2020/2500M-0124

ISSN 1797-3457 (verkkojulkaisu)
ISBN (PDF) 978-951-25-3348-0

TIIVISTELMÄRAPORTTI

FPGA-pohjaisen TRNG:n stokastisen mallin todentaminen ja testaus

TkT Matti Tommiska, toimitusjohtaja Xiphera Oy, matti.tommiska@xiphera.com
DI Valtteri Marttila, suunnittelija Xiphera Oy, valtteri.marttila@xiphera.com

Tiivistelmä

Tutkimushankkeessa todennettiin Xiphera OY:n kehittämän FPGA-pohjaisen (FPGA = Field Programmable Gate Array, kenttäohjelmoitava logiikkapiiri) aidon satunnaislu-kugeneraattorin (TRNG, True Random Number Generator) pohjana olevan entropialähteen stokastisen mallin oikeellisuus kattavilla testeillä. Hanke lisäsi suomalaista kryptografian osaa-mista ja huoltovarmuutta lisäävää tuotetarjontaa maanpuolustukselle kriittisiin sovelluksiin.

1. Johdanto

Tiedon salaus ja suojaus (kryptografia) on vuosituhansia vanha tieteenhaara, jonka kehittäjänä ja käyttöönottajana sotilassovellukset ovat aina olleet eturintamassa. Nykyään yleisin jako kryptografian sisällä tehdään symmetristen (esimerkiksi laajalti käytetty AES (Advanced Encryption Standard AES)) ja epäsymmetristen salausmenetelmien (esimerkkeinä RSA, elliptisiin käyriin perustuvat salausmenetelmät, jne.) kesken, mutta kaiken luotettavan kryptografian edellytyksenä on myös kyky tuottaa luotettavasti satunnaisuutta aidolla satunnaislukugeneraattorilla.

Satunnaislukujen sovelluksia kryptografiassa ovat esimerkiksi yksityisten avainten (private key) luonti epäsymmetrisissä salausmenetelmissä ja yhteyskohtaisten salausavainten (session keys) ja alustusvektorien (initialization vector) luonti symmetrisissä salausmenetelmissä. Lisäksi aitoja satunnaislukuja tarvitaan muun muassa siementämään näennäissatunnaislukugeneraattorit.

Salausmenetelmät voidaan lähtökohtaisesti toteuttaa joko ohjelmistollisesti tai laitteistolli-sesti, tai edellisten yhdistelmällä. Turvallisuuskriittisissä sovelluksissa laitteistollinen toteutustapa on ehdottomasti etusijainen ja usein myös välttämätön, koska ohjelmistollinen to-teutus on huomattavasti laitteistollista toteutusta haavoittuvaisempi. Tähän ovat syynä muun muassa ohjelmistollisten toteutus riippuvuus kolmansien osapuolien tekemistä sa-lauskirjastoista, käyttöjärjestelmistä ja suorittimista. Laitteistollisella toteutuksella saavu-tetaan huomattavasti parempi salausmenetelmän toteutuksen ymmärrys ja omistajuus, pienempi hyökkäyspinta-ala (attack surface), vahvempi suoja sivukanavahyökkäyksiä vastaan sekä usein myös kertaluokkia parempi suorituskyky.

Laitteistollinen salaus toteutetaan usein uudelleenohjelmoitavilla logiikkapiireillä (Field Programmable Gate Array, FPGA), joiden teknisiksi eduiksi voidaan myös laskea kenttäpäivitettävyys, edulliset kehityskustannukset sekä sisäänrakennetut tietoturvaominaisuu-det. Neljä suurinta FPGA-valmistajaa ovat Intel, Lattice, Microchip ja Xilinx, joita kaikkia käytettiin tässä tutkimuksessa. Tällä tavoiteltiin ja saavutettiin valmistajakentän

mahdollisimman kattavasti tukeva TRNG-toteutus, mikä myös osaltaan vahvistaa huoltovarmuutta.

2. Tutkimuksen tavoite ja suunnitelma

TRNG:n luotettava toteutus on edellytys koko salausmenetelmän (sekä epäsymmetriset että symmetriset standardit) laitteistolliselle toteutukselle, jonka kokonaisedut esiteltiin "Johdanto" kappaleessa.

Tutkimuksen lähtökohtana oli Xiphera Oy:n kehittämä aito satunnaislukugeneraattori, jonka pohjana olevan entropialähteen toiminnallisuus oli jo aiemmin testattu FPGA-pohjaisilla kehityskorteilla (development kit) huoneenlämpotilassa dieharder-testillä.

Xipheran suunnittelemassa entropialähteessä on sekä vaakasuora että pystysuora parametri, joiden arvot varmennettiin kattavalla testauksella, jonka eräänä pohjana olivat kansainväliset standardit.

TRNG-standardeista relevanteimmat ovat yhdysvaltalaisen NIST:in (National Institute of Standards and Technology) erityisjulkaisut (Special Publication) SP 800-90A, SP 800-90B ja SP 800-90C, samoin NIST:in julkaisema liittovaltion tiedonkäsittelystandardi FIPS 140-3 sekä viime vuosina erityisesti eurooppalaisissa vaatimuksissa yleistynyt Saksan BSI:n (Das Bundesamt für Sicherheit in der Informationstechnik) AIS-31 standardi.

Sekä amerikkalaiset että saksalaiset standardit sisältävät vaatimukset TRNG:n sekä online- että offline-testeille. Näistä online-testillä tarkoitetaan TRNG:n ja sen sisältämän entropialähteen toiminnallisuuden jatkuvaa seurantaa, jolloin voidaan välittömästi havaita TRNG:n tuottaman satunnaisuuden laadun romahtaminen (ns. catastrophic failure). Sen sijaan offline-testillä verrataan TRNG:n tuottaman satunnaisuuden tilastollista vastaavuutta ideaalisen satunnaislähteen tuottamaan satunnaisuuteen.

Offline-testitkin ovat tyypillisesti laskennallisesti huomattavasti vaativampia kuin online-testit. Lisäksi AIS-31 tämän tutkimuksen kannalta olennaisesti edellyttää myös TRNG:n pohjana olevan fysikaalisen ilmiön stokastisen mallin esittämistä.

Edellä mainittuihin lähtökohtiin perustuen tutkimuksen keskeiset tavoitteet olivat neljään työaihioon (TA) jaettuina:

TA1: TRNG:n sisältämän entropialähteen stokastisen mallin johtaminen ja todentaminen,

TA2: TRNG:n sisältämän entropialähteen kattava testaus sallittujen käyttöolosuhteiden ääripisteissä,

TA3: TRNG:n sisältämän entropialähteen robustisuuden selvittäminen lämpötilan suhteen, ja

TA4: TRNG:n sisältämän entropialähteen mitoittamisen ns. crossover -piste. Tämä tarkoittaa edellä mainittujen vaakasuoran ja pystysuoran suureiden minimiarvoja, joiden alittuessa TRNG ei enää tuota luotettavasti satunnaisuutta

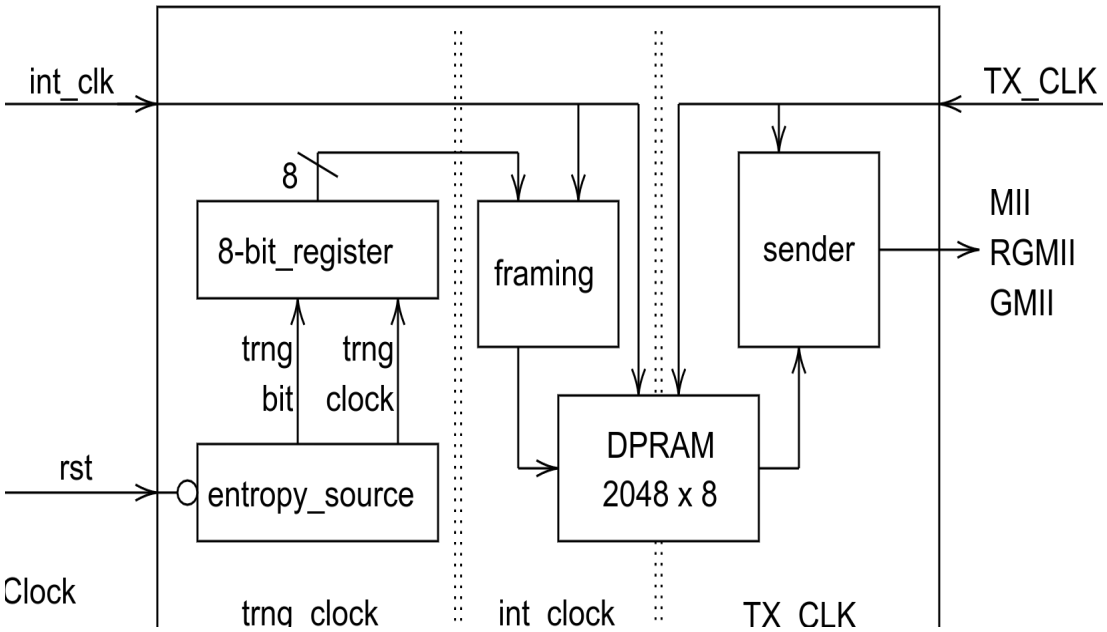
3. Aineisto ja menetelmät

Kuten aiemmassa kappaleessa todettiin, saksalaisen AIS-31 standardin vaatimuksena on stokastinen matemaattinen malli TRNG:n sisältämän entropialähteen toiminnan pohjalla

olevalle fysikaaliselle ilmiölle. Tässä tutkimuksessa kaikkein teoreettisin osuus kohdistuikin tähän työaihioon TA1, jossa johdettiin stokastinen matemaattinen malli Xiphera Oy:n ke-hittämän TRNG:n sisältämälle entropialähteelle..

TA2:ssa tavoitteena oli TRNG:n laitteistollinen toteutus valmistajariippumattomasti neljän edellä mainitun FPGA-valmistajan teknologialla. Tämä toteutettiin hankkimalla kolme ke-hityskorttia per FPGA-valmistaja, jotta saavutettiin tilastollisesti riittävän kattava otos FPGA-valmistajaa kohti. FPGA-valmistajien piiritarjoomasta valittiin esiselvityksen pohjal-ta Intel® Cyclone® 10 GX, Xilinx® UltraScale+™ MPSoC, Lattice© Semiconductor ECP5™ ja Microchip® IGLOO2™, jotka tarjosivat kattavan poikkileikkauksen modernista FPGA-teknologiasta.

TA3:ssa kaikki entropialähteen toteutukset testattiin kattavasti sallittujen käyttölämpötila-alueiden ääripisteissä. Itse testausjärjestelmän suunnittelu ja toteutus oli tutkimushankkeen insinöörimäisin osuus, ja kehitetty satunnaisbittien keruumekanismi tehtiin mahdollisimman FPGA-valmistajasta riippumattomaksi, ja sen korkean tason lohkokaavio on esitetty alla:



TA4:ssa edellä kuvattujen testien lopputulokset analysoitiin ja FPGA-valmistajien väliset erot TRNG-toteutuksen sisältämän entropialähteen robustisuuden osalta kvantifioitiin. Testitulokset analysoitiin kattavasti offline-testeillä, joiden avulla selvitettiin TRNG:n robustisuus lämpötilan suhteen. Lisättäköön, että tutkimushankkeen aikana myös päivitettiin tietämys satunnaislukutestien tarjoomasta, ja testeissä käytettiin parhaina ja vaativimpina pidettäviä TestU01, Practrand, ja gjrand-testejä.

Lisäksi selvitettiin TRNG:n sisältämän entropialähteen ns. crossover -piste, mikä mahdollistaa TRNG:n perustana olevan konstruktion optimaalisen mitoittamisen sekä vaaka- että pystysuoran parametrin suhteen.

4. Tulokset ja pohdinta

Tutkimuksen tieteellinen merkittävyys koostui TRNG:n stokastisen mallin johtamisesta ja todentamisesta, mallin kattavasta testaamisesta neljällä eri FPGA-valmistajan tuotteilla sekä TRNG:n robustisuuden kvantifioinnista.

Edellä mainituista tieteellisen merkittävyyden määreistä kaikkein suurin uutuusarvo on julkisesti saatavilla olevan tiedon mukaan TRNG:n robustisuuden ja crossover -pisteiden määrittäminen. Tyypillisesti aiemmassa kansainvälisessä tutkimuksessa on toteutettu FPGA-pohjainen aito satunnaislukugeneraattori vain yhden FPGA-valmistajan yhdellä kehityskortilla; lisäksi testaus on usein suoritettu huoneenlämmössä ja lopputuloksena on ilmoitettu ainoastaan pass/fail -tyyppinen arvio TRNG:n aitoudesta.

Tutkimus on aihealueeltaan sekä tulostavoitteiltaan merkittävää ja konkreettisesti hyödynnettävää maanpuolustukselle. Laitteistollinen tiedon salauksen ja suojauksen toteutus saavuttaa korkeamman suojaustason ja Suomessa kehitetty, mallinnettu ja kattavasti testattu FPGA-pohjainen TRNG on kriittinen osa jokaista salausjärjestelmää.

Tutkimus nostaa suomalaisen laitteistollisen kryptografian osaamista ja tarjoaa käyttöönotettavia ratkaisuja ja testauspalveluja niin Puolustusvoimien kuin sen strategisen kumppaniverkoston hankkeisiin.

5. Loppupäätelmät

Tutkimushanke onnistui saavuttamaan alkuperäiset tavoitteet määritellyssä aikataulussa ja budjetissa. Lisäksi tutkimushanke tuotti uutta tieteellistä tietoa entropialähteen stokastisen mallin johtamisessa ja todentamisessa, sen robustisuuden raja-arvojen määrittämisessä ja yleisesti suomalaisen salain-teknologian osaamisen ja huoltovarmuuden parantamisessa.

Mahdolliset jatkotutkimusaiheet sisältävät vaihtoehtoisten entropialähteiden stokastisen mallin johtamisen ja todentamisen, sekä entropialähteen testaamisen muillakin FPGA-piiriperheillä ja ASIC-piireillä.

6. Tutkimuksen tuottamat tieteelliset julkaisut ja muut mahdolliset raportit

Valtteri Marttila. Design and implementation of test platform to quantify the robustness of FPGA-based true random number generator design; FPGA-pohjaisen todellisen satunnaislukugeneraattorin testausjärjestelmän suunnittelu ja toteuttaminen. G2 pro gradu, diplomityö, 2020-08-17.

Matti Tommiska. Stochastic Model of the Entropy Source in Xiphera’s True Random Number Generator. Internal Report, 2020-12-14