyjen korrelaatioanalyysien perusteella kohinan vaikutusta voidaan vähentää lisäämällä tehonkulutusmittausten määrää. Suuremmilla tehonkulutusmittausmäärillä De La Piedran ja Usselmannin AES-toteutukset ovat mahdollisesti murrettavissa. Kokeillut tehonkulutusmallit saattoivat kuvata toteutusten tehonkulutusta huonosti ja paremmalla tehonkulutusmallilla hyökkäys saattaisi onnistua kerätyillä tehonkulutukseen verrannollisilla jännitemittauksilla.

De La Piedran AES-toteutuksessa signaalin ja kohinan suhdetta heikentää lisäksi varsinaisen salauksen rinnalla suoritettava toinen salaus. Toisen salauksen tuottamia salattuja lohkoja ei voida hyödyntää hyökkäyksessä. Toteutuksen tuottamat välitulokset tallennetaan siten, että rekisterien peräkkäisiä arvoja ei voida laskea käytettävissä olevalla tiedolla. Tällainen toteutus saattaa olla vastustuskykyinen Hammingin etäisyyksillä suoritettavia hyökkäyksiä vastaan ja hyökkäys ei välttämättä onnistu edes suurilla tehonkulutusmittausmäärillä. Hammingin painoa käytettäessä ei tarvita tietoa peräkkäisistä rekisterien arvoista. Hammingin painolla hyökkäys saattaa onnistua, jos käytettävissä on paljon tehonkulutusmittauksia.

Usselmannin AES-toteutuksessa ei suoriteta ylimääräisiä operaatioita ja rekisterien peräkkäisiä arvoja voidaan laskea käytettävissä olevalla tiedolla. Simulaatioista tunnistetut laskettavissa olevat siirtymät vaativat toiseksi viimeisen kierroksen välitulosten laskentaa. Toiseksi viimeisen kierroksen välitulosten käyttäminen kasvattaa hyökkäykseen kuluvaa aikaa, mutta on nopeampi suorittaa kuin brute force-hyökkäys.

Alaluvun 4.2 kuvista havaittiin, että De La Piedran ja Usselmannin AES-toteutusten aiheuttamat jännitteen muutokset mittausvastuksen yli olivat noin kymmenyksen Katashitan AES-toteutuksesta. Yksittäisten tilanvaihdosten aiheuttamat tehonkulutukset ovat mahdollisesti samalla tavalla verrannollisia. Jos kohinan oletetaan olevan samaa suuruusluokkaa kaikilla toteutuksilla ja signaali-kohinasuhteen heikentymisen vaikuttavan tarvittavien mittaustulosten määrään lineaarisesti, tehonkulutusmittauksia tarvittaisiin De La Piedran ja Usselmannin AES-toteutuksia vastaan

noin 30000. Signaali-kohinasuhteen ja tarvittavien mittaustulosten määrän suhde ei välttämättä ole lineaarinen.

Heikon signaali-kohinasuhteen vuoksi korrelaatiopiikin havaitsemiseen tarvittava tehonkulutusmittausmäärä voi olla suuri. Tehonkulutusmittausten määrän kasvattaminen lisää hyökkäykseen kuluvaa aikaa. Jos tarvittava tehonkulutusmittausmäärä on esimerkiksi kymmeniä miljoonia, voi hyökkäykseen kuluva aika kasvaa epäkäytännöllisen suureksi.

Käytettävissä olevien tehonkulutusmittausten määrä voi olla rajallinen. Käytännöllisessä hyökkäyksessä salauslaitteen tehonkulutusta voidaan mitata rajallinen aika. Salauslaite saattaa tuottaa salattuja lohkoja epäsäännöllisesti tai hitaasti. Tarvittavan tehonkulutusmittausmäärän kerääminen voi kestää epäkäytännöllisen kauan.

Tehonkulutusmittauksiin kuluva aika riippuu pääosin salauslaitteen nopeudesta. Mittauslaitteiston täytyy olla riittävän nopea mittausten onnistumiseksi. Hyökkäyksen kannalta ei ole merkitystä onko salatut lohkot kerätty järjestyksessä, kunhan jokainen tehonkulutukseen verrannollinen jännitemittaus ja salattu lohko vastaavat toisiaan. Voidaan kerätä esimerkiksi vain joka toinen saluslaitteen lähettämä salattu lohko, mutta tämä hidastaa keräystä. Tulosten laskemiseen kuluva aika riippuu tietokoneen nopeudesta, tehonkulutusmittausten määrästä ja laskennan suorittavan ohjelman tehokkuudesta.

Tässä työssä käytetyllä hyökkäysjärjestelyllä Katashitan AES-toteutuksen oikea salausavain saatiin selville noin viidessä tunnissa. Suuri osa ajasta kului tehonkulutusmittausten suorittamiseen, koska salauslaitteen toimintaa hidastettiin viivästämällä sille lähetettäviä salaamattomia lohkoja. 4000 tehonkulutusmittauksella laskentaan kului noin kaksi tuntia. Laskentaan kuluvaa aikaa voidaan vähentää kohdistamalla laskenta viimeiseen AES-kierrokseen, jos hetki jolloin viimeistä kierrosta suoritetaan on tiedossa. Havainnollistamisen vuoksi tässä työssä korrelaatio laskettiin jokaiselle mitatulle näytteelle.

Mittausjärjestelyjä kehittämällä mittaukset voidaan suorittaa niin nopeasti kuin salauslaite suorittaa salausta. Hyökkäystulosten laskentaa voidaan nopeuttaa käyttämällä tehokkaammalla ohjelmaa, jolloin tulosten laskenta 4000 tehonkulutusmittauksella kestää muutamia minuutteja.

5 Yhteenveto

Tässä työssä esiteltiin differentiaalinen tehoanalyysihyökkäys AES-salausalgoritmia vastaan. Differentiaalinen tehoanalyysihyökkäys on sivukanavahyökkäys, joka käyttää hyväkseen elektronisen salauslaitteen tehonkulutuksen vuotamaa tietoa laitteen toiminnastaa. Tehonkulutuksen vuotaman tiedon avulla voidaan selvittää laitteen käyttämä salausavain.

Differentiaalisen tehoanalyysihyökkäyksen suorittamiseksi mitataan salauslaitteen tehonkulutukseen verrannollista jännitettä sen suorittaessa salausoperaatioita ja kerätään salauslaitteen salaamaa tietoa tiedonsiirtokanavasta. Salatun tiedon ja avainarvausten avulla voidaan laskea salauslaitteen mahdollisesti tuottamia AES-välituloksia. Avainarvaus tehdään viimeisen kierrosavaimen osasta.

AES-salauksessa tavun kokoisella avainarvauksella voidaan laskea tavun kokoinen osa jokaisesta viimeisen AES-kierroksen välituloksesta. Jos hyökkäyksessä käytetään muita kuin viimeisen kierroksen välituloksia hyökkäykseen kuluva aika kasvaa merkittävästi, sillä tarvitaan arvaus myös toiseksi viimeisestä kierrosavaimesta.

Välitulosten avulla voidaan arvioida salauslaitteen kuluttamaa tehoa. Tehonkulutuksen arviointi kohdistuu pieneen osaan laitteen kokonaistehonkulutusta. Tehonkulutus arvioidaan kahden AES-välituloksen Hammingin etäisyydellä tai yhden välituloksen Hammingin painolla.

Oikea avainarvaus voidaan tunnistaa korrelaatiopiikin perusteella. Korrelaatiopiikki syntyy jos arvioitu tehonkulutus ja mitattu tehonkulutus korreloivat keskenään. Hyökkäys kohdistetaan kerrallaan tavun suuruiseen osaan viimeisen kierroksen kierrosavainta. Tavun suuruisen osan kaikkien mahdollisuuksien läpikäymiseen vaaditaan 2^8 eli 256 avainarvausta. Tehonkulutus arvioidaan ja korrelaatio mitattuun tehonkulutukseen verrattavissa olevaan jännitteeseen lasketaan jokaisella avainarvauksella. Korrelaatiotuloksia verrataan toisiinsa ja itseisarvoltaan suurimman korrelaatiopiikin tuottaneen avainarvauksen arvioidaan olevan laitteen käyttämä kierrosavaimen osa.

Tässä työssä suoritettiin differentiaalinen tehoanalyysihyökkäys kahta elektronista salauslaitetta vastaan. Kummankin salauslaitteen käyttämät salausavaimet saatiin selvitettyä kun käytettiin Toshihiro Katashitan AES-toteutusta.

Toinen salauslaite ohjelmoitiin käyttämään Katashitan AES-toteutuksen lisäksi Antonio De La Piedran ja Rudolf Usselmannin AES-toteutuksia. De La Piedran ja Usselmannin AES-toteutuksia käytettäessä salausavainta ei saatu selvitettyä. Toteutuksissa voi olla ominaisuuksia jotka vaikeuttavat differentiaalisen tehoanalyysihyökkäyksen suorittamista. Esimerkiksi pieni signaali-kohinasuhde tai joidenkin operaatioiden toteuttaminen epäsynkronisesti voi vaikeuttaa hyökkäystä.

AES on matemaattisesti turvallinen salausalgoritmi. Se on vastustuskykyinen tavanomaisia hyökkäysmenetelmiä vastaan joissa analysoidaan salaamattomia ja salattuja lohkoja. AES-algoritmissa on heikkouksia, joita voidaan hyödyntää differentiaalisessa tehoanalyysihyökkäyksessä. AES-salausta vastaan hyökätessä riittää yhden kierrosavaimen selvittäminen. Salausavain voidaan laskea käänteisen avaimenlaajennusoperaation avulla. AES ei käytä sarakkeidensekoitusoperaatiota viimeisellä kierroksella. Tavun kokoinen osa viimeisen kierroksen välituloksista voidaan laskea

tavun kokoisella osalla viimeisestä kierrosavaimesta. Hyökkäys voidaan kohdistaa pieneen osaan avainta, mikä vähentää laskentaan kuluvaa aikaa. AES-salauksen tavujenkorvaus on hyvin epälineaarinen ja sen seurauksena väärillä avainarvauksilla lasketut arvioidut tehonkulutukset eivät ole lineaarisesti verrannollisia varsinaiseen tehonkulutukseen.

Differentiaalinen tehoanalyysihyökkäys ei vaadi erikoislaitteita. Hyökkäyksen suorittamiseen tarvitaan tietokone ja oskilloskooppi. Oskilloskoopin täytyy olla riittävän nopea, tarkka ja mittaustulokset täytyy voida tallentaa. Useimmat modernit oskilloskoopit täyttävät vaatimukset. Tavallisen kannettavan tietokoneen laskentateho riittää DPA-hyökkäyksen laskentaan, jos kohde on haavoittuvainen hyökkäykselle.

Koska differentiaalinen tehoanalyysihyökkäys ei vaadi kalliita erikoislaitteita ja se on nopea suorittaa on sen uhka merkittävä. Tarvittavat laitteet ovat yhden henkilön kannettavissa. Tarvittavan tiedon kerääminen ja tulosten laskenta voidaan suorittaa erikseen. Kun tarvittava tieto on kerätty sitä voidaan analysoida rauhassa. Riittävä määrä tietoa voidaan joissain tapauksissa kerätä minuuteissa. Hyökkäys voidaan useissa tilanteissa suorittaa vahingoittamatta salauslaitetta, jolloin hyökkäystä ei välttämättä voida havaita.

Suoritettujen hyökkäysten perusteella kaikki toteutukset eivät ole yhtä haavoittuvaisia hyökkäykselle. Differentiaalista tehoanalyysihyökkäystä voidaan hidastaa pienentämällä signaali-kohinasuhdetta. Kaikki AES-laskentaan liittymätön toiminta laitteessa lisää kohinaa hyökkäyksen kannalta. Differentiaaliselle tehoanalyysihyökkäykselle ollaan kohinan lisäämisen lisäksi kehitetty myös muita suojaustekniikoita. [6]

Erityisiä suojaustekniikoita on syytä käyttää jos salauslaite sijaitsee sellaisessa paikassa jossa ulkopuolinen taho saattaa päästä mittaamaan sivukanavatietoa. Tehonkulutus ei ole ainoa sivukanavatieto jota voidaan käyttää hyväksi. Tehonkulutuksen lisäksi sivukanavatietoa voidaan kerätä esimerkiksi operaatioiden ajasta, sähkömagneettisesta säteilystä ja äänestä. Differentiaalinen tehoanalyysihyökkäys ei ole uhka, jos ulkopuolisella taholla ei ole mahdollisuutta suorittaa tarvittavia mittauksia.

Useissa tilanteissa riittää, että tieto säilyy salaisena tietyn ajan. AES-toteutuksen ja salauslaitteen ominaisuuksien välinnalla voidaan hidastaa DPA-hyökkäystä. Vastustuskykyiset AES-toteutukset voivat hidastaa salauslaitteen toimintaa sekä kuluttaa enemmän tehoa ja pinta-alaa piiriltä. Tarvittava suojauksen taso täytyy arvioida käyttötarkoituksen mukaan. On tärkeää tietää, että salauslaite jossa differentiaalista tehoanalyysihyökkäystä ei olla otettu huomioon, saattaa olla murrettavissa minuuteissa.

Viitteet

[1] Kocher, P., Jaffe, J., Jun, B. *Differential Power Analysis.* Advances in Cryptology - Proceedings of Crypto '99, Lecture Notes in Computer Science, Vol. 1666. Springer-Verlag. 1999. ISBN 3-540-66347-9 s.388-397.

[2] Cryptography Research. *http://www.cryptography.com/company/about.html*

[3] Daemen, J., Rijmen, V. *The Design of Rijndael: AES- The Advanced Encryption Standard.* Berlin. Springer. 2002. ISBN 3-540-42580-2. 236 s.

[4] Stinson, D. *Cryptography : theory and practice.* Boca Raton. Chapman and Hall/CRC. 2002. ISBN 1-58488-206-9. 339 s.

[5] Milton, J. S. *Introduction To Probability And Statistics:Principles and Applications for Engineering and the computing sciences.* 4. painos. New York, McGraw-Hill, 2003. ISBN 978-0-07-119859-2. 832 s.

[6] Mangard, S., Oswald, E., Popp, T. *Power Analysis Attacks: Revealing the Secrets of Smart Cards.* New York, Springer, 2007. ISBN 978-0-387-30857-9. 337 s.

[7] Stallings, W. *Cryptography and Network Security: Principles and Practices.* New Jersey. Pearson Prentice Hall. 2006. ISBN 0-13-187316-4. 680 s.

[8] Brown, S., Vranesic, Z. *Fundamentals of Digital Logic with VHDL Design.* 2. painos. New York, McGraw-Hill, 2005. ISBN 0-07-124482-4. 939 s.

[9] Koskinen, L. *Desimointi- ja kanavansuodatin radiovastaanottimeen.* Diplomityö. 1999. Teknillinen korkeakoulu, Sähkö- ja tietoliikennetekniikan osasto. 65 s.

[10] Biryukov, A., Dunkelman O., Keller N., Khovratovich D., Shamir A. *Key Recovery Attacks of Practical Complexity on AES-256 Variants with up to 10 Rounds.* Advances in Cryptology EUROCRYPT 2010. 2010. ISBN 978-3-642-13189-9. s. 299-319.

[11] MORITA TECH. *SAKURA-G Specification Ver. 1.0.* http://satoh.cs.uec.ac.jp/SAKURA/hardware/SAKURA-G_Spec_Ver1.0_English.pdf

[12] Maxim Integrated. *DS1088L Fixed-Frequency EconOscillator Datasheet.* http://datasheets.maximintegrated.com/en/ds/DS1088-DS1088L.pdf

[13] Pan, J., Van Woudenberg, J., Den Hartog, J., Witteman, M. *Improving DPA by peak distribution analysis.* SAC'10 Proceedings of the 17th international conference on Selected areas in cryptography. 2011. ISBN: 978-3-642-19573-0. s. 241-261.

[14] De La Piedra, A. *http://opencores.org/project,threeaesc*

[15] Usselmann, R. *http://opencores.org/project,aes_core*

A Esimerkki AES-salausalgoritmin toiminnasta

Tässä liitteessä esitellään esimerkkien avulla AES-algoritmin toimintaa. Algoritmin ensimmäinen kierros ja ensimmäisen kierrosavaimen luominen esitetään yksityiskohtaisesti.

Esimerkissä käytettävä salausavain on heksadesimaalilukuina esitettynä 00 10 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F. Avaimen pituus on 128 bittiä. AES voi käyttää myös 192 ja 256 bitin mittaisia avaimia, mutta näitä tapauksia ei käsitellä tässä liitteessä. Esimerkissä käytettävä salattava lohko on 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00. AES-lohkon pituus on 128 bittiä riippumatta avaimen pituudesta.

A.1 Laskutoimitukset Galois field 2^8 kentässä

AES-käyttää laskutoimituksissa Galois field 2^8 kenttää. Käytettävässä kentässä summaukset ovat XOR-operaatioita eli eksklusiivisia tai-operaatioita. XOR on bittioperaatio jonka totuustaulu näkyy kuvassa 42.

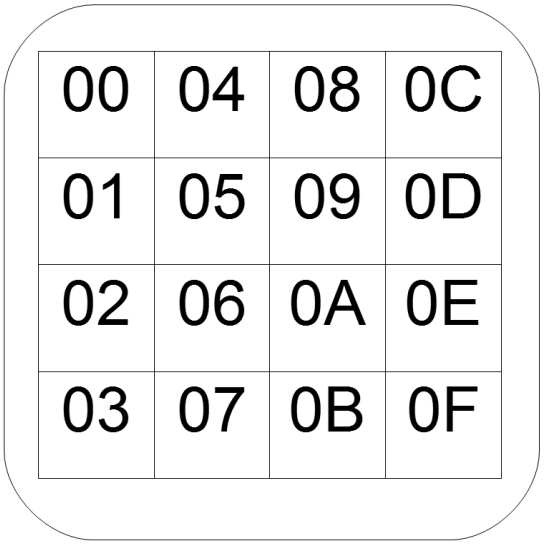
XOR	0	1
0	0	1
1	1	0

Kuva 42: XOR-operaation totuustaulu.

Ennen ensimmäisen kierroksen alkua AES suorittaa summauksen salattavan lohkon ja salausavaimen kesken. Avaimensummauksen eli XOR-operaation jälkeinen AES-välitulos on 00 10 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F. AES-välitulokset järjestetään kuvassa 43 nähtävällä tavalla.

A.2 Avaimenlaajennus

AES-kierrokset käyttävät salausavaimen avulla luotuja kierrosavaimia. Kierrosavaimet luodaan avaimenlaajennus-operaatiolla, jonka lopputulosta kutsutaan laajenne-



Kuva 43: Esimerkkilohkon ensimmäinen välitulos.

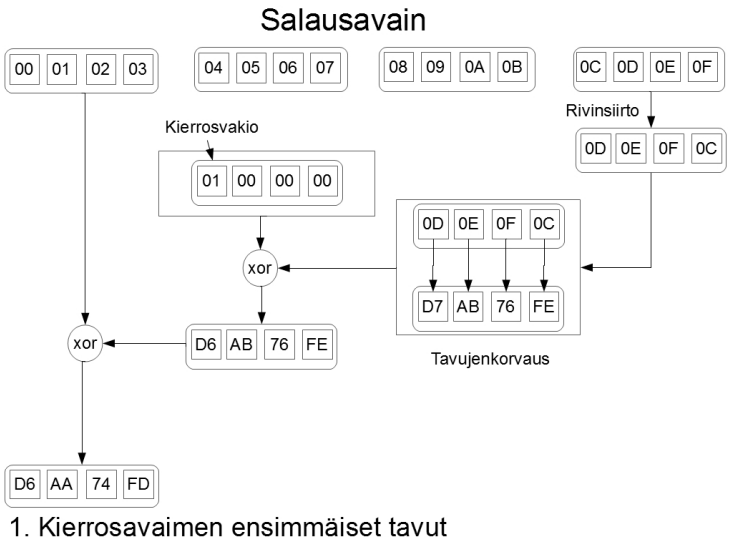
tuksi avaimeksi. Esimerkin salausavaimella luotu laajennettu avain näkyy kuvassa 44

```
AVAIN:       00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
KIERROS 1:  D6 AA 74 FD D2 AF 72 FA DA A6 78 F1 D6 AB 76 FE
KIERROS 2:  B6 92 CF 0B 64 3D BD F1 BE 9B C5 00 68 30 B3 FE
KIERROS 3:  B6 FF 74 4E D2 C2 C9 BF 6C 59 0C BF 04 69 BF 41
KIERROS 4:  47 F7 F7 BC 95 35 3E 03 F9 6C 32 BC FD 05 8D FD
KIERROS 5:  3C AA A3 E8 A9 9F 9D EB 50 F3 AF 57 AD F6 22 AA
KIERROS 6:  5E 39 0F 7D F7 A6 92 96 A7 55 3D C1 0A A3 1F 6B
KIERROS 7:  14 F9 70 1A E3 5F E2 8C 44 0A DF 4D 4E A9 C0 26
KIERROS 8:  47 43 87 35 A4 1C 65 B9 E0 16 BA F4 AE BF 7A D2
KIERROS 9:  54 99 32 D1 F0 85 57 68 10 93 ED 9C BE 2C 97 4E
KIERROS 10: 13 11 1D 7F E3 94 4A 17 F3 07 A7 8B 4D 2B 30 C5
```

Kuva 44: Laajennettu avain.

Ensimmäisen kierrosavaimen ensimmäiset tavut luodaan kuvan 45 mukaisesti salausavaimen ensimmäisten ja viimeisten tavujen avulla. Viimeisille neljälle tavulle tehdään aluksi riviensiirto, tavujenkorvaus ja kierrosvakionsummaus. Laskettu tulos summataan XOR-operaatiolla ensimmäisten neljän tavun kanssa.

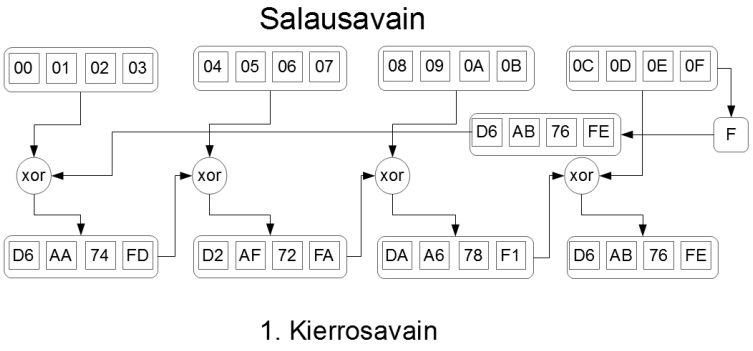
Riviensiirrossa tavuja siirretään yksi paikka vasemmalle ja tavujenkorvaus korvaa tavut toisilla. Operaatioiden toiminta esitetään seuraavissa alaluvuissa. Kierrosvakio vaihtuu joka summauksen jälkeen. Kierrosvakiot ovat käyttöjärjestyksessä: 01, 02,



Kuva 45: Kierrosavaimen ensimmäisten tavujen luominen.

04, 08, 10, 20, 40, 80, 1B ja 36.

Kierrosavaimen muut tavut luodaan kuvan 46 mukaisesti XOR-operaatioilla. Jokainen kierrosavain luodaan vastaavalla tavalla edeltävän kierrosavaimen avulla.



Kuva 46: Kierrosavaimen luominen.

A.3 AES-kierros

AES-kierros koostuu neljästä operaatiosta: tavujenkorvaus, riviensiirto, sarakkeidensekoitus ja kierrosavaimensummaus. Kuvassa 47 nähdään esimerkkilohkon välitulokset jokaisen operaation jälkeen ensimmäisellä kierroksella.

63	F2	30	FE
7C	6B	01	D7
77	6F	67	AB
7B	C5	2B	76

(a) Välitulos tavujenkorvauksen jälkeen.

63	F2	30	FE
6B	01	D7	7C
67	AB	77	6F
76	7B	C5	2B

(b) Välitulos riviensiirron jälkeen.

6A	2C	B0	27
6A	6D	D9	9C
5C	33	5D	21
45	51	61	5C

(c) Välitulos sarakkeidensekoituksen jälkeen.

BC	FE	6A	F1
C0	C2	7F	37
28	41	25	57
B8	AB	90	A2

(d) Välitulos ensimmäisen AES-kierroksen jälkeen.

Kuva 47: Esimerkkilohkon välitulokset ensimmäiseltä AES-kierrokselta.

A.3.1 Tavujenkorvaus

AES-kierros alkaa tavujenkorvauksella. Jokainen lohkon tavu korvataan toisella tavulla. Jokaiselle tavulle on korvaava tavu niin kutsutussa korvauslaatikkossa. Kuvassa 48 nähdään esimerkki korvauslaatikon käytöstä. Esimerkiksi tavu 8B korvataan tavulla 3D. Tavun ensimmäinen heksaluku valitsee rivin ja toinen heksaluku valitsee sarakkeen, jolta korvaava tavu valitaan.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CD	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	05	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Kuva 48: AES tavujenkorvaus.

Esimerkkissä ensimmäisen AES-kierroksen tavujenkorvaus ottaa tulona kuvassa 43 näkyvän AES-välituloksen. Operaatio tuottaa kuvassa 47a näkyvän AES-välituloksen korvaamalla jokaisen tavun esitetyllä tavalla.

A.3.2 Riviensiirto-operaatio

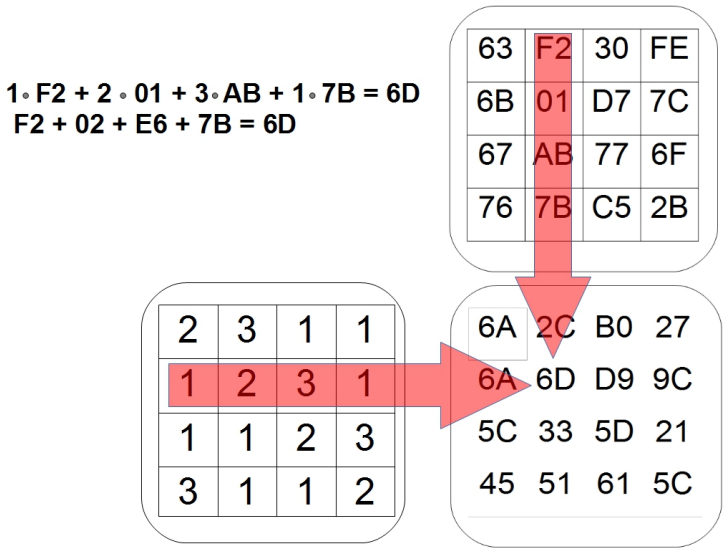
Riviensiirto-operaatiossa AES-välituloksen tavuja siirretään horisontaalisesti vasemmalle. Ensimmäisen rivi säilyy muuttumattomana, mutta toisen rivin tavuja siirretään yksi paikka vasemmalle. Kolmannen rivin tavuja siirretään kaksi paikkaa ja neljännen rivin tavuja kolme paikkaa vasemmalle. Rivin vasemmalta reunalta yli siirrettäessä seuraava paikka on rivin oikea reuna eli rivin viimeinen paikka.

Kuvassa 47a näkyvä tavujenkorvaus-operaation tulos välitetaan riviensiirto-operaatiolle ja riviensiirron tulos nähdään kuvassa 47b. Esimerkiksi kolmannen rivin toinen tavu 6F siirretään saman rivin viimeiseen paikkaan, koska kolmannen rivin tavuja siirretään kaksi paikkaa vasemmalle.

A.3.3 Sarakkeiden sekoitusoperaatio

Sarakkeiden sekoitusoperaatiossa edeltävä AES-välitulos kerrotaan ennalta määrätyllä matriisilla. Kuvassa 49 näkyy ennalta määrätty matriisi ja esimerkki yhden alkion laskemisesta. Sarakkeiden sekoitusoperaation tuottaman AES-välituloksen jo-

kainen alkio riippuu operaatiota edeltäneen AES-välituloksen yhden sarakkeen jokaisesta alkioista. Huomioitavaa on, että laskuoperaatiot suoritetaan $GF(2^8)$ kentässä.



Kuva 49: AES sarakkeiden sekoituksessa käytettävä matriisi.

.

A.3.4 Kierrosavaimensummaus

Kierrosavaimensummaus on XOR-operaatio AES-välituloksen ja kierrosavaimen välillä. Summauksen toiminta käytettävässä kentässä on esitetty alaluvussa A.1.