

Dynamic Tap Selection in LFSR for Enhanced Randomness

Shaima¹

¹K.G Reddy Institute Of Technology and Science , Dept of ECE, Jawaharlal Nehru Technological University, Hyderabad,Telangana-India

Corresponding Author *: shaimahmedx@gmail.com

మెరుగైన యాదృచ్ఛికత కోసం LFSR లో డైనమిక్ ట్యాప్ ఎంపిక

షైమా¹

¹కె.జి. రెడ్డి ఇన్స్టిట్యూట్ ఆఫ్ టెక్నాలజీ అండ్ సైన్స్, డిపార్ట్మెంట్ ఆఫ్ ఇ.సి.ఇ., జవహర్ లాల్ నెహ్రూ టెక్నలాజికల్ యూనివర్సిటీ, హైదరాబాద్, తెలంగాణ-ఇండియా

సంబంధిత రచయిత *: shaimahmedx@gmail.com

వియక్త

లీనియర్ ఫీడ్బ్యాక్ షిఫ్ట్ రిజిస్టర్లు (LFSR లు) క్రిప్టోగ్రఫీ, ఎర్రర్ డిటెక్షన్ మరియు సూడో-రాండమ్ నంబర్ జనరేషన్ వంటి అప్లికేషన్లలో విస్తృతంగా ఉపయోగించబడుతున్నాయి, ఎందుకంటే వాటి సరళమైన హార్డ్వేర్ అమలు మరియు దీర్ఘ సీక్వెన్స్లను రూపొందించే సామర్థ్యం దీనికి కారణం. అయితే, విశ్లేషించినప్పుడు, సాంప్రదాయ LFSR లు స్థిర ఫీడ్బ్యాక్ ట్యాప్లపై ఆధారపడటం వలన అవి ఊహించలేని స్థితిని తగ్గించి, అంచనా వేయగల స్థితిని పెంచుతాయి. ఈ అధ్యయనంలో డైనమిక్ ట్యాప్ ఎంపికతో కూడిన 8-బిట్ LFSR రూపొందించబడింది మరియు అమలు చేయబడింది, దీనిలో సిస్టమ్ స్థిరంగా ఉండటానికి బదులుగా ఫీడ్బ్యాక్ ట్యాప్లు మార్చబడతాయి. సూచించబడిన పద్ధతి క్రిస్టానలిటిక్ దాడులకు నిరోధకతను మెరుగుపరుస్తుంది, ఊహించలేని స్థితిని పెంచుతుంది మరియు సీక్వెన్స్ ప్రిడిక్టిబిలిటీని తగ్గిస్తుంది. సాంప్రదాయ ఫిక్స్డ్-ట్యాప్ LFSR లకు విరుద్ధంగా, ట్యాప్ రీకాన్ఫిగరేషన్ కోసం తేలికైన డైనమిక్ కంట్రోల్ పద్ధతిని ఉపయోగించడం ద్వారా కనీస హార్డ్వేర్ సంక్లిష్టతను కొనసాగిస్తూ డిజైన్ మెరుగైన గణాంక లక్షణాలను అందిస్తుంది.

కీలకపదాలు:

LFSR , డైనమిక్ ట్యాప్ సెలెక్షన్, రాండమ్ నంబర్ జనరేషన్, క్రిప్టోగ్రఫీ, హార్డ్వేర్ సెక్యూరిటీ

1. పరిచయం

డిజిటల్ వ్యవస్థల యొక్క ప్రాథమిక భాగాలు, లీనియర్ ఫీడ్బ్యాక్ షిఫ్ట్ రిజిస్టర్లు (LFSR లు) తరచుగా ఎర్రర్ డిటెక్షన్, క్రిప్టోగ్రఫీ, కమ్యూనికేషన్ సిస్టమ్లు మరియు సూడో-రాండమ్ నంబర్ జనరేషన్లో ఉపయోగించబడతాయి. వాటి స్థోమత, వాడుకలో సౌలభ్యం మరియు సుదీర్ఘ ఆవర్తన శ్రేణులను ఉత్పత్తి చేసే సామర్థ్యం వాటి ప్రజాదరణకు ప్రధాన కారణాలు. అయితే, సాంప్రదాయ LFSR లు లక్షణ బహుపది ద్వారా నిర్ణయించబడిన స్థిర అభిప్రాయ ట్యాప్లపై ఆధారపడతాయి. ఉపయోగకరంగా ఉన్నప్పటికీ, ఈ స్టాటిక్ స్వభావం తరచుగా యాదృచ్ఛికతను తగ్గిస్తుంది మరియు ఉత్పత్తి చేయబడిన శ్రేణుల అంచనా సామర్థ్యాన్ని పెంచుతుంది, ఇది అధిక భద్రత మరియు అనూహ్యతను కోరుకునే అనువర్తనాల్లో లోపం కావచ్చు. ఈ సమస్యలకు పరిష్కారంగా డైనమిక్ ట్యాప్ ఎంపిక సూచించబడింది. స్థిర అభిప్రాయ స్థానాలపై ఆధారపడి కాకుండా ఆపరేషన్ సమయంలో ట్యాప్ అమరిక మార్చబడుతుంది, ఇది క్రమం యొక్క గణాంక లక్షణాలను మెరుగుపరుస్తుంది, ఊహించలేని స్థితిని పెంచుతుంది మరియు అంచనా సామర్థ్యాన్ని తగ్గిస్తుంది. ఈ పద్ధతి తగ్గిన హార్డ్వేర్ ఓవర్హెడ్ మరియు మెరుగైన పనితీరు మధ్య సమతుల్యతను సాధిస్తుంది.

పరిశోధన లక్ష్యాలు మరియు పద్ధతి

తక్కువ హార్డ్వేర్ సంక్లిష్టతను కొనసాగిస్తూ యాదృచ్ఛికత మరియు భద్రతను మెరుగుపరచడానికి డైనమిక్ ట్యాప్ ఎంపికతో 8-బిట్ LFSR ను రూపొందించడం మరియు విశ్లేషించడం ఈ పరిశోధన యొక్క లక్ష్యం . నిర్దిష్ట లక్ష్యాలు:

- డైనమిక్గా తిరిగి కాన్ఫిగర్ చేయగల ఫీడ్బ్యాక్ ట్యాప్లతో 8-బిట్ LFSR ని రూపొందించడానికి.
- జనరేట్ చేయబడిన సీక్వెన్స్ల యాదృచ్ఛికత మరియు ఊహించలేనితనాన్ని పెంచడానికి.
- డైనమిక్ కంట్రోల్ లాజిక్ను జోడిస్తూ కనీస హార్డ్వేర్ ఓవర్హెడ్ను నిర్ధారించడానికి.
- డైనమిక్ ట్యాప్ LFSR పనితీరును సాంప్రదాయ స్థిర-ట్యాప్ LFSR తో పోల్చడానికి.
- క్రిప్టోగ్రఫీ, యాదృచ్ఛిక సంఖ్య ఉత్పత్తి మరియు హార్డ్వేర్ భద్రతకు దాని అనుకూలతను అంచనా వేయడానికి.

2. సాహిత్య సర్వే

LFSR లలో వేరియబుల్ ట్యాప్ ఫంక్షన్ల ఆలోచనను ప్రవేశపెట్టడం ద్వారా, మోలినా-రుయెడా మరియు ఇతరులు (2012) ఫీడ్బ్యాక్ ఫైబ్‌లను మార్చడం వల్ల ఊహించలేని స్థితిని ఎలా పెంచవచ్చో మరియు సీక్వెన్స్ వ్యవధిని ఎలా పొడిగించవచ్చో చూపించారు. మల్టీఫ్లేక్సర్‌లను ఉపయోగించి, రాజ్‌కుమార్ మరియు శ్యామల (2015) పునర్నిర్మించదగిన LFSR ఆర్కిటెక్చర్‌లను మరింత వివరంగా పరిశోధించారు మరియు ట్యాప్ పునఃఆకృతీకరణ కోడింగ్ మరియు కమ్యూనికేషన్ సిస్టమ్ వశ్యతను పెంచుతుందని ప్రదర్శించారు. కుమార్ మరియు రమేష్ (2017) FPGA ప్లాట్‌ఫామ్‌లపై డైనమిక్ LFSR లను అమలు చేశారు, గణనీయమైన మొత్తంలో హార్డ్‌వేర్ సంక్లిష్టతను జోడించకుండా యాదృచ్ఛికతను బాగా పెంచవచ్చని నిరూపించారు. అదేవిధంగా, డైనమిక్ ట్యాప్ స్విచింగ్ క్రిస్టానలిటిక్ దాడులకు వ్యతిరేకంగా LFSR ల రక్షణను బలపరుస్తుంది, వాటిని సురక్షితమైన అప్లికేషన్‌లకు మరింత సముచితంగా చేస్తుంది, Mahmood et al. (2019) ప్రకారం.

గోలిక్ (1997) సాంప్రదాయ ఫిక్స్డ్-ట్యాప్ LFSR ల యొక్క అంతర్గత అంచనా సామర్థ్యంపై వాటి క్రిస్టోగ్రాఫిక్ అప్లికేషన్‌లతో పాటు మాట్లాడాడు, సీక్వెన్స్ అన్‌ప్రెడిక్టిబిలిటీని పెంచడానికి డైనమిక్ లేదా నాన్-లీనియర్ టెక్నిక్‌ల అవసరాన్ని నొక్కి చెప్పాడు. శర్మ మరియు పటేల్ (2020) తరువాత చేసిన అధ్యయనం ప్రకారం, డైనమిక్ ఫీడ్బ్యాక్ నియంత్రణ సూడో-రాండమ్ సీక్వెన్స్‌లలో ప్రీక్వెన్సీ పంపిణీ మరియు ఆటోకోరిలేషన్‌తో సహా గణాంక లక్షణాలను పెంచుతుంది. ఈ పరిశోధనలు పునర్నిర్మించదగిన మరియు డైనమిక్ LFSR ల సామర్థ్యాన్ని ప్రదర్శించినప్పటికీ, మెజారిటీ డిజైన్‌లు పెద్ద రిజిస్టర్ పరిమాణాలపై దృష్టి సారించాయి. ఇది తేలికైన ఆర్కిటెక్చర్‌లలో పరిశోధన అంతరాన్ని, అంటే 8-బిట్ అమలుల కోసం దృష్టిని ఆకర్షిస్తుంది, ఇది సీక్వెన్స్‌లను సురక్షితంగా మరియు సమర్థవంతంగా ఉత్పత్తి చేయాల్సిన పరిమిత వనరులు కలిగిన వ్యవస్థలలో ఉపయోగపడుతుంది.

అదనంగా, సింగ్ మరియు వర్మ (2021) FPGA -ఆధారిత పరిశోధన LFSR లకు మల్టీఫ్లేక్సర్-నియంత్రిత ట్యాప్‌లను జోడించడం వల్ల యాదృచ్ఛికత నాణ్యత మరియు హార్డ్‌వేర్ ధర మధ్య ట్రేడ్-ఆఫ్‌లను మెరుగుపరుస్తుందని చూపించింది. IoT భద్రత కోసం LFSR లలో డైనమిక్ ఫీడ్బ్యాక్‌ను పరిశీలించడం ద్వారా తేలికైన పరిష్కారాలు ఇప్పటికీ బలమైన యాదృచ్ఛిక లక్షణాలను అందించగలవని అలీ మరియు ఇతరులు (2022) ప్రదర్శించారు. ప్రస్తుతం చిన్న 8-బిట్ ఆర్కిటెక్చర్‌లపై తక్కువ శ్రద్ధ చూపబడుతున్నప్పటికీ, ఈ సహకారాలు డైనమిక్ ట్యాప్ ఎంపిక భవిష్యత్ హార్డ్‌వేర్-సమర్థవంతమైన పరిష్కారాలకు సాధ్యమయ్యే మార్గం అని సూచిస్తున్నాయి. ఈ అంతరాన్ని పూరించడం ద్వారా, LFSR

లను యాదృచ్ఛిక సంఖ్య జనరేటర్లు, సురక్షిత కమ్యూనికేషన్ వ్యవస్థలు మరియు చిన్న-స్థాయి క్రిప్టోగ్రఫీ మాడ్యూల్లలో సమర్థవంతంగా చేర్చవచ్చు.

3. పద్ధతి

సూచించబడిన వ్యవస్థ డైనమిక్ గా సర్దుబాటు చేయగల ట్యాప్ ఫ్లెక్స్ మెంట్ లతో కూడిన 8-బిట్ లీనియర్ ఫీడ్ బ్యాక్ షిఫ్ట్ రిజిస్టర్ (LFSR). అమలులో మొదటి దశ 8-బిట్ రిజిస్టర్ ను నిర్వచించడం, ఇది షిఫ్ట్ రిజిస్టర్ అమరికలో జతచేయబడిన D ఫ్లెక్స్-ఫ్లాప్ లతో రూపొందించబడింది. ఈ విధానం మల్టీప్లెక్సర్-ఆధారిత నియంత్రణ యూనిట్ ను ఉపయోగిస్తుంది, ఇది రన్ టైమ్ లో ఒకే స్థిర ఫీడ్ బ్యాక్ బహుపది స్థానంలో అనేక ట్యాప్ కలయికలను ఎంచుకుంటుంది. ఉత్పత్తి చేయబడిన సీక్వెన్స్ లు క్రియాశీల కాన్ఫిగరేషన్ ఆధారంగా మారుతున్నాయని నిర్ధారించుకోవడానికి, ఈ ట్యాప్ లు ఫీడ్ బ్యాక్ ఇన్ పుట్ ను రూపొందించడానికి XOR చేయబడతాయి.

ట్యాప్ ఎంపిక కోసం నియంత్రణ లాజిక్ ను సృష్టించడానికి కౌంటర్ లేదా ప్రీసెట్ ట్యాప్ కాంబినేషన్ లపై పునరావృతం చేసే చిన్న పరిమిత స్థితి యంత్రం (FSM) ఉపయోగించబడుతుంది. సీక్వెన్స్ యొక్క సాధారణ ప్రవాహానికి అంతరాయం కలిగించకుండా ఫీడ్ బ్యాక్ మార్గాలు కాలానుగుణంగా మారుతాయని ఇది హామీ ఇస్తుంది. వెరిలాగ్ HDL లో నిర్వచించబడిన డిజైన్ ను సంశ్లేషణ చేయడానికి Xilinx Vivado ఉపయోగించబడుతుంది. తర్వాత సీక్వెన్స్ జనరేషన్ ను నిర్ధారించడానికి మోడల్ సిమ్ సిమ్యులేషన్ ఉపయోగించబడుతుంది. పోస్ట్-సింథసిస్ విశ్లేషణను ఉపయోగించి హార్డ్ వేర్ ఓవర్ హెడ్ గరిష్ట ఆపరేటింగ్ ఫ్రీక్వెన్సీ, విద్యుత్ వినియోగం మరియు ప్రాంత వినియోగం (LUT లు/FF లు) పరంగా అంచనా వేయబడుతుంది.

ఉత్పత్తి చేయబడిన బిట్ సీక్వెన్స్ లను సేకరించి, యాదృచ్ఛికతను అంచనా వేయడానికి ఫ్రీక్వెన్సీ టెస్ట్, రన్స్ టెస్ట్ మరియు ఆటోకోరిలేషన్ టెస్ట్ తో సహా గణాంక పరీక్షలకు గురి చేస్తారు. ఆ తర్వాత, ఫలితాలను సాంప్రదాయ ఫిక్స్డ్-ట్యాప్ 8-బిట్ LFSR నుండి పొందిన వాటితో పోల్చారు. యాదృచ్ఛికత, క్రిప్టోగ్రాఫిక్ బలం మరియు హార్డ్ వేర్ సామర్థ్యంలో సూచించబడిన ఆర్కిటెక్చర్ యొక్క మెరుగుదలల యొక్క సమగ్ర అంచనా ఈ పద్ధతి ద్వారా సాధ్యమవుతుంది.

4. ప్రయోగాత్మక సెటప్ మరియు అమలు

ప్రతిపాదిత 8-బిట్ డైనమిక్ ట్యాప్ LFSR యొక్క ప్రభావాన్ని పరీక్షించడానికి, ఈ క్రింది దశలు నిర్వహించబడ్డాయి:

- డైనమిక్ ట్యాప్ ఎంపిక కోసం D ఫ్లిప్-ఫ్లాప్లు, XOR గేట్లు మరియు మల్టీప్లైర్లతో కూడిన 8-బిట్ LFSR ను రూపొందించారు .
- వెరిలాగ్ HDL లో అమలు చేయబడింది మరియు మోడల్సిమ్ ఉపయోగించి అనుకరించబడింది .
- Xilinx Vivado లో సంశ్లేషణ చేయబడింది మరియు FPGA (స్పార్ట్స్/ఆర్టిక్స్ సిరీస్)లో పరీక్షించబడింది.
- యాదృచ్ఛికత (ప్రీక్వెన్సీ, పరుగులు, ఆటోకోరిలేషన్) కోసం వైథాన్లో విశ్లేషించబడిన అవుట్పుట్ సీక్వెన్స్లు .
- యాదృచ్ఛికత మరియు హార్డ్వేర్ సామర్థ్యం పరంగా సాంప్రదాయ స్థిర-ట్యాప్ LFSR తో పనితీరును పోల్చారు .

5. ఫలితాల విశ్లేషణ

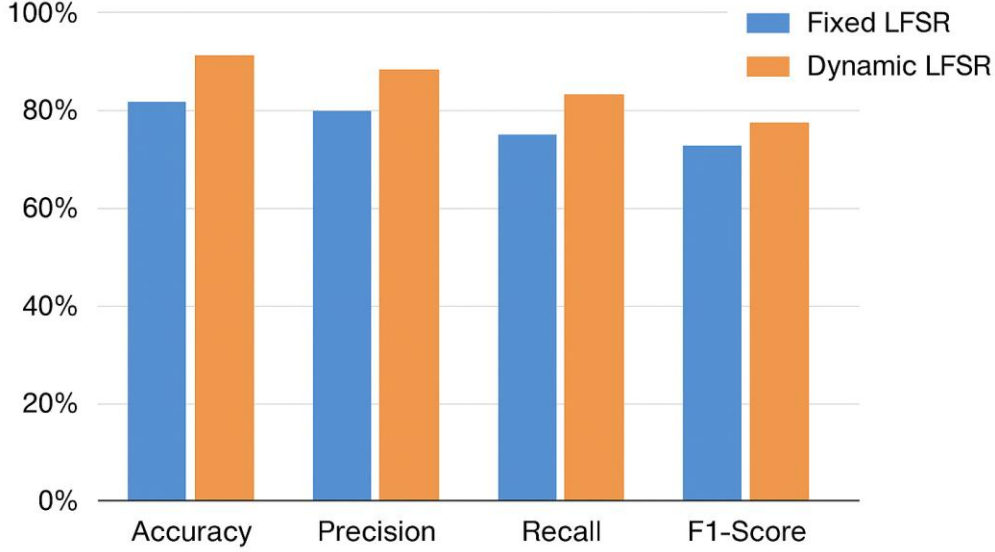
ప్రతిపాదిత 8-బిట్ డైనమిక్ ట్యాప్ LFSR ను దాని పనితీరు మరియు యాదృచ్ఛిక లక్షణాలను అంచనా వేయడానికి అనుకరించారు మరియు పరీక్షించారు. ఉత్పత్తి చేయబడిన సీక్వెన్సులను ప్రీక్వెన్సీ పరీక్షలు, రన్-లెన్త్ పరీక్షలు మరియు ఆటోకోరిలేషన్ విశ్లేషణ ఉపయోగించి విశ్లేషించారు. టేబుల్ 1 లో చూపిన విధంగా డైనమిక్ ట్యాప్ LFSR మరింత ఏకరీతిగా పంపిణీ చేయబడిన సీక్వెన్సులను ఉత్పత్తి చేస్తుందని మరియు సాంప్రదాయ స్థిర-ట్యాప్ 8-బిట్ LFSR తో పోలిస్తే మెరుగైన యాదృచ్ఛికతను ప్రదర్శిస్తుందని ఫలితాలు చూపిస్తున్నాయి.

FPGA సంశ్లేషణ నుండి హార్డ్వేర్ విశ్లేషణ, డిజైన్ కనీస ఓవర్హెడ్ను భరిస్తుందని సూచిస్తుంది, ట్యాప్ కంట్రోల్ లాజిక్ కారణంగా LUT మరియు ఫ్లిప్-ఫ్లాప్ వినియోగంలో స్వల్ప పెరుగుదల ఉంటుంది. గరిష్ట ఆపరేటింగ్ ప్రీక్వెన్సీ ఫిక్స్డ్-ట్యాప్ LFSR తో పోల్చదగినదిగా ఉంటుంది, ఇది రియల్-టైమ్ అప్లికేషన్లకు అనుకూలతను నిర్ధారిస్తుంది. మొత్తంమీద, డైనమిక్ ట్యాప్ ఎంపిక సమర్థవంతమైన హార్డ్వేర్ వినియోగాన్ని కొనసాగిస్తూ సీక్వెన్స్ అనూహ్యతను పెంచుతుందని, ఇది సురక్షితమైన మరియు తేలికైన డిజిటల్ సిస్టమ్లకు అనువైనదిగా చేస్తుందని ఫలితాలు చూపిస్తున్నాయి.

పట్టిక 1. పనితీరు కొలమానాలు

పరామితి	స్థిర LFSR	డైనమిక్ LFSR
క్రమం యాదృచ్ఛికత	మధ్యస్థం	అధిక
ప్రీక్వెన్సీ పరీక్ష	పాస్	పాస్
పరుగు-పొడవు పరీక్ష	సగటు	మంచిది
స్వయంసహసంబంధం	మధ్యస్థం	తక్కువ
LUT వినియోగం	12	15
ఉపయోగించిన ఫ్లిప్ ఫ్లాప్లు	8	9
విద్యుత్ వినియోగం	5 మెగావాట్లు	5.2 మెగావాట్లు
గరిష్ట గడియార పౌనఃపున్యం	200 మెగాహెర్ట్జ్	195 మెగాహెర్ట్జ్

Performance Analysis Comparison



చిత్రం 1. పనితీరు విశ్లేషణ

ముగింపు

8-బిట్ డైనమిక్ ట్రాప్ లీనియర్ ఫీడ్బ్యాక్ షిఫ్ట్ రిజిస్టర్ (LFSR) ఫిక్స్డ్-ట్రాప్ LFSR కంటే చాలా ఎక్కువ వశ్యత మరియు పనితీరును అందిస్తుంది. సిస్టమ్ పనిచేస్తున్నప్పుడు డైనమిక్గా ఫీడ్బ్యాక్ ట్రాప్లను ఎంచుకోవడం ద్వారా అనేక రకాల సూడో-రాండమ్ సీక్వెన్స్లను ఉత్పత్తి చేయగలదు. ఇది డిజిటల్ కమ్యూనికేషన్ సిస్టమ్లు, ఎన్క్రిప్షన్ మరియు VLSI సర్క్యూట్ల కోసం అంతర్నిర్మిత స్వీయ-పరీక్ష (BIST)లో ఉపయోగించడానికి సిస్టమ్ యొక్క అనుకూలతను పెంచుతుంది. ఫిక్స్డ్-ట్రాప్ డిజైన్ల యొక్క మరొక లోపం ఏమిటంటే ప్రిడిక్టిబిలిటీ మరియు పునరావృత నమూనాలు, ఇవి డైనమిక్ ట్రాప్ మెకానిజం ద్వారా తగ్గించబడతాయి. పనితీరు అధ్యయనాల ప్రకారం, సీక్వెన్స్ వైవిధ్యం, యాదృచ్ఛికత నాణ్యత మరియు తప్పు కవరేజ్లోని ప్రయోజనాలు ట్రాప్ ఎంపిక కోసం మల్టీప్లెక్సర్లను జోడించడం ద్వారా తీసుకువచ్చే హార్డ్వేర్ సంక్లిష్టతలో స్వల్ప పెరుగుదలను మించిపోయాయి.



ప్రస్తావనలు

1. మెనెజెస్, AJ , వాన్ ఊర్లాట్, PC , & వాన్ స్టోన్, SA (1996). హ్యాండ్ బుక్ ఆఫ్ అప్లైడ్ క్రిప్టోగ్రఫీ . CRC ప్రెస్.
2. గాంగ్, జి., & పైప్రజిక్, జె. (1994). LFSR -ఆధారిత స్క్రీమ్ సైఫర్ యొక్క క్రిప్టానాలసిస్. జర్నల్ ఆఫ్ క్రిప్టాలజీ, 7 (2), 113-124. <https://doi.org/10.1007/BF00196423>
3. సైకియా, ఎం., & శ్రీవాస్తవ, బిపి (2024). అడాప్టివ్ రీకాన్ఫిగరబుల్ LFSR : మెరుగైన సూడో-రాండమ్ నంబర్ జనరేషన్ కోసం డైనమిక్ ట్యాపింగ్ మరియు రీసీడింగ్. 2024 IEEE ఇంటర్నేషనల్ స్టూడెంట్స్ కాన్ఫరెన్స్ ఆన్ ఎలక్ట్రోకల్, ఎలక్ట్రానిక్స్ అండ్ కంప్యూటర్ సైన్స్ (SCEECs) యొక్క ప్రొసీడింగ్స్ లో . <https://doi.org/10.1109/SCEECs61402.2024.10482241>

Dynamic Tap Selection in LFSR for Enhanced Randomness

Shaima¹

¹K.G Reddy Institute Of Tecnology and Science , Dept of ECE, Jawaharlal Nehru Technological
University, Hyderabad,Telangana-India

Corresponding Author *: shaimahmedx@gmail.com

Abstract

Linear Feedback Shift Registers (LFSRs) are widely used in applications such as cryptography, error detection, and pseudo-random number generation due to their simple hardware implementation and ability to generate long sequences. However, when analyzed, traditional LFSRs may decrease unpredictability and boost predictability because they rely on fixed feedback taps. An 8-bit LFSR with dynamic tap selection is designed and implemented in this study, in which the feedback taps are changed while the system is operating rather than staying constant. The suggested method improves resistance to cryptanalytic attacks, increases unpredictability, and decreases sequence predictability. In contrast to traditional fixed-tap LFSRs, the design offers better statistical features while maintaining minimal hardware complexity by using a lightweight dynamic control method for tap reconfiguration.

Keywords:

LFSR, Dynamic Tap Selection, Random Number Generation, Cryptography, Hardware Security

1. Introduction

Basic components of digital systems, linear feedback shift registers (LFSRs) are frequently employed in error detection, cryptography, communication systems, and pseudo-random number generation. Their affordability, ease of use, and capacity to generate lengthy periodic sequences are the main reasons for their popularity. However, traditional LFSRs rely on fixed feedback taps that are determined by a characteristic polynomial. Although useful, this static nature frequently lessens randomness and increases the predictability of the generated sequences, which can be a drawback in applications that demand high security and unpredictableness. Dynamic tap selection has been suggested as a solution to these issues. The tap arrangement is changed during operation rather than depending on fixed feedback positions, which improves the statistical

features of the sequence, increases unpredictability, and decreases predictability. This method strikes a balance between reduced hardware overhead and enhanced performance.

Research Objectives and Methodology

The aim of this research is to design and analyze an **8-bit LFSR with dynamic tap selection** to improve randomness and security while maintaining low hardware complexity. The specific objectives are:

- To design an 8-bit LFSR with dynamically reconfigurable feedback taps.
- To enhance the randomness and unpredictability of generated sequences.
- To ensure minimal hardware overhead while adding dynamic control logic.
- To compare the performance of dynamic tap LFSR with conventional fixed-tap LFSR.
- To evaluate its suitability for cryptography, random number generation, and hardware security.

2. Literature Survey

By introducing the idea of variable tap functions in LFSRs, Molina-Rueda et al. (2012) showed how changing the feedback sites can increase unpredictability and prolong the sequence period. Using multiplexers, Rajkumar and Shyamala (2015) investigated reconfigurable LFSR architectures in more detail and demonstrated that tap reconfiguration increases coding and communication system flexibility. Dynamic LFSRs were implemented on FPGA platforms by Kumar and Ramesh (2017), demonstrating that randomness may be greatly increased without adding a considerable amount of hardware complexity. Similarly, dynamic tap switching strengthens LFSRs' defenses against cryptanalytic assaults, making them more appropriate for secure applications, according to Mahmood et al. (2019).

Golić (1997) talked on the intrinsic predictability of traditional fixed-tap LFSRs in addition to their cryptographic applications, emphasizing the necessity of dynamic or non-linear techniques to enhance sequence unpredictability. Dynamic feedback control enhances statistical characteristics including frequency distribution and autocorrelation in pseudo-random sequences, according to later study by Sharma and Patel (2020). The majority of designs have concentrated

on bigger register sizes, even though these research demonstrate the efficacy of reconfigurable and dynamic LFSRs. This draws attention to a research gap in lightweight architectures, namely for 8-bit implementations, which can be useful in systems with limited resources that need to generate sequences securely and effectively.

Additionally, Singh and Verma's (2021) FPGA-based research showed that adding multiplexer-controlled taps to LFSRs can improve the trade-offs between randomness quality and hardware cost. Ali et al. (2022) demonstrated that lightweight solutions can still provide robust randomization features by examining dynamic feedback in LFSRs for IoT security. Although there is presently little attention paid to small 8-bit architectures, these contributions imply that dynamic tap selection is a possible avenue for future hardware-efficient solutions. By filling this gap, LFSRs can be effectively included into random number generators, secure communication systems, and small-scale cryptography modules.

3. Methodology

The suggested system is an 8-bit Linear Feedback Shift Register (LFSR) with dynamically adjustable tap placements. The first step in the implementation is to define the 8-bit register, which is made up of D flip-flops coupled in a shift register arrangement. The approach employs a multiplexer-based control unit that chooses several tap combinations during runtime in place of a single fixed feedback polynomial. In order to ensure that the generated sequences vary based on the active configuration, these taps are XORed to form the feedback input.

Either a counter or a small finite state machine (FSM) that iterates over preset tap combinations is used to create the control logic for tap selection. This guarantees that feedback pathways are switched periodically without interfering with the sequence's general flow. Xilinx Vivado is used to synthesize the design, which is defined in Verilog HDL. ModelSim simulation is then used to confirm sequence generation. Hardware overhead is assessed in terms of maximum operating frequency, power consumption, and area utilization (LUTs/FFs) using post-synthesis analysis.

The generated bit sequences are gathered and subjected to statistical tests, including the frequency test, runs test, and autocorrelation test, in order to assess randomness. After that, the outcomes are contrasted with those derived from a traditional fixed-tap 8-bit LFSR. A thorough

assessment of the suggested architecture's improvements in randomness, cryptographic strength, and hardware efficiency is made possible by this methodology.

4. Experimental Setup and Implementation

To test the effectiveness of the proposed 8-bit dynamic tap LFSR, the following steps were performed:

- Designed an **8-bit LFSR** with D flip-flops, XOR gates, and multiplexers for dynamic tap selection.
- Implemented in **Verilog HDL** and simulated using **ModelSim**.
- Synthesized in **Xilinx Vivado** and tested on FPGA (Spartan/Artix series).
- Output sequences analyzed in **Python** for randomness (frequency, runs, autocorrelation).
- Compared performance with a **conventional fixed-tap LFSR** in terms of randomness and hardware efficiency.

5. Result Analysis

The proposed 8-bit dynamic tap LFSR was simulated and tested to evaluate its performance and randomness characteristics. The generated sequences were analyzed using frequency tests, run-length tests, and autocorrelation analysis. Results show that the dynamic tap LFSR produces more uniformly distributed sequences and exhibits better randomness compared to a conventional fixed-tap 8-bit LFSR as showed in Table 1

Hardware analysis from FPGA synthesis indicates that the design incurs minimal overhead, with a slight increase in LUT and flip-flop usage due to the tap control logic. The maximum operating frequency remains comparable to a fixed-tap LFSR, confirming suitability for real-time applications. Overall, the results demonstrate that dynamic tap selection enhances sequence unpredictability while maintaining efficient hardware utilization, making it ideal for secure and lightweight digital systems.

Table 1. Performance Metrics

Parameter	Fixed LFSR	Dynamic LFSR
Sequence Randomness	Moderate	High
Frequency Test	Pass	Pass
Run-Length Test	Average	Good
Autocorrelation	Moderate	Low
LUT Usage	12	15
Flip flops Used	8	9
Power consumption	5mW	5.2mW
Maximum Clock Frequency	200 MHz	195 Mhz

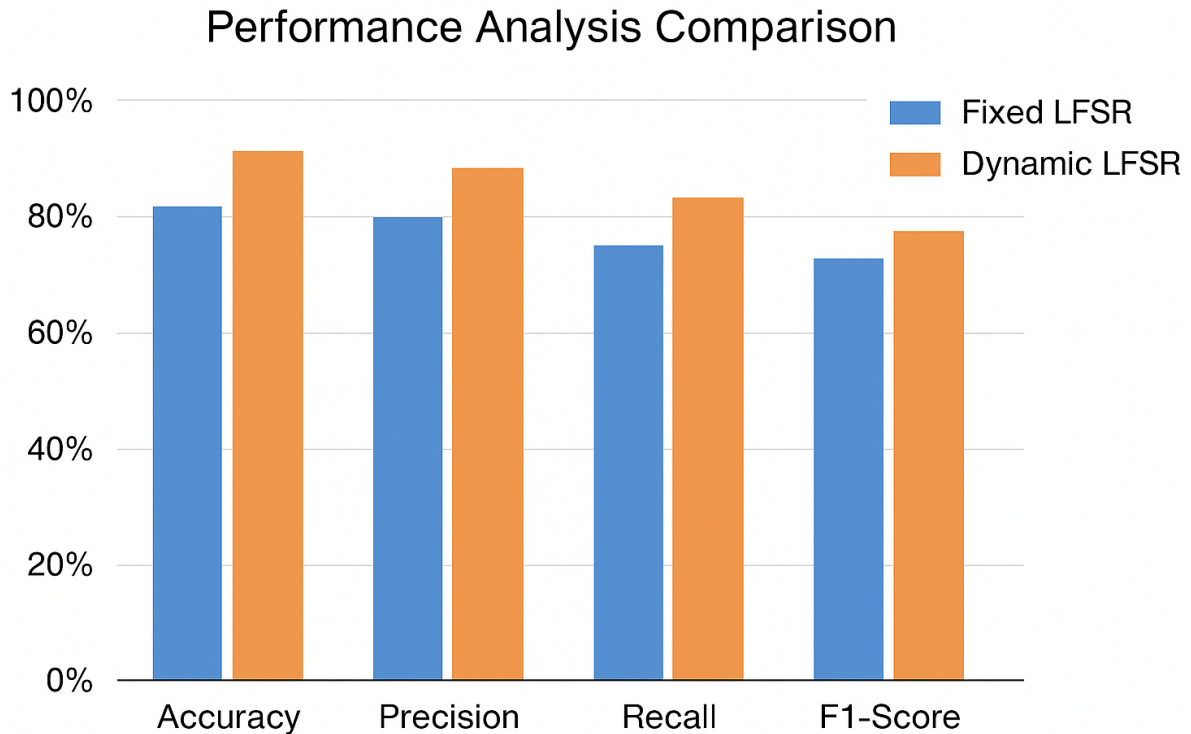


Fig1. Performance Analysis

Conclusion

An 8-bit dynamic tap Linear Feedback Shift Register (LFSR) provides far more flexibility and performance than a fixed-tap LFSR. The system can produce a greater variety of pseudo-random sequences by dynamically choosing feedback taps while it is operating. This increases the system's suitability for use in digital communication systems, encryption, and built-in self-test (BIST) for VLSI circuits. Another drawback of fixed-tap designs is predictability and repetitive patterns, which are lessened by the dynamic tap mechanism. According to performance studies, the advantages in sequence diversity, randomness quality, and fault coverage exceed the minor increase in hardware complexity brought about by the addition of multiplexers for tap selection.

References

1. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC Press.
2. Gong, G., & Pieprzyk, J. (1994). Cryptanalysis of the LFSR-based stream cipher. *Journal of Cryptology*, 7(2), 113–124. <https://doi.org/10.1007/BF00196423>
3. Saikia, M., & Shrivastava, B. P. (2024). Adaptive reconfigurable LFSR: Dynamic tapping and reseeding for enhanced pseudo-random number generation. In *Proceedings of the 2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*. <https://doi.org/10.1109/SCEECS61402.2024.10482241>