УНИВЕРЗИТЕТ У НОВОМ САДУ

**ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА У НОВОМ САДУ**

**Немања Газивода**

# НОВА МЕТОДА ЗА ПОВЕЋАЊЕ ЕФЕКТИВНЕ РЕЗОЛУЦИЈЕ СТОХАСТИЧКИХ МЕРНИХ ИНСТРУМЕНАТА ВИСОКИХ ПЕРФОРМАНСИ

- Докторска дисертација -

ментор:
проф. др Драган Пејић

Нови Сад, 2019. године

УНИВЕРЗИТЕТ У НОВОМ САДУ ● **ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА**
21000 НОВИ САД, Трг Доситеја Обрадовића 6

# КЉУЧНА ДОКУМЕНТАЦИЈСКА ИНФОРМАЦИЈА

| | |
|---|---|
| Редни број, **РБР**: | |
| Идентификациони број, **ИБР**: | |
| Тип документације, **ТД**: | Монографска документација |
| Тип записа, **ТЗ**: | Текстуални штампани материјал |
| Врста рада, **ВР**: | Докторска дисертација |
| Аутор, **АУ**: | Немања Газивода |
| Ментор, **МН**: | Др Драган Пејић, ванредни професор |
| Наслов рада, **НР**: | Нова метода за повећање ефективне резолуције стохастичких мерних инструмената високих перформанси |
| Језик публикације, **ЈП**: | Српски (ћирилица) |
| Језик извода, **ЈИ**: | Српски |
| Земља публиковања, **ЗП**: | Србија |
| Уже географско подручје, **УГП**: | Војводина |
| Година, **ГО**: | 2019. |
| Издавач, **ИЗ**: | Факултет техничких наука |
| Место и адреса, **МА**: | Нови Сад, Трг Доситеја Обрадовића 6 |
| Физички опис рада, **ФО**: | 10 поглавља/111 страна/71 цитата/4 табеле/53 слике/ - /2 прилога |
| Научна област, **НО**: | Електротехничко и рачунарско инжењерство |
| Научна дисциплина, **НД**: | Електрична мерења |
| Предметна одредница/Кључне речи, **ПО**: | Стохастичка дигитална мерна метода, дитерски сигнали, псеудослучајни генератори бројева, истински случајни генератори бројева, метода, ефективна резолуција,мерна несигурност, |
| **УДК** | Монографска документација |
| Чува се, **ЧУ**: | Библиотека Факултета техничких наука, Универзитет у Новом Саду |
| Важна напомена, **ВН**: | |
| Извод, **ИЗ**: | . Дисертација истражује утицај примене дитерског сигнала (дискретног аналогног униформног шума) генерисаног новом методом на повећање ефективне резолуције мерних инструмената базираних на стохастичкој дигиталној мерној методи. У дисертацији је дат преглед досадашњих решења базираних на стохастичкој дигиталној мерној методи у циљу сагледавања потребе и оправданости истраживања. Предложено решење представља комбинацију псеудослучајног и истински случајног генератора и као такво задржава најбоље особине из обе области. Дат је предлог нове методе генерисања шума униформне расподеле амплитуда. Уместо уобичајеног начина генерисања коришћењем генератора псеудослучајних бројева и Д/А конвертора, овде се предлаже генерисање засновано на неуниформном одабирању тестерастог или троугаоног напона. Осим уштеде због некоришћења Д/А конвертора, добит је и могућност генерисања напона из континуалног, уместо дискретног скупа амплитуда. Већина данашњих хардверских генератора псеудослучајног напона, се базира на употреби микроконтролера и Д/А конвертора, па је на тај начин резолуција генерисања псеудослучајног напона ограничена резолуцијом Д/А конвертора. Одабирањем тестерастог или троугаоног напона предложеном методом се остварује готово неограничена резолуција. Употреба овако генерисаног дитерског сигнала доводи до повећања ефективне резолуције код стохастичких мерних инстурмената. Симулацијом је одређена оптимална структура генератора на основу предложене методе. Експериментална мерења су изведена помоћу развијеног прототипа хардверског генератора. |

| | | | |
|---|---|---|---|
| Датум прихватања теме, **ДП**: | | 31.01.2019. | |
| Датум одбране, **ДО**: | | | |
| Чланови комисије, **КО**: | Председник: | др Платон Совиљ, ванредни професор | |
| | Члан: | др Драган Ковачевић, научни саветник | |
| | Члан: | др Зоран Митровић, редовни професор | Потпис ментора |
| | Члан: | др Марјан Урекар, доцент | |
| | Члан, ментор: | др Драган Пејић, ванредни професор | |

UNIVERSITY OF NOVI SAD ● **FACULTY OF TECHNICAL SCIENCES**
21000 NOVI SAD, Trg Dositeja Obradovića 6

# KEY WORDS DOCUMENTATION

| | |
|---|---|
| Accession number, **ANO**: | |
| Identification number, **INO**: | |
| Document type, **DT**: | Monographic publication |
| Type of record, **TR**: | Printed textual material |
| Contents code, **CC**: | Ph. D. thesis |
| Author, **AU**: | Nemanja Gazivoda |
| Mentor, **MN**: | Ph.D. Dragan Pejić, Associate Professor |
| Title, **TI**: | A Novel Method for increasing the Effective Resolution of High Performance Stochastic Measuring Instruments |
| Language of text, **LT**: | Serbian |
| Language of abstract, **LA**: | English |
| Country of publication, **CP**: | Republic of Serbia |
| Locality of publication, **LP**: | Vojvodina |
| Publication year, **PY**: | 2019. |
| Publisher, **PB**: | Faculty of Technical Sciences |
| Publication place, **PP**: | Novi Sad, Trg Dositeja Obradovića 6 |
| Physical description, **PD**: | 10 chapters/111 pages/71 ref./4 tables/53 pictures/ - /2 appendixes |
| Scientific field, **SF**: | Electrical and Computer Engineering |
| Scientific discipline, **SD**: | Electrical Measurements |
| Subject/Key words, **S/KW**: | Stochastic Digital Measurement Method, Dither signals, Pseudorandom Number Generators, True Random Number Generators, Method, Effective Resolution, Measurement Uncertainty |
| **UC** | Monographic documentation |
| Holding data, **HD**: | Library of the Faculty of Technical Sciences, University of Novi Sad |
| Note, **N**: | |
| Abstract, **AB**: | The dissertation investigates the impact of the application of the dithering signal (discrete analogue uniform noise) generated by the new method for increasing the effective resolution of measurement instruments based on the stochastic digital measurement method. The dissertation provides an overview of the existing solutions based on the stochastic digital measurement method in order to understand the need and justification of the research. The proposed solution represents a combination of a pseudorandom and truly random generator and as such holds the best features in both areas. A suggestion of a new way of generating the noise of the uniform distribution of amplitudes is presented. Instead of the usual way of generating using a pseudorandom number generator and a D/A converter, the generation based on the nonuniform sampling of sawtooth or triangle voltage is proposed. In addition to the savings due to the non-use of a D/A converter, the possibility of generating voltages from a continual instead of a discrete amplitude set is also obtained. Most of today's hardware pseudorandom voltage generators are based on the use of a microcontroller and D/A converter, so in this way the resolution of the pseudorandom voltage generation is limited by the resolution of the D/A converter. By sampling the sawtooth or triangle voltage using the proposed method, almost unlimited resolution is achieved. The use of this generated dither signal leads to an increase in effective resolution in stochastic measuring instruments. The simulation determined the optimal structure of the generator based on the proposed method. Experimental measurements were made using developed hardware. |

| | | | |
|---|---|---|---|
| Accepted by the Scientific Board on, **ASB**: | | 31.01.2019. | |
| Defended on, **DE**: | | | |
| Defended Board, **DB**: | President: | PhD Platon Sovilj, associate professor | |
| | Member: | PhD Dragan Kovačević, scientific advisor | |
| | Member: | PhD Zoran Mitrović, full professor | Mentor's sign |
| | Member: | PhD Marjan Urekar, assistant professor | |
| | Member, Mentor: | PhD Dragan Pejić, associate professor | |

# САДРЖАЈ

# Изјава захвалности

Посебну захвалност дугујем свом ментору др Драгану Пејићу на стрпљивости, подршци, помоћи, разумевању и пажњи са којом је учествовао у изради ове дисертације.

# СПИСАК ТАБЕЛА



# СПИСАК СЛИКА

# СПИСАК СЛИКА - НАСТАВАК

# СПИСАК СЛИКА - НАСТАВАК

# СПИСАК СЛИКА - НАСТАВАК

# 1. УВОД

У данашње време мерни инсрументи и опрема су углавном дигитални. Временски континуални сигнали се одабирају и конвертују у дискретне, дигиталне величине. У процесу конверзије из аналогне у дигиталну величину тачност и брзина су два међусобно супротстављена захтева. Један од значајнијих проблема у теорији и пракси метрологије (науке о мерењима) у прошлости је представљало тачно мерење изобличених сигнала мале амплитуде у присуству шума. Овај проблем је присутан и данас.

Стохастичка дигитална мерна метода (СДММ) је развијена на Катедри за електрична мерења деведесетих година прошлог века. Ову методу карактерише једноставан хардвер: сабирање и множење се реализују И и ИЛИ логичким колима, интеграљење коришћењем бројача. Да би могао да се користи овако једноставан хардвер за обављање рачунских операција, неопходно је имати операнде у облику поворке импулса. Средња вредност поворке импулса, иначе сразмерна вероватноћи појаве јединица, носи информацију о величини над којом се жели вршити рачунање. Да би се стохастичко рачунање могло применити и на улазне аналогне величине, неопходно је извршити претварање аналогне величине у поворку импулса. Стохастички аналогни А/Д (аналогно-дигитални) конвертор врши претварање аналогне информације у поворку импулса уз поређење са помоћним напоном (дитером) - шумом униформне расподеле амплитуда.

Шумове из природних извора карактерише континуалност у времену и континуалност по амплитуди, нажалост ови шумови немају тражену униформну расподелу. Други пример су вештачки генерисани шумови код којих се користе псеудослучајни генератори бројева униформне расподеле у спрези са Д/А (дигитално-аналогним) конвертором. На излазу Д/А конвертора се добија напон униформне расподеле амплитуда; напон је дискретан у времену (одређен временом постављања

(settling time) Д/А конвертора) и дискретан по амплитуди (одређен резолуцијом Д/А конвертора). Иако је генерисање псеудослучајног броја униформне расподеле врло изучавана област, мало је решења која су лако хардверски изводива. Углавном се заснивају на Linear Feedback Shift Register - LFSR (померачким регистрима са линеарном повратном спрегом), којима се добија секвенца коначне дужине и који су у потпуности предвидиви. Поред особина LFSR структуре, на перформансе добијеног псеудослучајног напона у извесној мери утичу и ограничења Д/А конвертора (резолуција, стабилност, монотоност, опсег, итд...).

Начини генерисања униформног шума у радовима из ове области [1-3] су засновани на коришћењу LFSR структуре без Д/А конвертора. Врши се усредњавање импулса коришћењем нискофреквентног (НФ) филтера ради добијања напонског сигнала. Расподела амплитуда након НФ филтера није униформна, него је приближно нормална. Различитим поступцима се врши мењање средње вредности нормалне расподеле ради добијања напона униформне расподеле. Примена НФ филтера за усредњавање и уобличавање је врло једноставно и јефтино решење. Недостатак је потреба за врло великом фреквенцијом у дигиталном делу, у односу на фреквенцију којом се могу очитавати генерисани напони униформне расподеле амплитуда.

У радовима се углавном подразумева шум униформне расподеле (дитер, енглески - dither) [4], уз претпоставку да је идеалних особина. Јасно је да од квалитета овог шума директно зависи квалитет конверзије аналогне у стохастичку величину.

Циљ ове дисертације јесте ***формулисање нове методе генерисања шума униформне расподеле вредности амплитуда, која је заснована на неуниформном одабирању тестерастог континуалног напона.***

***Хипотеза ове тезе гласи: предложена метода генерисања униформног шума (дитера) омогућава добијање континуалног уместо дискретног скупа вредности апмлитуда приближно униформне расподеле, што резултује повећањем ефективне резолуције инструмената базираних на стохастичкој дигиталној мерној методи.***

# ПРЕГЛЕД ПОГЛАВЉА

- Прво поглавље је увод у којем је изложена тема којом се бави дисертација и постављена је хипотеза.

- Друго поглавље представља преглед стохастичке дигиталне мерне методе. Описане су предности мерења на интервалу у односу на мерење у тачки. Дат је преглед до сада развијених метода заснованих на стохастичкој дигиталној мерној методи.

- Треће поглавље даје дефиницију ефективне резолуције стохастичких мерних инструмената и приказује анализу утицаја систематске грешке, коначне резолуције Д/А конвертора којим се генерише дитерски сигнал, на грешку мерења.

- У четвртом поглављу је објашњен значај употребе дитерских сигнала у мерењу стохастичким мерним инструментима. Дат је приказ најзначајнијих метода за реализацију псеудослучајних и истински случајних генератора шума.

- У петом поглављу је дат предлог нове методе за генерисање дискретног аналогног униформног шума.

- У шестом поглављу је описан развијени симулациони модел и приказана је анализа резултата добијених симулацијом.

- У седмом поглављу је презентован начин валидације симулационог модела и приказани су добијени резултати.

- Осмо поглавље представља рекапитулацију рада.

- Девето поглавље је закључак.

- Десето поглавље приказује списак коришћене литературе.

- Прилози на крају тезе: преглед статистичких тестова у оквиру NIST софтверског пакета и првобитно хардверско решење генератора дискретног аналогног униформног шума.

# 2. ПРЕГЛЕД СТОХАСТИЧКЕ ДИГИТАЛНЕ МЕРНЕ МЕТОДЕ И РЕШЕЊА БАЗИРАНИХ НА ЊОЈ

## 2.1 Мерење у тачки

У свету се данас, када се говори о стандардном дигиталном мерењу, подразумева мерење у тачки, односно мерење стандардном семплинг методом [5].

Стандардна семплинг метода је базирана на трансформацији континуалног аналогног сигнала у дискретни дигитални сигнал одабирањем у еквидистантним временским интервалима.

При употреби методе мерења у тачки се јављају два извора систематске грешке. То су дискретизација по времену и дискретизација по амплитуди улазног сигнала [6]. Уколико су притом задовољени услови Никвист-Шенонове теореме о одабирању (семповању) грешка услед дискретизације по времену се може занемарити као узрок систематске грешке мерења [7-8]. Међутим дискретизацију по амплитуди није могуће у потпуности елиминисати и она увек представља узрок систематске грешке мерења.

Стандардна семплинг метода подразумева одабирање континуалног аналогног сигнала А/Д конвертором у практично бесконачно кратком временском интервалу $\Delta t$ и његово претварање у дискретну вредност. Уколико се учестаност одабирања улазног сигнала обележи са $f_s$ а највиша учестаност у оквиру улазног сигнала са $f_{MAX}$ онда следи:

$$f_s = \frac{1}{\Delta t} = 2 f_{MAX} \qquad (2.3.1.3)$$

Тренд развоја технологије мерења је последњих деценија био везан за стандардну семплинг методу. Ту се пре свега мисли на развој линеарних А/Д конвертора високе резолуције.

Овај добро познати концепт је магистрала у развоју, не само у области мерења, него и телекомуникација, управљања, енергетске електронике и других [9].

Најбржи А/Д конвертори су флеш А/Д конвертори код којих је $\Delta t$ око 1 ns. Проблем флеш А/Д конвертора је мала резолуција. Пораст резолуције (максимална је на нивоу од 10 бита) прати и значајан пораст мерне несигурности. Са порастом резолуције од једног бита хардвер флеш А/Д конвертора се дуплира.

Може се закључити да су спори А/Д конвертори тачни и прецизни а да су брзи А/Д конвертори нетачни и непрецизни.

Проблеми при мерењу у тачки настају код мерења на високим учестаностима, као и при мерењу сигнала у присутству шума.

За ефикасну примену методе мерења у тачки је такође било потребно обезбедити и брзу и ефикасну обраду дискретних дигиталних вредности сигнала на излазу из А/Д конвертора. Ово је постигнуто применом брзих дигиталних сигнал процесора (ДСП).

Закључак је да је у мерењима у тачки методологија исцрпљена, а да остаје само напредак у технологији [6].

## 2.2 Мерење на интервалу

Насупрот претходно описаном мерењу у тачки јавља се појам мерења на интервалу. Мерењем на интервалу коначне временске дужине могу да се елиминишу ограничења мерења у тачки и да се задржи већина његових предности. Предности мерења на интервалу се пре свега односе на могућности мерења сигнала високих учестаности, затим сигнала у присутству шума и на високу линеарност и тачност мерења.

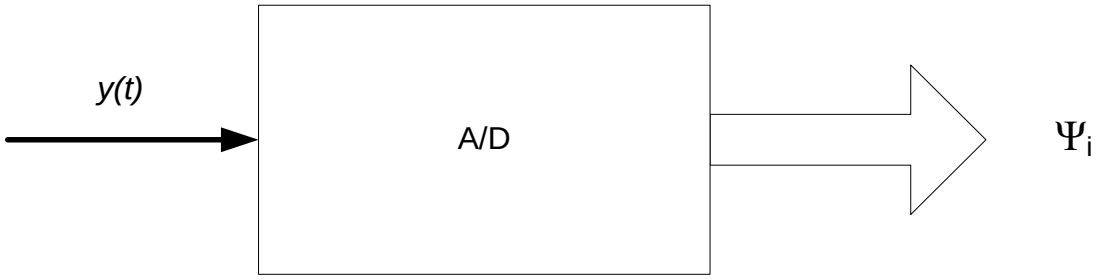
У мерењима на интервалу се примењују брзи флеш А/Д конвертори мале резолуције. То са собом повлачи врло велику грешку квантизације. Како би се ова грешка свела на најмању могућу меру улазном сигналу се додаје униформни шум средње вредности 0 у опсегу једног кванта примењеног флеш А/Д конвертора (дитер) и тада он ефективно постаје стохастички флеш А/Д конвертор. Стандардна девијација грешке квантизације тада опада са квадратним кореном броја одмерака у одговарајућем интервалу мерења.

У мерењима на интервалу је осим мерења средње вредности могуће мерити и ефективну вредност улазног сигнала. Тада се мерни блок мора проширити још једним флеш А/Д конвертором, још једним генератором дитера, множачем и акумулатором. Потребно је обезбедити да дитерски сигнали буду међусобно некорелисани, и ако се на канале оба А/Д конвертора доведе исти сигнал, средња вредност садржаја акумулатора је тада једнака квадрату ефективне вредности мерене величине на интервалу. Стандардна девијација грешке квантизације задовољава услове Централне граничне теореме и Теорије узорака. Показује се да је стандардна девијација грешке обрнуто пропорционална квадратном корену броја одмерака на интервалу и да се за веома велики број одмерака може постићи да грешка мерења ефективне вредности улазног сигнала буде врло мала.

## 2.3 Стохастичка дигитална мерна метода

У току дугогодишњег истраживачког и научног рада на Катедри за електрична мерења је развијена стохастичка дигитална мерна метода (СДММ) као практична реализација мерења на интервалу. Основа СДММ је метода А/Д конверзије базирана на стохастичкој адиционој А/Д конверзији (САДК). Ова мерна метода представља нов приступ мерењима на електродистрибутивној мрежи и развијана је независно од степена развоја технологије електронских компоненти потребних за њену реализацију.

Код мерења класичном мерном инструментацијом грешка мерења се готово на исти начин пропагира преко целог мерног опсега [6]. Ово је карактеристика класичног А/Д конвертора односно униформног квантизера. Слика 2.3.1 приказује упрошћен блок класичног А/Д конвертора.




**Слика 2.3.1 Приказ класичног А/Д конвертора**

Улога квантизера је пресликавање континуалног скупа аналогних улазних вредности сигнала *y(t)* у дискретни скуп дигиталних вредности $\Psi_i$ на излазу. Ако квантизер има *N* прагова одлучивања, где је сваки посебни праг $p_i$, и важи $0 \leq i \leq N$ и уколико су прагови еквидистантни, односно $p_i - p_{i-1} = const.$ за све вредости, ради се о униформном квантизеру. Уколико се са *N* означи број излазних нивоа квантизера а са *B* број бита по одмерку онда је:

$$N = 2^B \tag{2.3.1}$$

Може се закључити да се употребом већег броја бита за представљање одмерка повећава и број излазних нивоа *N* [10]. На овај начин се смањује грешка квантизације, што као резултат на излазу квантизера даје дискретни дигитални сигнал који представља тачнију репрезентацију улазне континуалне вредности.

Такође се може дефинисати и битски проток у секунди квантизованог сигнала *br* (bit rate) једначином:

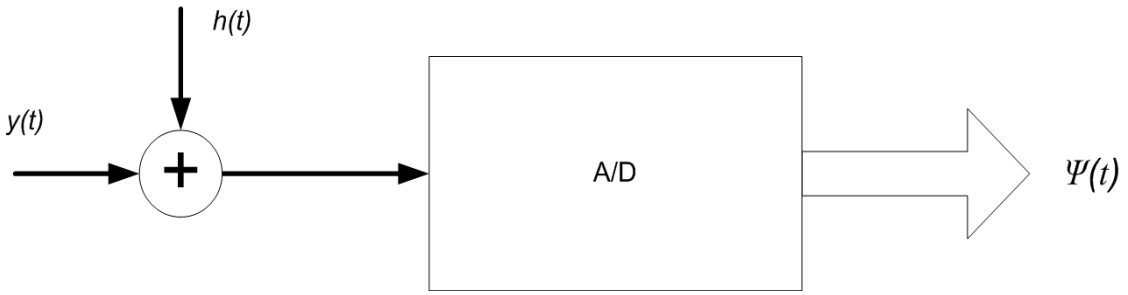
$$br = f_S \cdot B \tag{2.3.2}$$

где $f_S$ представља учестаност одабирања улазног сигнала а $B$ број бита по одмерку.

Код описаног А/Д конвертора грешка квантизације има униформну расподелу на целом опсегу мерених вредности. Дакле прецизност А/Д конвертора зависи од величине кванта. На основу тога се може закључити да мале вредности амплитуде улазног сигнала доводе до повећане непрецизности. Овај проблем се може превазићи повећањем резолуције (броја бита) А/Д конвертора. Међутим повећањем резолуције се смањује квант А/Д конвертора и он постаје осетљив на утицај шума, што доводи до смањивања прецизности конверзије, тиме смањујући ефективну резолуцију А/Д конвертора.

Из претходно поменутог произилази да се са повећањем резолуције А/Д конвертора повећава комплексност саме изведбе А/Д конвертора али и намећу високи захтеви ка дигиталном блоку за обраду (микропроцесору или ДСП-у) због повећаног протока података на излазу А/Д конвертора. Ово доводи до незанемарљивог усложњавања осталих компоненти система и на крају високе цене уређаја базираних на оваквим решењима.

### 2.3.1 Математички модел СДММ




**Слика 2.3.1.1 Флеш А/Д конвертор са збиром улазног сигнала и дитера**

Елементи уређаја приказаног на Слици 2.3.1.1 су:

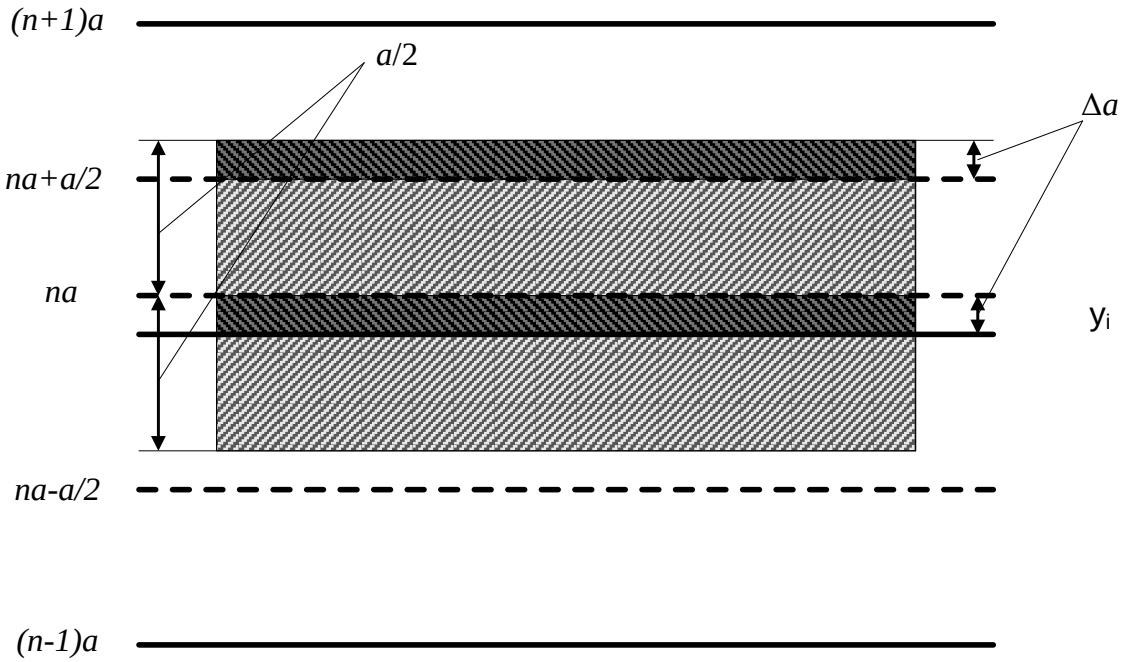
- аналогни сабирач и
- униформни квантизер ( флеш А/Д конвертор).

На улаз квантизера се доводи збир улазног напона *y(t)* и дитерског сигнала *h(t),* који мора одговарати улазном напонском опсегу квантизера. Ако се усвоји да је дитерски сигнал случајан и да има униформну расподелу онда важи:

$$p(h) = \frac{1}{a}, |h| \le \frac{a}{2} \qquad (2.3.1.1)$$

где *a* представља квант униформног квантизера, а *p(h)* функцију густине расподеле вероватноће дитерског сигнала [11].

Анализирајмо случај приказан на слици 2.3.1.2, када се на улаз аналогног сабирача доводи непроменљив напон $y(t) = y$, такав да се налази између *n*-тог и *(n+1)*-вог квантног нивоа ($na \le y \le (n+1)a$).




**Слика 2.3.1.2 Дитерски сигнал униформне расподеле суперпониран улазном напону**

Пуним линијама су означени квантни нивои *(n-1)a*, *na* и *(n+1)a*, а испрекиданим линијама прагови одлучивања *na-a/2* и *na+a/2* који представљају границе напона које се у процесу А/Д конверзије додељују квантном нивоу *na*. Ово се чини на такав начин да случајна променљива $\Psi$ поприма вредности $\Psi_1=(n+1)a$ када је сума напона и дитера већа од прага *na+a/2*, odnosno $\Psi_2=na$, када је сума мања од истог прага. Ако се са $\Delta a$ обележи растојање до најближег квантног нивоа, може се формулисати израз за средњу вредност променљиве $\Psi$:

$$\bar{\psi} = \psi_1 \cdot p_1 + \psi_2 \cdot p_2 = (n+1)a \cdot \frac{|\Delta a|}{a} + na \cdot \frac{a - \Delta a}{a} = na + \Delta a = y \qquad (2.3.1.2)$$

Уведене ознаке $p_1$ и $p_2$, које представљају вероватноће да функција $\Psi$ поприма вредности $\Psi_1$ и $\Psi_2$, респективно су одређене графичким путем.

Средња вредност (математичко очекивање) излаза из квантизера, на чијем улазу се налази дитеровани једносмерни напон *y* је управо једнака мереној вредности. Грешка квантизације је у потпуности уклоњена. Међутим треба нагласити да се до оваквог резултата дошло на основу бесконачно много мерења и усредњавања резултата. Грешка случајне променљиве $\Psi$ се обично изражава њеном средњом квадратном грешком или стандардном девијацијом.

$$\overline{e^2} = \sigma^2{}_\Psi = (\Psi_1 - \overline{\Psi})^2 \cdot p_1 + (\Psi_2 - \overline{\Psi})^2 \cdot p_2 = (a - |\Delta a|)^2 \cdot \frac{|\Delta a|}{a} + |\Delta a|^2 \cdot \frac{a - \Delta a}{a} \quad (2.3.1.3)$$
$$\sigma^2{}_\Psi = (a - |\Delta a|) \cdot |\Delta a|$$

Уколико се при мерењу узме коначан број дитерованих одмерака улазног сигнала податак о грешци мерења даје теорија узорака и централна гранична теорема.

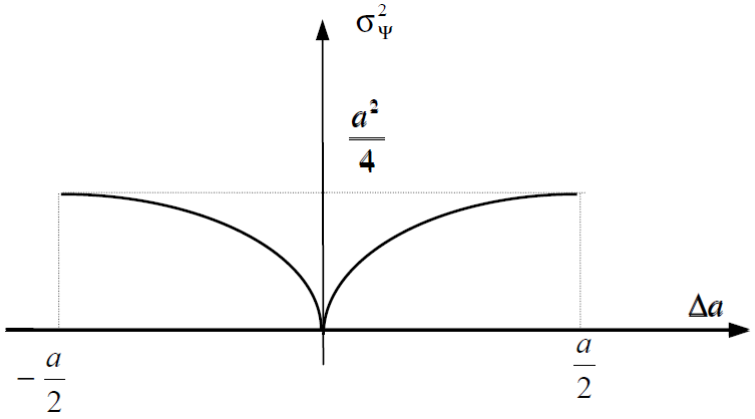
Ако се у обзир узме скуп одмерака $\Psi_1$, $\Psi_2$,..., $\Psi_N$ и уколико се одмерци узимају независно тада је мерена вредност исказана средњом вредношћу:

$$\overline{\Psi} = \frac{1}{N}\sum_{i=1}^{N} \Psi_i \approx y \quad (2.3.1.4)$$

На дати скуп одмерака се може применити централна гранична теорема, по којој $\overline{\Psi}$ има Гаусову расподелу, при чему је варијанса од $\overline{\Psi}$ :

$$\sigma^2{}_{\overline{\Psi}} = \frac{\sigma^2{}_\Psi}{N} \quad (2.3.1.5)$$

Једначине (2.3.1.3), (2.3.1.4) и (2.3.1.5) у потпуности описују ситуацију када се узима коначан број дитерованих одмерака улазног сигнала.



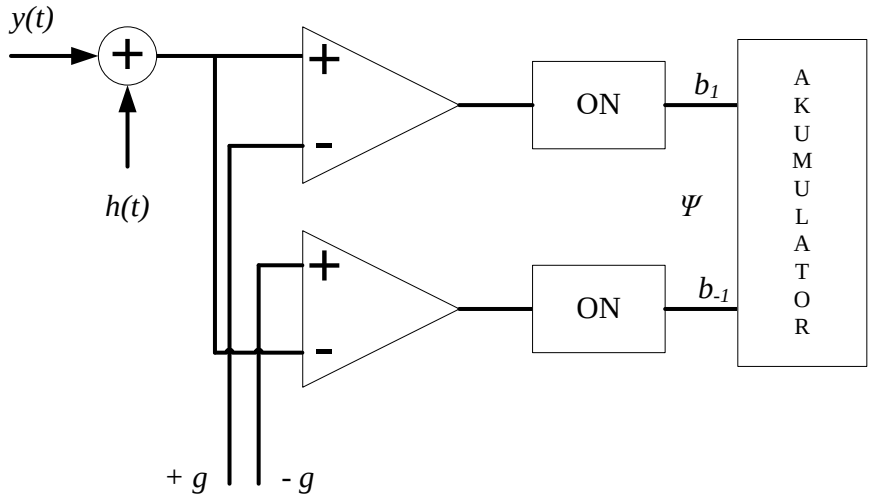

**Слика 2.3.1.3 Зависност варијансе излаза А/Д конвертора од растојања до најближег квантног нивоа**

На основу слике 2.3.1.3 се може закључити да је грешка мерења најмања када се мерени напон поклапа са квантним нивоом, а највећа када је $|\Delta a|=a/2$ (када се мерени напон поклапа са прагом одлучивања.

### 2.3.2 Стохастички адициони флеш А/Д конвертор са једним генератором дитерског сигнала (САДК1Г)

У претходно разматраном математичком моделу није био наведен конкретан број квантних нивоа, те изведене релације важе за произвољан број квантних нивоа.

Најосновнија хардверска примена СДММ је у двобитном стохастичком адиционом флеш А/Д конвертору са једним генератором дитера (САДК1Г), чија блок шема је приказана на слици 2.3.2.1.




**Слика 2.3.2.1 Блок шема САДК1Г**

САДК1Г има три квантна нивоа:

- *2g*,
- 0 и
- *-2g*,

где је $2g=a$ и при чему важе услови:

$$\begin{aligned} &|y+h| \le 3g \\ &|y| \le 2g \\ &p(h) = \frac{1}{2g} \\ &|h| \le g \end{aligned} \qquad (2.3.2.1)$$

Функција $\Psi$ представља излаз САДК1Г и дефинисана је као:

$$\Psi = (b_1 - b_{-1}) \cdot 2g \tag{2.3.2.2}$$

Вредности $b_1$ и $b_{-1}$ су излази два компаратора који чине саставни део двобитног флеш А/Д конвертора и њихове вредности су одређене скупом {0,1}, уз изузетак да важи: $-b_1 \cdot b_{-1} \neq 1$ (не могу оба излаза у исто време бити јединице). $+g$ и $-g$ представљају напонске прагове компаратора. Из (2.3.2.1) се види да је дефинисани квант униформног квантизера $a=2g$, који у ствари представља и квант целокупног стохастичког адиционог флеш А/Д конвертора. ON блокови представљају лимитере напонског нивоа којима се излазни напони компаратора прилагођавају напонским нивоима логичких кола која се користе за даљу обраду дигиталног сигнала.

Из досадашњег разматрања произилази да сигнал на улазу у САДК1Г мора бити константан и временски непроменљив. Међутим показало се да се на улаз САДК1Г може довести и временски променљив сигнал (периодичан и стационаран током једне периоде мерења).

Уколико је $y=f(t)$, посматрањем излаза САДК1Г - $\Psi$ у временском интервалу $t \in [t_1, t_2]$ долази се до неколицине закључака [11].

Средња вредност функције $y=\varphi(t)$ у интервалу $t \in [t_1, t_2]$ , где је $\varphi(t)$ интеграбилна функција је иста без обзира да ли је $t$ детерминистичка променљива или случајна променљива униформне расподеле $p(t) = \frac{1}{t_2 - t_1}$ и износи $\overline{y} = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} \varphi(t) dt$ .

Када је $t$ случајна променљива униформне расподеле $p(t) = \frac{1}{t_2 - t_1}$ , тада је и $y$ случајна променљива у функцији времена $t$.

$$\overline{y} = \int_{-\infty}^{+\infty} y \cdot p(y) dy = \int_{-\infty}^{+\infty} y \cdot dP_y \tag{2.3.2.3}$$

Функција *p(y)* представља функцију густине расподеле вероватноће случајне промењљиве *y*, а $dP_x$ елементарну вероватноћу-диференцијал функције расподеле вероватноће случајне промењљиве *y*. Из констатације да је *y* зависно од *t* следи:

$$dP_y = dP_{y/t} \cdot dP_t = p(y/t) \cdot p(t) \cdot dy \cdot dt \tag{2.3.2.4}$$

Узимајући у обзир Дираков делта импулс δ може се закључити да је:

$$\begin{aligned} p_{\Psi/t}(\Psi) &= \delta\left[\Psi - f(t)\right] \\ p(t) &= \frac{1}{t_2 - t_1} = \frac{1}{T} \end{aligned} \tag{2.3.2.5}$$

Одавде се средња вредност *y* може написати као:

$$\begin{aligned} \overline{y} &= \int_{t_1}^{t_2}\int_{-\infty}^{+\infty} y \cdot \delta\left[y - \varphi(t)\right] \cdot \frac{1}{t_2 - t_1} \cdot dt \cdot dy \\ \overline{y} &= \frac{1}{t_2 - t_1} \cdot \int_{t_1}^{t_2} dt \int_{-\infty}^{+\infty} y \cdot \delta\left[y - \varphi(t)\right] \cdot dy \\ \overline{y} &= \frac{1}{t_2 - t_1} \cdot \int_{t_1}^{t_2} \varphi(t)dt \end{aligned} \tag{2.3.2.6}$$

Средња вредност (математичко очекивање) $\overline{\Psi}$ излаза $\Psi$ из САДК1Г у временском интервалу $t \in [t_1, t_2]$ је дата изразом:

$$\overline{\Psi} = \frac{1}{t_2 - t_1}\int_{t_1}^{t_2} f(t)dt \tag{2.3.2.7}$$

Стандардна девијација (средња квадратна грешка) излаза $\Psi$ у временском интервалу $t \in [t_1, t_2]$ је дата изразом:

$$\overline{e^2} = \sigma^2 = \frac{2g}{t_2 - t_1}\int_{t_1}^{t_2} \left|f(t)\right| dt - \left[\frac{1}{t_2 - t_1}\int_{t_1}^{t_2} f(t)dt\right]^2 \tag{2.3.2.8}$$

Трећи централни момент расподеле случајне величине $\Psi$ је ограничен и он представља довољан услов за примену централне граничне тереме и теорије узорака.

$$\overline{\Psi^3} = \frac{(2g)^2}{t_2 - t_1} \int_{t_1}^{t_2} f(t)dt = (2g)^2 \cdot \overline{\Psi} \qquad (2.3.2.9)$$

Примена САДК1Г је ограничена на једносмерне и споропроменљиве улазне сигнале (стационарне током једне периоде мерења). Његова главна предност је једноставан хардвер који пружа могућност једноставне имплементације у паралелним (вишеканалним) мерењима.

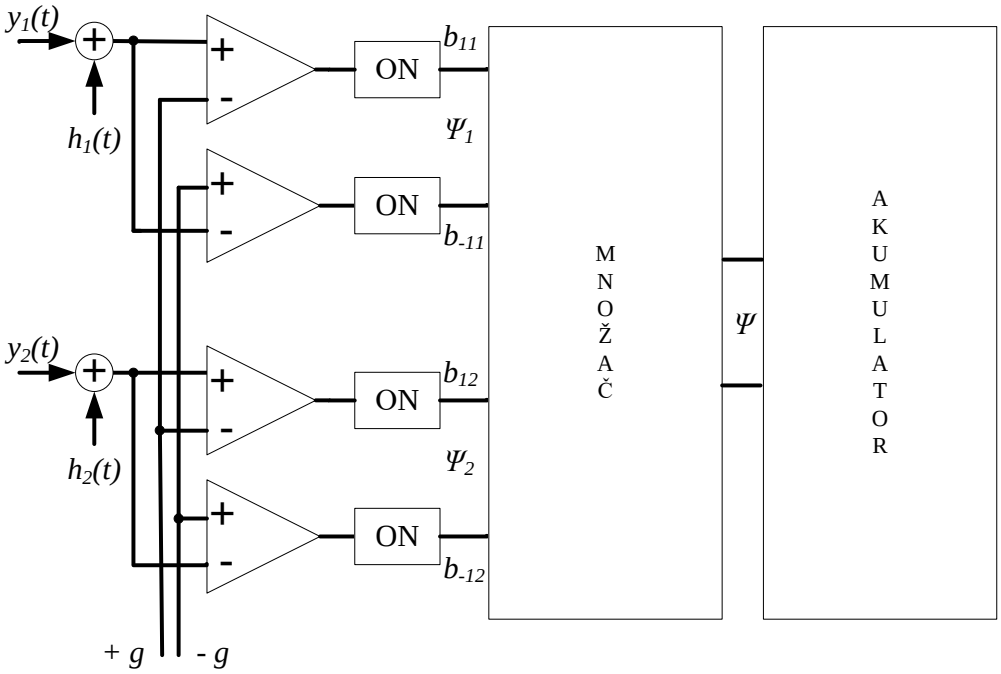
### 2.3.3 Стохастички адициони флеш А/Д конвертор са два генератора дитерског сигнала (САДК2Г)

Двобитни стохастички адициони флеш А/Д конвертор са два генератора дитера (САДК2Г) се састоји од два САДК1Г, множача и акумулатора.

На улазе оба САДК1Г се доводи збир улазних сигнала и дитера $y_1(t)+h_1(t)$ и $y_2(t)+h_2(t)$. Излазни сигнали са оба САДК1Г, $\Psi_1$ и $\Psi_2$, се воде на улаз множача који по завршетку операције множења ова два сигнала генерише $\Psi$ које управља радом акумулатора. Акумулатор је реализован као *up-down* бројач. То значи да врши бројање навише за $\Psi=1$, не мења стање за $\Psi=0$ и броји наниже за $\Psi=-1$.

Додатни услов у односу на већ постављене услове за сигнале код САДК1Г је да дитерски сигнали $h_1$ и $h_2$ морају бити некорелисани.

Овако реализовани стохастички мерни инструмент мери средњу вредност производа два сигнала на коначном временском интервалу.




**Слика 2.3.3.1 Блок шема САДК2Г**

Имајући у виду да је принцип функционисања САДК2Г заснован на САДК1Г може се извршити уопштавање принципа описаних у претходном поглављу. Уз услов

да су време $t$ и дитерски сигнали $h_1$ и $h_2$ међусобно некорелисане промењљиве, а да $y_1$ и $y_2$ зависе од времена $t$ следи:

$$\begin{aligned} dP_{\Psi} &= dP_{y_1} \cdot dP_{y_2} \cdot dP_{h1} \cdot dP_{h_2} \\ dP_{\Psi} &= dP_{y_1/t} \cdot dP_{y_2/t} \cdot dP_t \cdot dP_{h1} \cdot dP_{h_2} \\ dP_{\Psi} &= \delta\left[y_1 - f_1(t)\right] \cdot \delta\left[y_2 - f_2(t)\right] \cdot \frac{1}{T} \cdot \frac{1}{2g} \cdot \frac{1}{2g} \cdot dy_1 \cdot dy_2 \cdot dt \cdot dh_1 \cdot dh_2 \end{aligned} \tag{2.3.3.1}$$

Средња вредност (математичко очекивање) је дато изразом:

$$\begin{aligned} \overline{\Psi} = \int_{t_1}^{t_2} \frac{dt}{T} \int_{-2g}^{+2g} \delta\left[y_1 - f_1(t)\right] dy_1 \int_{-2g}^{+2g} \delta\left[y_2 - f_2(t)\right] dy_2 \times \\ \int_{-g}^{+g} \Psi_1(y_1 + h_1) \frac{dh_1}{2g} \int_{-g}^{+g} \Psi_2(y_2 + h_2) \frac{dh_2}{2g} \end{aligned} \tag{2.3.3.2}$$

На основу слике 2.3.1.2 је показано да важи:

$$\int_{-g}^{+g} \Psi_i(y_i + h_i) \cdot \frac{dh_i}{2g} = \Psi_1 \cdot p_1 + \Psi_2 \cdot p_2 = y_i, \qquad i = 1,2 \tag{2.3.3.3}$$

Сходно томе израз (2.3.3.2) се може написати као:

$$\overline{\Psi} = \int_{t_1}^{t_2} \frac{dt}{T} \int_{-2g}^{+2g} \delta\left[y_1 - f_1(t)\right] \cdot y_1 dy_1 \int_{-2g}^{+2g} \delta\left[y_2 - f_2(t)\right] \cdot y_2 dy_2 \tag{2.3.3.4}$$

На крају се добија израз (2.3.3.5) у којем је средња вредност $\Psi$ једнака производу вредности улазних величина.

$$\overline{\Psi} = \frac{1}{T} \int_{t_1}^{t_2} f_1(t) \cdot f_2(t) \cdot dt \tag{2.3.3.5}$$

У (2.3.3.5) је описан случај када је у временском интервалу ($t_1$, $t_2$) узето бесконачно много одбирака улазних величина и на основу тога је одређена средња вредност $\Psi$.

За коначан број одмерака реалних улазних сигнала $y_1 = f_1(t)$ и $y_2 = f_2(t)$ важи израз :

$$\overline{\Psi} = \frac{1}{N} \cdot \sum_{k=1}^{N} \Psi_k \tag{2.3.3.6}$$

На основу централне граничне теореме и теорије узорака исказана је грешка квантизације у виду њене стандардне девијације.

$$\begin{aligned} \sigma^2{}_{\overline{\Psi}} &= \frac{\sigma^2{}_{\Psi}}{N} \\ \sigma^2{}_{\Psi} &= \overline{(\Psi - \overline{\Psi})^2} = \overline{\Psi^2} - \overline{\Psi}^2 \end{aligned} \tag{2.3.3.7}$$

У [11] је показано да важи израз:

$$\overline{\Psi^2} = \frac{(2g)^2}{T} \int_{t_1}^{t_2} |f_1(t)| \cdot |f_2(t)| \cdot dt \tag{2.3.3.8}$$

Затим се може изразити грешка методе мерења помоћу СААДК2Г као:

$$\sigma^2{}_{\Psi} = \frac{(2g)^2}{T} \int_{t_1}^{t_2} |f_1(t) \cdot f_2(t)| \cdot dt - \left[ \frac{1}{T} \int_{t_1}^{t_2} f_1(t) \cdot f_2(t) \cdot dt \right]^2 \tag{2.3.3.10}$$

На основу израза (2.3.3.9) се може закључити да се у случају познавања таласних облика сигнала на улазима СААДК2Г, $y_1=f_1(t)$ и $y_2=f_2(t)$, може одредити грешка мерења на временском интервалу $(t_1, t_2)$.

Изложена теорија функционисања СААДК2Г је валидна као и у случају СААДК1Г ако се може показати да је трећи централни момент $M_3$ случајне променљиве $\Psi$ ограничен.

$$\begin{aligned} M_3 &= \overline{\Psi^3} - \overline{\Psi} \cdot \left( 3\sigma^2{}_{\Psi} + \overline{\Psi}^2 \right) \\ \overline{\Psi^3} &= \frac{(2g)^4}{T} \int_{t_1}^{t_2} f_1(t) \cdot f_2(t) \cdot dt \end{aligned} \tag{2.3.3.11}$$

Уколико је производ функција $f_1(t) \cdot f_2(t)$ апсолутно интеграбилан, тада је и функција $\sigma^2{}_{\Psi}(t)$ апсолутно интеграбилна и на основу израза (2.3.3.11) се показује да је трећи централни момент $M_3$ ограничен.

Закључак је да је излаз САДК2Г сразмеран интегралу производа улазних напона на коначном временском интервалу. Међутим ако се на оба улаза САДК2Г доведе исти сигнал на излазу се добија вредност сразмерна интегралу квадрата улазног сигнала у времену. Уколико се та вредност подели са временом интеграљења и изврши кореновање добија се ефективна вредност улазног сигнала.

Битно је приметити и да је на основу израза (2.3.3.7) стандардна грешка квантизације обрнуто пропорционална квадратном корену из укупног броја одмерака.

$$\sigma_{\overline{\Psi}} = \frac{\sigma_{\Psi}}{\sqrt{N}} \tag{2.3.3.12}$$

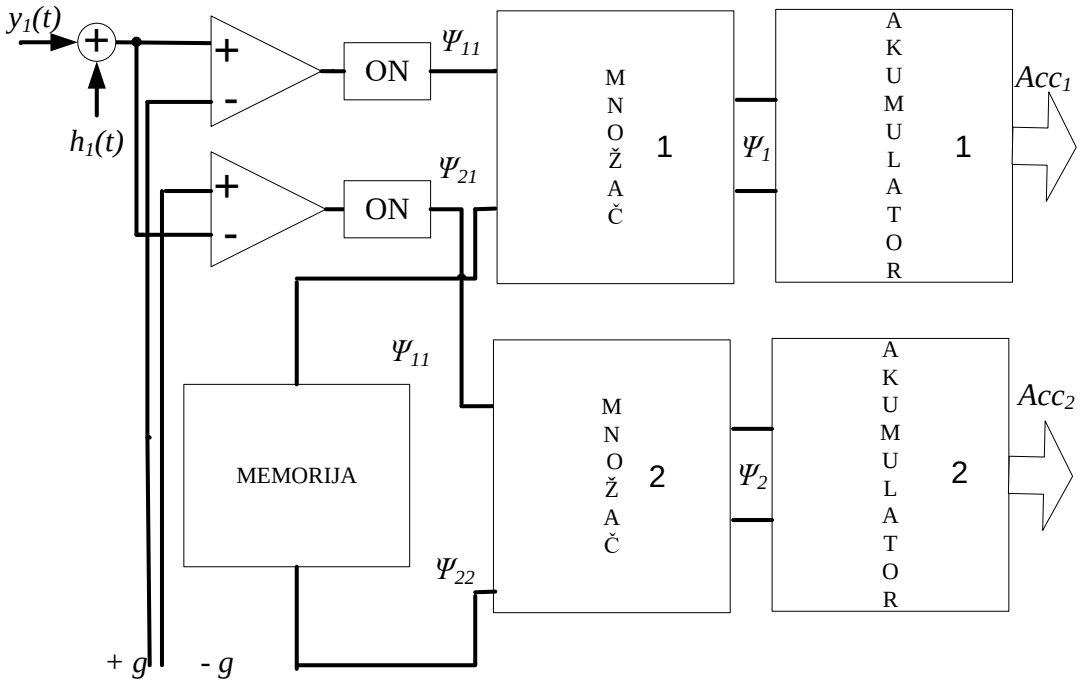
Један од ограничавајућих фактора у развоју САДК2Г је био напонски офсет брзих компаратора који чине флеш А/Д конвертор. Овај проблем је превазиђен применом методе периодичне замене улазних крајева компаратора, описане у [11].

Закључак је да је даље побошање у примени методе САДК2Г директно везано за реализацију дитерских сигнала што квалитетнијих статистичких карактеристика, нарочито је занимљива примена хардверског генератора истински случајног шума (који би теоретски обезбедио бесконачно велику резолуцију САДК) [12].

### 2.3.4 Стохастички дигитални процесор ортогоналних трансформација

Стохастички адициони А/Д конвертор је имплементиран у уређају за развој периодичног улазног напона у Фуријеов ред, односно за одређивање спектралних компоненти улазног сигнала (хармоника) [13-14]. Заменом одговарајућих базисних функција уместо синусних и косинусних могуће је извршити развој у било који ред, што је показано у [15].

Мерење појединих вредности хармоника сложеноперидичног сигнала је могуће вршити уколико се на улаз једног СААДК доведе дитерован сложеноперидични сигнал *y1(t)* а на улаз другог СААДК се доведе дитерован сигнал базисне функције *y2(t)* из скупа ортонормираних базисних функција (најчешће Фуријеовог). Резултат овако извршеног мерења је вредност једног Фуријеовог коефицијента (синусног или косинусног). Уколико уместо једне базисне функције имамо две, могуће је мерити вредности два Фуријеова коефицијента и на тај начин израчунати амплитуду произвољног хармоника улазног сигнала. С' обзиром да је облик базисних функција унапред познат други улаз се може поједноставити тако што ће се заменити меморијским блоком у који су смештени одбирци дитероване базисне функције.




**Слика 2.3.4.1 Блок шема стохастичког дигиталног процесора ортогоналних трансформација**

При мерењу амплитуде основног хармоника вредности Фуријеових коефицијената се израчунавају према:

$$a_0 = \sqrt{\frac{2 \cdot Acc_1}{N}} \cdot a$$
$$b_0 = \sqrt{\frac{2 \cdot Acc_2}{N}} \cdot a \qquad (2.3.4.1)$$

При чему *Acc1* и *Acc2* представљају садржаје првог и другог акумулатора на крају мерног интервала, $N$ је укупан број одбирака за време интервала мерења, а $a$ представља квант стохастичког адиционог флеш А/Д конвертора. Према томе амплитуда првог хармоника $U_0$ је једнака:

$$U_0 = \sqrt{\frac{a_0^{\,2} + b_0^{\,2}}{2}} \qquad (2.3.4.2)$$

# 3. ЕФЕКТИВНА РЕЗОЛУЦИЈА СТОХАСТИЧКИХ МЕРНИХ ИНСТРУМЕНАТА

Када се говори о стохастичком конвертору лако може наступити забуна у погледу броја бита са којима се ради. Саставни део стохастичког конвертора је флеш А/Д конвертор, по правилу **врло ниске резолуције**. У основној верзији стохастичког конвертора се налази двобитни флеш А/Д конвертор са свега три могућа стања: -1, 0 и +1. Одатле потиче велика грешка дискретизације по вредности. Добит у коришћењу флеш А/Д конвертора мале резолуције јесте у његовој једноставности, из чега проистиче мали број могућих извора систематске грешке. Велика грешка услед дискретизације по вредности се смањује додавањем дитерских сигнала и усредњавањем великог броја резултата мерења (oversampling).

Појам ефективног броја бита А/Д конвертора (ENOB - Effective Number Of Bits) је дефинисан следећом релацијом:

$$ENOB = \frac{FS}{\text{RMS NOISE}\sqrt{12}} \tag{3.1}$$

где је *FS* улазни опсег А/Д конвертора, а *RMS NOISE* ефективна вредност шума који се убацује у резултат мерења.

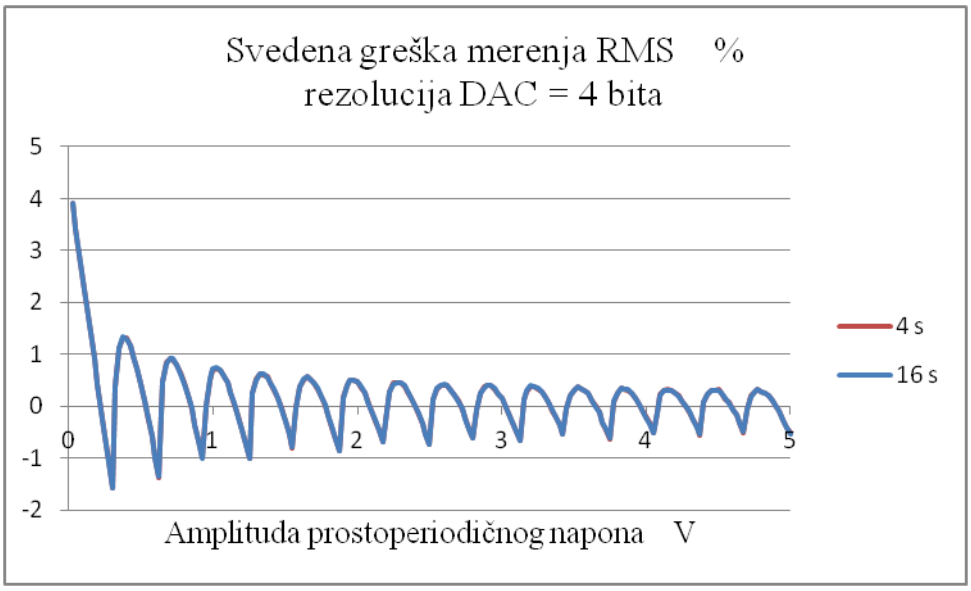
Код стохастичке дигиталне мерне методе прецизност расте са квадратним кореном из трајања мерења. Значи да све дужа мерења имају мање расипање резултата, односно све мању вредност шума додату на праву вредност у оквиру резултата мерења. **Величина овог шума исказана према опсегу А/Д конвертора је у директној вези са ефективном резолуцијом А/Д конвертора**. Очекује се да ће са продужавањем времена мерења расти и ефективна резолуција А/Д конвертора. Ова претпоставка је дата у теоријском моделу стохастичког адиционог А/Д конвертора, где се претпоставља да нема утицаја систематских грешака на резултат мерења, већ само случајних, чији се утицај смањује продужавањем мерења. Међутим у реалним условима увек постоје преостале систематске грешке. Код дугачких временских

периода мерења, где се утицај случајних грешака смањује, долази до тога да чак и врло мале систематске грешке постају значајне.

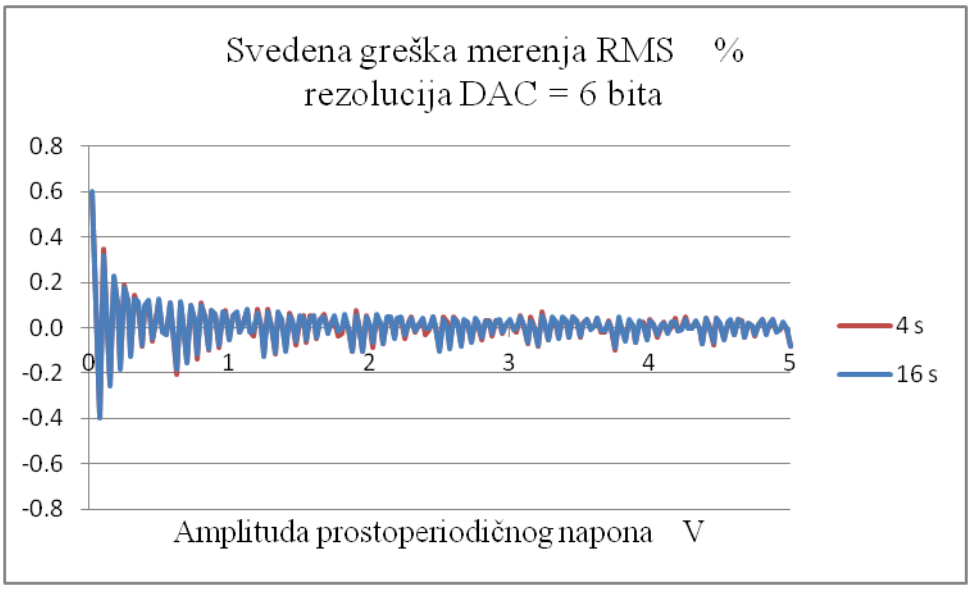
У наставку је дат приказ утицаја једне систематске грешке на резултат мерења: коначне резолуције Д/А конвертора којим се генерише дитерски сигнал.

Симулирано је понашање САДК2Г на чији улаз је доведен простопериодичан напон амплитуде до 5 V, одређивана је сведена грешка мерења ефективне вредности напона, а варирана је резолуција Д/А конвертора којим се врши генерисање дитерских сигнала. Симулирана су мерења у трајању од 4 и 16 секунди. За генератор дитерских сигнала је узета уграђена random функција из Matlab софтверског пакета. Као додатни корак је извршено претварање реалне вредности дитера у једну од могућих $2^n$, при чему је $n$ резолуција (број бита) Д/А конвертора. Ово практично значи да је узет најбољи расположиви random генератор, али је његова резолуција смањена ради сагледавања утицаја резолуције на понашање стохастичког конвертора.

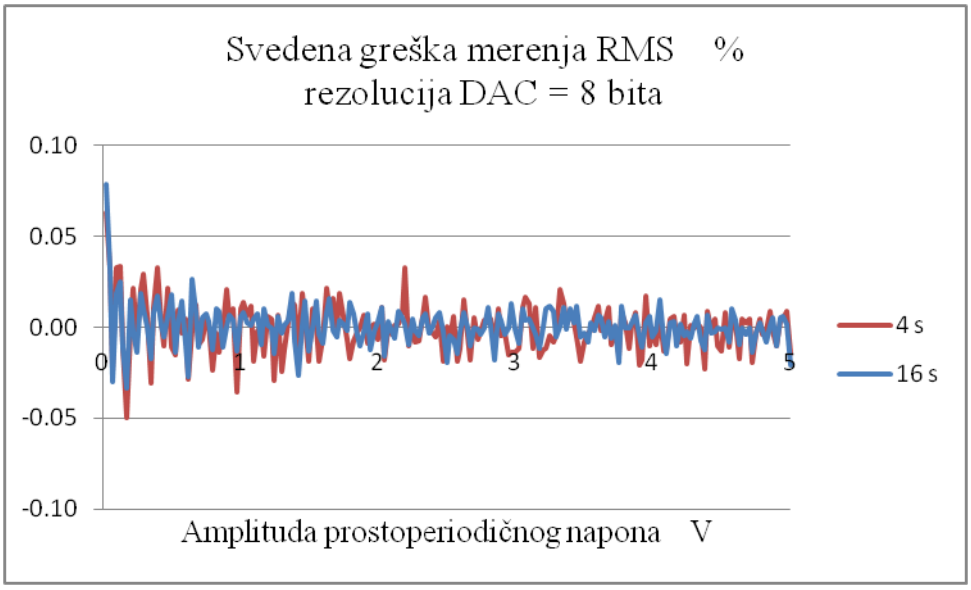
На сликама 3.1 - 3.5 су приказани добијени резултати који приказују сведену грешку мерења при различитим резолуцијама Д/А конвертора и различитим временима трајања мерења.



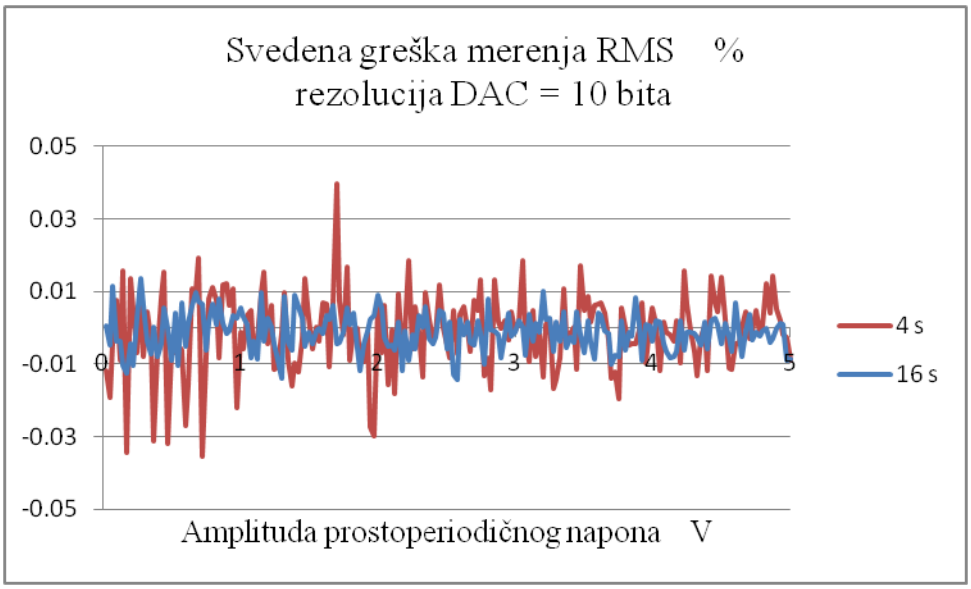

**Слика 3.1 Приказ сведене грешке мерења при резолуцији Д/А конвертора од 4 бита**



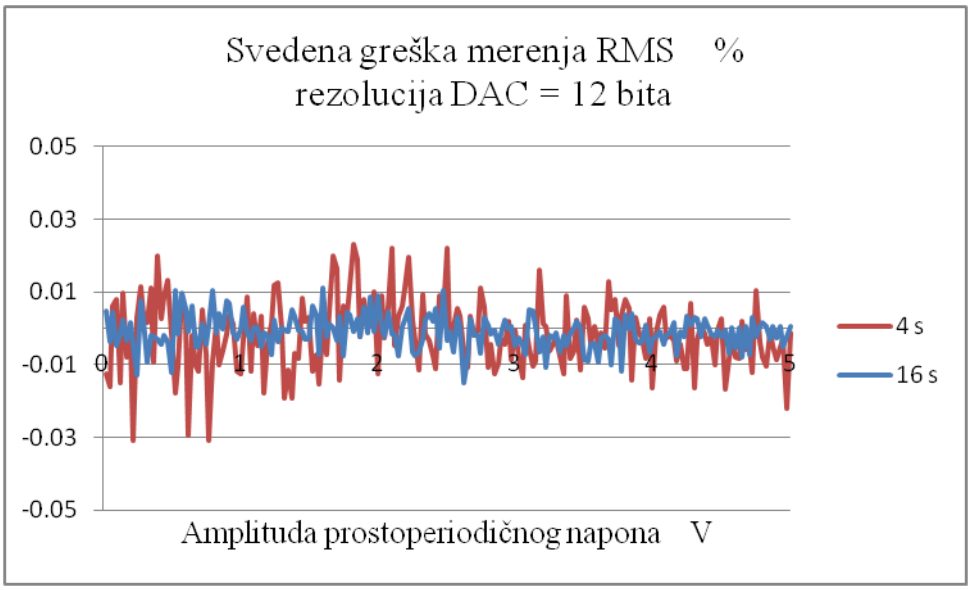

**Слика 3.2 Приказ сведене грешке мерења при резолуцији Д/А конвертора од 6 бита**




**Слика 3.3 Приказ сведене грешке мерења при резолуцији Д/А конвертора од 8 бита**




**Слика 3.4 Приказ сведене грешке мерења при резолуцији Д/А конвертора од 10 бита**




**Слика 3.5 Приказ сведене грешке мерења при резолуцији Д/А конвертора од 12 бита**

На првом графику, који приказује сведену грешку мерења при резолуцији Д/А конвертора од 4 бита, се може уочити 16 сличних образаца. Овакво понашање грешке потиче управо од резолуције Д/А конвертора, пошто је $2^4$=16.

При следећој резолуцији Д/А конвертора (6 бита), може се уочити више сличних образаца на графику, као и мањи опсег у којем се јавља грешка. Даљим повећањем

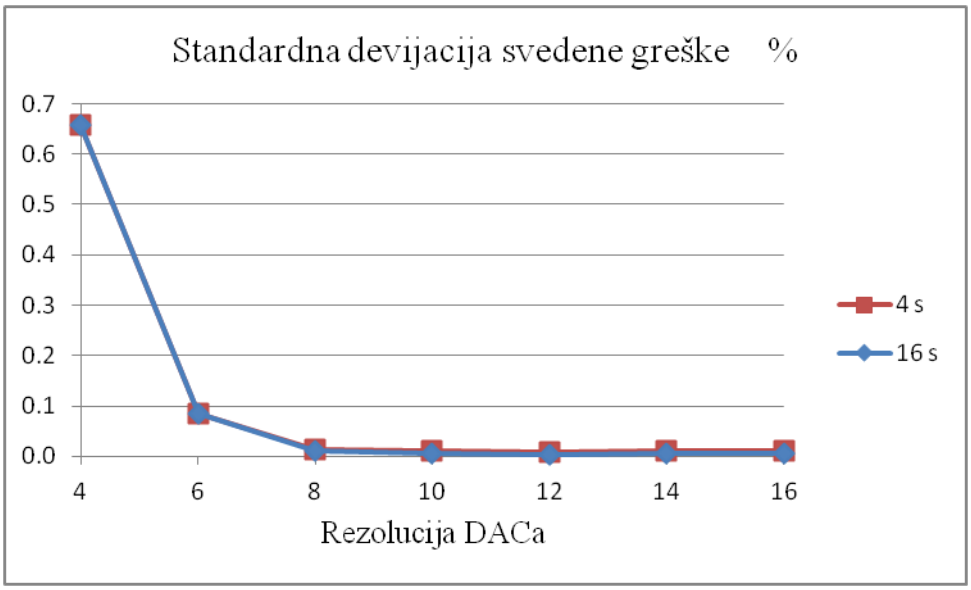
резолуције је све теже уочити понашање грешке која потиче од резолуције Д/А конвертора. Објашњење је да је систематска грешка услед резолуције Д/А конвертора сада по величини слична случајној грешци која потиче од стохастичке природе конвертора, односно грешци која постоји због неидеалности вредности дитера. Опсег грешке се опет смањио.

На прва два графика се не примећују разлике при различитим дужинама времена мерења, док се на преостала три јасно може уочити да је грешка при трајању мерења од 4 секунде приметно већа од грешке при трајању мерења од 16 секунди.

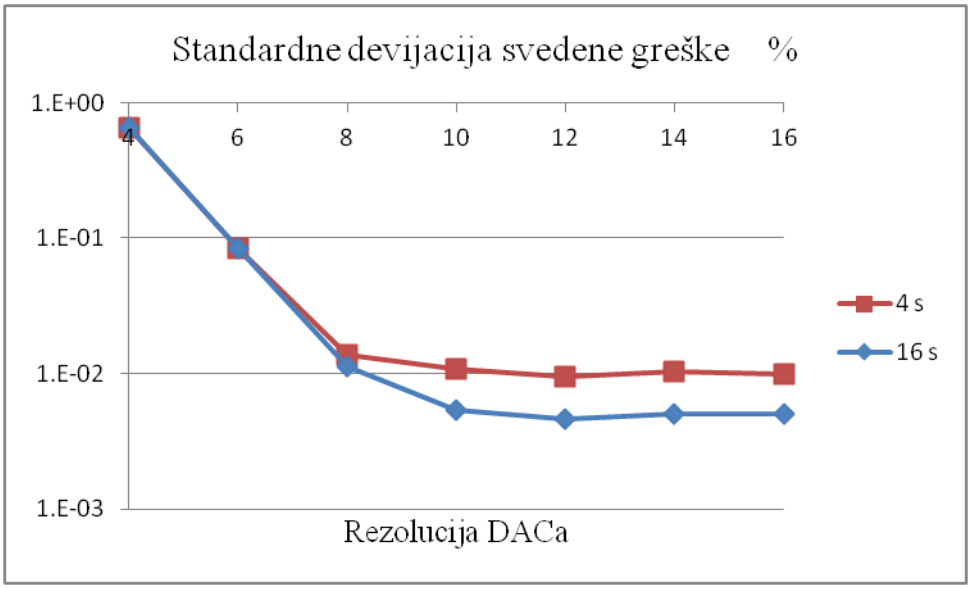
Даљим повећањем резолуције Д/А конвертора опсег грешке скоро да се не смањује, што значи да случајна компонента грешке постаје доминантна у односу на систематску компоненту услед коначне резолуције Д/А конвертора.

Повећавањем дужине мерења, случајна компонента грешке се смањује, па опет постаје битна резолуција Д/А конвертора којим се врши генерисање дитера.

За сваку резолуцију Д/А конвертора је одређена стандардна девијација сведене грешке. На сликама 3.6 - 3.7 је приказана зависност стандардне девијације сведене грешке од резолуције Д/А конвертора, при различитим временима трајања мерења и при линеарној и логаритамској вертикалној оси.



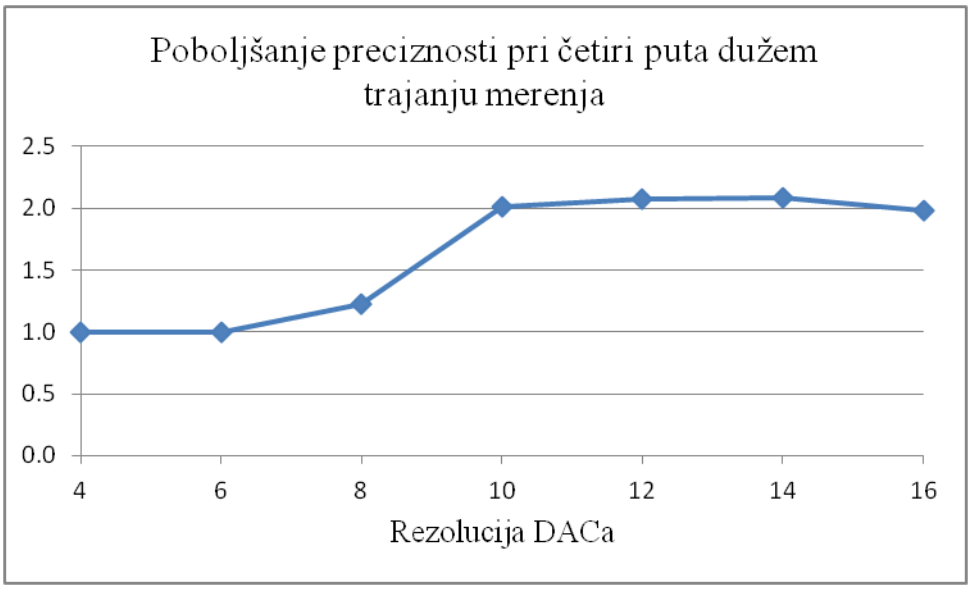

**Слика 3.6 Зависност стандардне девијације сведене грешке мерења од резолуције Д/А ковертора при линераној вертикалној оси**




**Слика 3.7 Зависност стандардне девијације сведене грешке мерења од резолуције Д/А ковертора при логаритамској вертикалној оси**

На обе слике се примећују две зоне. У првој зони, при вредностима резолуције Д/А конвертора од 4 и 6 бита, се добија скоро иста сведена грешка мерења без обзира на трајање мерења. Истовремено се примећује смањење сведене грешке мерења са порастом резолуције примењених Д/А конвертора. Друга зона се добија при већим вредностима резолуције Д/А конвертора и карактерише је стагнација сведене грешке мерења при порасту резолуције Д/А конвертора. На графику са логаритамском вертикалном осом се примећује да сведена грешка мерења при дужем мерењу има мању вредност. На графику са линеарном вертикалном осом се то не види, пошто је реч о врло малим вредностима грешке.

Израчунат је количник стандардне девијације сведене грешке мерења при дужини трајања мерења од 4 секунде и 16 секунди и приказан је на слици 3.8.




**Слика 3.8 Количник стандардне девијације сведене грешке мерења при дужини трајања мерења од 4 секунде и 16 секунди**

На графику са слике 3.8 се уочавају две зоне. Прва зона се добија при мањим вредностима резолуције Д/А конвертора и није могуће уочити побољшања са продужавањем трајања мерења. Друга зона показује приближно дупло бољу прецизност при четири пута дужем трајању мерења.

Код двобитног стохастичког адиционог флеш А/Д конвертора теорија предвиђа дупло побољшање у прецизности када се трајање мерења продужи четири пута. У првој зони се то не добија, пошто имамо врло малу резолуцију Д/А конвертора који врши генерисање дитера. Систематска грешка која потиче од мале резолуције Д/А конвертора је доминантна и не смањује се при повећању трајања мерења. Побољшавање прецизности мерења са квадратним кореном из трајања мерења се односи на случајну компоненту грешке која потиче искључиво од стохастичке природе конвертора, односно од присуства дитера.

Повећањем резолуције дитера смањује се систематска грешка, те постаје самерљива или мања од случајне грешке. Ово се види у другој зони графика, за вредности резолуције Д/А конвертора од 8, 10 и 12 бита. Тада имамо да је случајна

грешка значајнија од систематске грешке, поново почиње да важи теоријом предвиђено побољшање прецизности у зависности од продужавања трајања мерења.

Претходна анализа је послужила као мотив за формулисање нове методе за генерисање дитерских сигнала који немају коначну резолуцију.

# 4. ДИТЕРСКИ СИГНАЛИ

Коректно функционисање (прецизност) САДК у највећој мери зависи управо од статистичких карактеристика дитерских сигнала.

Захтеви које дитерски сигнали морају да испуне су стриктни и подразумевају да:

1. морају имати униформну расподелу вредности нулте средње вредности (вероватноћа појављивања било које вредности је једнака),
2. амплитудски опсег дитерског сигнала мора бити унутар строго дефинисаних граница (мора одговарати улазном опсегу брзих компаратора),
3. дитерски сигнали испуњавају услов да су некорелисани (међусобно статистички независни) и
4. дитерски сигнали и улазни сигнали такође морају бити некорелисани.

У досадашњој реализацији САДК2Г дитерски сигнали су генерисани у две фазе.

У првој фази је коришћењем LFSR (engleski - Linear Feedback Shift Register-LFSR) структуре генерисана псеудослучајна секвенца бројева.

У другој фази је секвенца псеудослучајних бројева са излаза LFSR структуре доведена на улаз Д/А конвертора, на чијем излазу је добијен аналогни напон - дитер (шум униформне расподеле амплитуда нулте средње вредности).

Овакав начин генерисања дитера се учинио као довољно ефикасан ауторима током година реализовања разних мерних уређаја. Иако теорија предвиђа стално смањивање грешке мерења са продужавањем трајања мерења, у пракси је уочено другачије понашање. Наиме, грешка у неком моменту престане да опада, иако меримо све дуже. Закључак је да тада до израза долазе све неелиминисане систематске грешке, без обзира колико оне биле малог нивоа. Теоријском анализом и симулационим путем се дошло до закључка да је вероватно највећи преостали проблем неидеалност дитера. Генерисање дитера коришћењем LFSR и Д/А конвертора подразумева ограничену резолуцију. Овај рад даје предлог за добијање дитера који су из континуалног опсега. Другим речима, рад даје предлог методе за генерисање дитера бесконачне резолуције.

У наредном поглављу је дат преглед псеудослучајних и истински случајних генератора бројева.

## 4.1 Псеудослучајни и истински случајни генератори бројева

Истински случајни бројеви и физички недетерминистички генератори случајних бројева све више добијају на значају. Случајни бројеви своју примену налазе у криптографији (математичка, стохастичка и квантна), Монте Карло и нумеричким симулацијама, статистичким истраживањима, алгоритмима случајности, индустрији игара на срећу, индустријском тестирању, мобилним комуникацијама, плаћању путем интернета, безготовинском плаћању, банкоматима, електронском банкарству, обезбеђивању сигурности дистрибуиране електроенергетске мреже (SCADA) итд..

Претпоставка је да истински случајни бројеви не могу бити прорачунати. Како рачунари раде на детерминистички начин, они их не могу генерисати.

Генератори случајних бројева су једна од десет најпопуларнијих тема за истраживање последњих година. У протеклој деценији било је у просеку око 83 патентне пријаве годишње. 1418 укупно од 1970. године и поприличан број објављених научних радова из ове области [16-22]. Ипак постоји оштар несклад између броја публикација и врло скромног броја производа (само 4 квантна генератора, и прегршт, већином укинутих, генератора базираних на шуму Зенер диоде).

У наставку је дата класификација и објашњени су основни принципи рада псеудослучајних и истински случајних генератора бројева.

Постоје два приступа у реализацији генератора случајних бројева: псеудослучајни (алгоритамски) и истински случајни (базирани на физичким процесима-недетерминистички). Као што сама реч "псеудо" и сугерише, псеудо-случајни бројеви нису у потпуности случајни. У суштини, псеудо-случајни генератори бројева су алгоритми који користе математичке формуле или "lookup" табеле за генерисање секвенци бројева који само наизглед делују насумично. Са друге стране истински случајни генератори бројева мере неки физички феномен (шум, електромагнетне појаве, квантне појаве) који је заиста случајне природе. Приступи имају прилично различите карактеристике и сваки од њих има своје предности и мане.

### 4.1.1 Псеудослучајни генератори бројева

Као што је већ напоменуто, псудослучајни генератори су ништа више него математичка формула, која служи за генерисање детерминистичког, периодичног низа бројева, који је у потпуности одређен почетним стањем (кључем), у литератури коришћен термин „семе“ (енглески "seed"). По дефиницији ови генератори доказиво нису случајни.

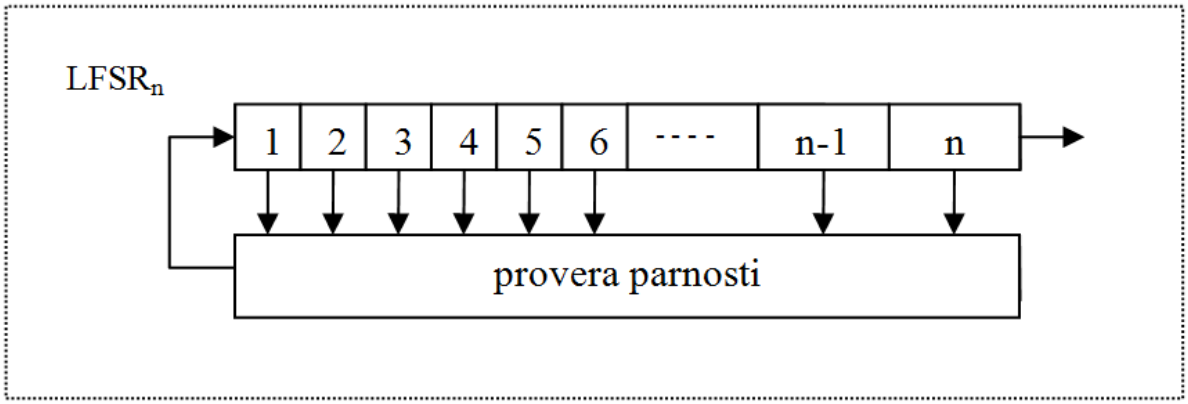
Велики део истраживања је посвећен теорији псеудослучајних бројева, и модерни алгоритми за генерисање случајних бројева су толико добри да секвенце бројева заиста изгледају као да су насумичне [23-25]. Што се тиче криптографске сврхе, велики број ових генератора се могу криптоанализирати тако да коришћење истих може представљати велики сигурносни ризик. Постоје пажљиво дизајниране, криптографски сигурне рачунске методе које стварају случајне бројеве, попут оних базираних на „Yarrow“ алгоритму, Фортуна, и другим [26-28]. Док већина модерних пседуослучајних генератора пролазе све познате статистичке тестове, постоје непотврђена мишљења да су одређени генератори много бољи од осталих. Истина је да сваки показује своју слабост у одређеним ситуацијама, и заправо се могу идентификовати као узрок грешака у стохастичким симулацијама, у Монте Карло прорачунима и у моделовању [29].

Дефиницију истински случајног генератора бројева не треба мешати са псеудослучајним генератором имплементираним у CMOS логици, или у сличном хардверу (LFSR). Такав генератор је и даље псеудослучајан, јер је математичка логика само хардверски реализована.

#### 4.1.1.1 Псеудослучајни генератор базиран на померачком регистру са линеарном повратном спрегом

Псеудослучајне секвенце бројева је могуће генерисати применом померачког регистра са линеарном повратном спрегом (engleski - Linear Feedback Shift Register-LFSR) [30]. Померачки регистар је одређене дужине и има повратну спрегу на основу принципа провере парности. Постоје тачно одређене структуре повратне спреге којима се постиже максимално дуга псеудослучајна секвенца генератора, тако да за померачки регистар дужине n бита добијамо секвенцу дугачку $2^n - 1$ . При томе, у зависности од врсте повратне спреге (парна провера парности или непарна провера), у псеудослучајној секвенци се равноправно јављају све вредности са истом вероватноћом осим најмање вредности (која се састоји од свих нула) или највеће вредности (састоји се од свих јединица). По истеку $2^n - 1$ вредности долази до понављања секвенце у потпуно истом облику.

Показује се да било који бит у померачком регистру има једнаку вероватноћу да му је вредност 1, односно 0. Такође, одабиром било којих m битова и формирањем речи дужине m, се добија псеудослучајна секвенца са униформном расподелом вредности. Користи се израз псеудослучајна секвенца, јер се ради о секвенци коначне дужине, која се у потпуности и на исти начин понавља. За довољно дугачак LFSR се добија дугачка секвенца која се најчешће у практичној реализацији може сматрати и скроз случајном. За померачки регистар дужине 40 бита, максимална секвенца је дугачка $2^{40} - 1$ , што при фреквенцији ишчитавања од 100 kHz даје трајање секвенце у износу од око четири месеца. Могуће је реализовати LFSR структуру дужине 168 бита која даје максималну секвенцу дужине $2^{168} - 1$ .




**Слика 4.1.1.1.1 LFSR структура**

На слици 4.1.1.1.1 је дата принципска шема LFSR структуре дужине n, која се састоји од померачког регистра са n ћелија и повратне спреге по принципу провере парности. Постоје тачно дефинисане повратне спреге које, за одабрану дужину померачког регистра, дају секвенцу максималне дужине. На слици је приказан општи случај где се из сваке ћелије враћа сигнал у коло повратне спреге. Најчешће се са свега два (до шест) места врши враћање сигнала да би се добила секвенца максималне дужине.

Моделовање рада LFSR који даје секвенцу максималне дужине се врши несводљивим полиномима над Галоовим пољима [31]. Дата је табела 4.1.1.1.1 са описом места са којих се узима сигнал за повратну спрегу за разне дужине померачког регистра, а које обезбеђују максималну дужину секвенце.

**Табела 4.1.1.1.1 Места са којих се узимају повратне спреге за реализовање максимално дугачке псеудослучајне секвенце**

| број бита | повратна спрега | број бита | повратна спрега | број бита | повратна спрега |
|---|---|---|---|---|---|
| 3 | 3, 2 | 18 | 18, 11 | 33 | 33, 20 |
| 4 | 4, 3 | 19 | 19, 6, 2, 1 | 34 | 34, 27, 2, 1 |
| 5 | 5, 3 | 20 | 20, 17 | 35 | 35, 33 |
| 6 | 6, 5 | 21 | 21, 19 | 36 | 36, 25 |
| 7 | 7, 6 | 22 | 22, 21 | 37 | 37, 5, 4, 3, 2, 1 |
| 8 | 8, 6, 5, 4 | 23 | 23, 18 | 38 | 38, 6, 5, 1 |
| 9 | 9,5 | 24 | 24, 23, 22, 17 | 39 | 39, 35 |
| 10 | 10, 7 | 25 | 25, 22 | 40 | 40, 38, 21, 19 |
| 11 | 11, 9 | 26 | 26, 6, 2, 1 | 41 | 41, 38 |
| 12 | 12, 6, 4, 1 | 27 | 27, 5, 2, 1 | 42 | 42, 41, 20, 19 |
| 13 | 13, 4, 3, 1 | 28 | 28, 25 | 43 | 43, 42, 38, 37 |
| 14 | 14, 5, 3, 1 | 29 | 29, 27 | 44 | 44, 43, 18, 17 |
| 15 | 15, 14 | 30 | 30, 6, 4, 1 | 45 | 45, 44, 42, 41 |
| 16 | 16, 15, 14, 13 | 31 | 31, 28 | 46 | 46, 45, 26, 25 |
| 17 | 17, 14 | 32 | 32, 22, 2, 1 | 47 | 47, 42 |

За померачки регистар од *n* бита максимално дугачка секвенца има $2^n - 1$ стања. Ово је за један мање од максималног броја стања која се могу добити од *n* бинарних бројева. Једно стање, код неких LFSR су то све нуле, а код других су у питању све јединице, се никада не дешава у исправном раду. Ако се на било који начин забрањено стање деси, долази до "закључавања" LFSR структуре, односно до остајања у том стању. Уколико је провера парности реализована помоћу XOR логике, недозвољено је стање са свим нулама. Ако је повратна спрега реализована XNOR логиком

недозвољено је стање са свим јединицама. Добра реализација LFSR структуре подразумева и проверу да ли се десило недозвољено стање и у том случају извођење LFSR из забрањеног стања. Ово се најчешће ради ресетовањем свих стања (уколико је недозвољено стање сачињено од свих јединица) или сетовањем свих стања (ако је недозвољено стање сачињено од свих нула).

Сваки елемент померачког регистра има исту вероватноћу појављивања нуле, односно јединице: -50%. Уколико m произвољних битова из LFSR структуре посматрамо као бинарну вредност, показује се да ће та вредност у довољно дугачком временском интервалу имати униформну расподелу, то јест да ће са истом вероватноћом да се појави свака од могућих вредности. Уколико је $m<n$ онда је број могућих различитих вредности које могу да се појаве $2^m$ , а не $2^m-1$ . Пошто максимална секвенца LFSR структуре дужине n бита износи $2^n-1$ , а за посматраних $m$ места имамо $2^m$ могућих вредности, очекујемо да се у току једног циклуса свака вредност дужине m бита понови приближно $\frac{2^n-1}{2^m} \approx 2^{n-m}$ пута [11].

### 4.1.2 Истински случајни генератори бројева

Према Керкхофовом принципу (холандски криптограф - Auguste Kerckhoffs), дефиниција генератора случајних бројева погодних за примену у криптографији подразумева да чак и ако је сваки детаљ познат о генератору (илустрација, алгоритми, итд.) он и даље мора бити у стању да произведе потпуно непредвидиве битове [32]. За разлику од псеудослучајних, физички (истински случајни, хардверске изведбе) генератори случајност базирају на физичким процесима, који имају фундаментално недерминистички начин понашања, што их уједно чини погоднијима за реализацију истински случајних генератора бројева. Физички генератор је део хардвера одвојен од рачунара, и обично је повезан преко USB или PCI магистрале. Учитавање бројева у кориснички програм је компликовано и обично захтева додатне драјвере. Цене генератора варирају од неколико стотина до неколико десетина хиљада долара (еура), у зависности од коришћеног физичког процеса у њему, као и брзине генерисања битова (генератори новијих генерација достижу брзину од 10 и више GBPS). Примери физичких процеса коришћеним у генераторима: термички шум, лавински и Зенеров ефекат, атмосферски радио шумови, радио-активни распад мерен Гајгеровим бројачем итд.. За разлику од псеудо-случајних, физички генератори имају неједнаку вероватноћу појаве нула и јединица, и генерално су конструисани тако да је корелација између битова јако мала, што је наиме и сама идеја случајности. У неким случајевима, физички систем се ресетује, тј. враћа се у почетно стање након производње бита, у циљу смањења аутокорелације.

Постоји много изведби и контрукција истинских случајних генератора и истраживање на ову тему је и даље у великој експанзији, али грубо се могу класификовати на следећи начин:

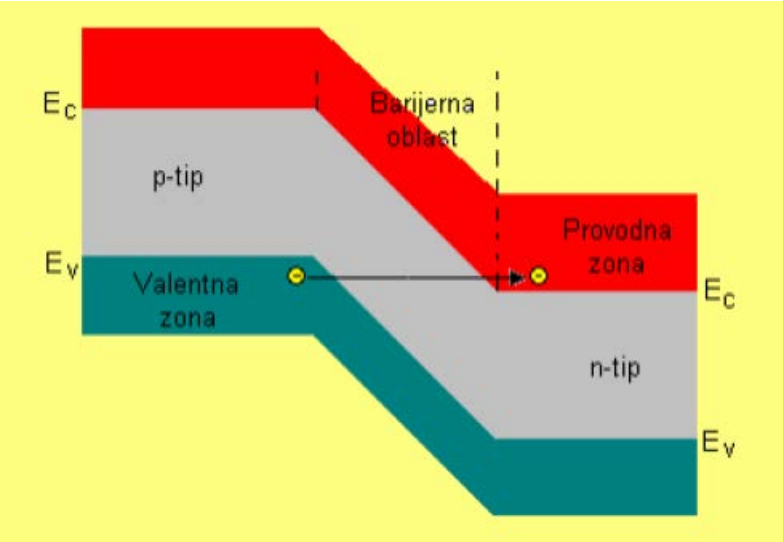
- генератори базирани на шуму,
- слободноосцилујући генератори
- генератори засновани на хаосу и
- квантни генератори.

Псеудо-случајни генератори такође могу бити класификовани у неколико категорија, тако да у зависности од врсте коришћеног алгоритма постоје: псеудо-случајни генератори логаритамског простора, генератори за линеране функције, полиномски генератори и други. У наредним поглављима ће бити описани основни појмови и изведбе везани за истински случајне генераторе бројева.

#### 4.1.2.1 **Генератори базирани на шуму**

Џонсон-Никвистов (Johnson- Nyquist) ефекат доводи до случајне појаве напона на крајевима било ког отпорног материјала, и одржава се на температурама већим од апсолутне нуле. Шум настаје због случајног термалног кретања квантног наелектрисања. Због одређених ефеката корелације електрона у проводнику, резултујући напон није у потпуности случајан [33-35].

Зенеров шум (у полупроводничким Зенер диодама) је узрокован тунелским ефектом, односно непосредним преласком електрона из валентне у проводну зону под утицајем електричног поља. Ако је струја довољно мале амплитуде, индивидуални "скокови" електрона кроз баријеру ће се видети као скокови напона кроз диоду формирајући такозвани *рози шум*, савршене случајности. Пролажење електрона кроз баријеру могуће је ако он може да задржи своју енергију и на другој страни баријере. Вероватноћа пролажења је утолико већа уколико је баријера ужа, а такође и уколико има више електрона са једне стране баријере и више слободних места (незаузетих енергетских нивоа) са друге стране [36].




**Слика 4.1.2.1.1 Тунелски ефекат код Зенеровог шума**

Занимљива особина овог шума је да при довољно великој вредности амплитуде инверзног напона, диода показује високоинтензивно лавинско појачање (лавински ефекат) [37]. Такав механизам доводи до великих амплитуда шума, уједно је и веома неосетљив на електромагнетно зрачење из околине. Међутим, Зенеров ефекат никада није опажен изолован у физичким уређајима од осталих ефеката, нити је квантна баријера константа. Већина претходно поменутих процеса у отпорницима и Зенер диодама имају одређени ефекат меморије, тачније тренутни напон зависи од напона у блиској прошлости и то доводи до корелације између случајних бројева.

Шум у полупроводничким уређајима представља спонтану флуктуацију у струји или напону. Интезитет тих осцилација зависи од врсте самог уређаја, процеса производње, као и од услова рада. Шум се сматра нежељеним ефектом, који се преклапа са корисним сигналом и има тенденцију да прекрије садржај корисне информације. Шум није исто што и дисторзија сигнала коју узрокују елементи струјног кола [38].

Електромагнетски или термички шум се може умањити спуштањем радне температуре кола. Друге врсте шумова, као што је праскави (popcorn) шум, не могу бити уклоњени, јер настају услед ограничавајућих околности физичких својстава. Шум се користи за класификацију полупроводничких уређаја у групе са различитим квалитетом и поузданошћу. Неки од најчешћих шумови су: термички, 1/f, $1/f^2$, праскави шум, лавински, пулсирајући итд..

Термички шум настаје насумичним кретањем електрона због термичке побуде (назван Johnson-Nyquist шум). Термално кретање електрона ствара флуктуације у напону на терминалима сваког резистивног елемента.

1/f шум је доминантан на ниским фреквенцијама и његова функција спектралне густоће је пропорционална 1/f. Присутан је у свим полупроводничким компонентама у присуству електромагнетног поља. Овај шум се обично повезује са кваровима, или са несавршеностима у процесу израде. Резултати истраживања показују да 1/f шум постоји и на веома ниским фреквенцијама реда $10^{-6}$ Hz [39].

Лавински шум у полупроводничким уређајима је повезан са обрнуто поларизованим спојевима. Под утицајем јаког електричног поља, електрони се крећу и добијају повећану кинетичку енергију. На крају слободног пута електрон се судари са атомом кристалне решетке. Ако између два судара електрон стекне кинетичку енергију једнаку или већу од енергије јонизације, извршиће јонизацију атома и створити још један слободан електрон. Сада оба електрона при следећем судару стварају још два електрона и на тај начин долази до умножавања електрона. Приликом стварања слободног електрона ствара се и шупљина, која се креће у супротном смеру. Прелазећи слободан пут, и она, сударом са атомом, може да изврши његову јонизацију. Према томе, било да почне процес умножавања носилаца електронима или шупљинама, услед тога што се при судару ствара пар електрон-шупљина долази до повећања инверзне струје.

Интензитет лавинског шума је обично много већи од било које друге компоненте шума. Срећом, овај тип постоји само у п-н спојевима при напонима блиским пробојном напону. Сам лавински феномен се углавном и користи као извор шума [40].

Популарни извора шума су и инверзни база-емитер пробој у биполарним транзисторима, ласерско фазни шум, итд..

Највећи проблем са свим врстама шумова је да случајност извора шума не може бити добро окарактеризована, мерена или чак контролисана приликом саме израде уређаја. Осим тога, неки механизми шума производе напоне мале амплитуде, које је потребно снажно појачати пре конверзије у дигиталну форму. Велика појачања уносе даљу девијацију од случајности, због ограниченог опсега појачавача, и додатне

нелинеаризације. Такође, брзо електрично пребацивање бинарне логике коришћене у колу генератора, прави јаке електромагнетне сметње, тако да више околних генератора (посебно на чипу) имају тенденцију да се међусобно синхронизују изазивајући драматичан пад укупне ентропије. Поврх свега тога високосензитивна појачала лако омогућавају манипулацију генератора заснованих на овом ефекту од стране спољних електромагнетхих поља.

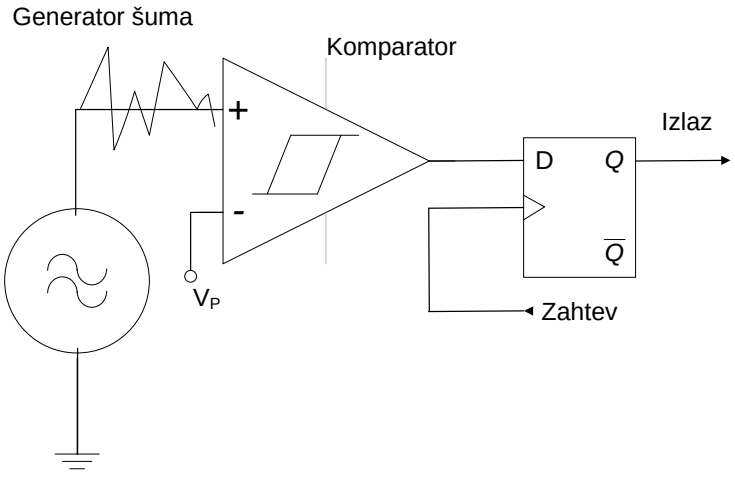
Може се закључити да генератори базирани на шуму имају један заједнички део. Случајан аналогни напон се узоркује периодично и упоређује са предефинисаним прагом: ако је већи, у том случају је генерисана логичка "1", у супротном логичка "0". Очигледно је да се праг може поставити тако да вероватноћа логичких "1" и "0" буде отприлике иста. Међутим, фино подешавање прага представља дуготрајан процес и велики је изазов одрадити га коректно. Такође је присутан и проблем стабилности: чак и најмање одступање од средње вредности (на пример због девијације температуре или напонске промене напајања) ће створити приметну зависност. Доказивост било ког истинског генератора базираног на шуму је јако компликована, на крају и немогућа због:

1. доказивости случајности експлоатисаног извора шума;

2. ефекта одабирања сигнала - поступка дигитализовања;

3. евентуалног коришћења накнадне-обраде.

На слици 4.1.2.1.2 је приказана поједностављена шема генератора базираног на шуму.




**Слика 4.1.2.1.2 Поједностављен приказ генератора базираног на шуму**

Шум пролази кроз компаратор чији је излаз или 0, или 1, у зависности да ли је позитивни улаз испод или изнад вредности прага ($V_P$). На захтев се генерише нови случајан бит на излазу.

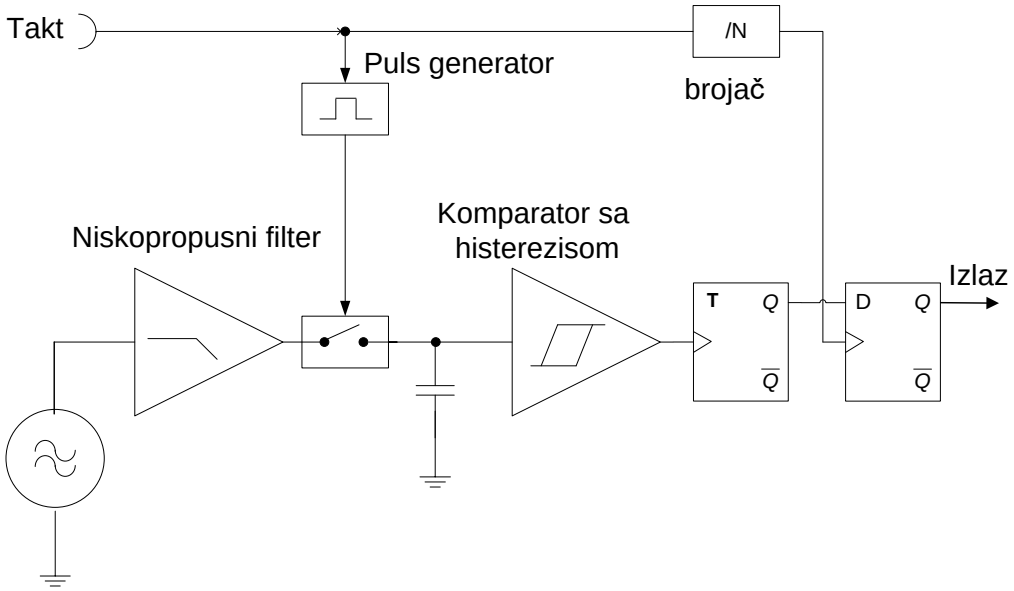
Идући од овог базичног електричног, истраживана су многа кола чији је циљ да се побољша случајност.

Прво, најочигледније побољшање било би да се на неки начин елеминише преднапон из тока шума у хардверу, без потребе за подешавањем прага напона.

У Бађини-Бучи (Bagini-Bucci) генератору, приказаном на слици 4.1.2.1.3, аналогни напон из слободног извора шума се периодично одабира на фреквенцији такта $f_1$ и упоређује са вредношћу прага на компаратору. Кад год компаратор произведе логичку "1", Т флип-флоп промени стање. Ако је процес узорковања случајан и стационаран, због временске симетрије процеса, излаз Т флип-флоп-а се пола времена налази у ниском стању и пола у високом стању. Идеја је да ће узорковање Д флип-флопа дати или логичку 0, или 1, са савршено једнаким вероватноћама. У пракси, догађају се незанемарљиве девијације.

Уједно постоје и одређени проблеми са овим дизајном. Пре свега се мисли на кондензатор за који се може рећи да поседује "меморију", памти претходни аналогни напон. Због коначне импедансе кола, када се напаја са другим напонским нивоом, напон ће у некој мери зависити од претходног, и самим тим стварати аутокорелацију. Следећи проблем је ако је Т флип-флоп фреквентно преслушаван, водећи до тога да

даје исти излаз неколико пута производећи тако позитивну аутокорелацију излаза, иако је основни случајни процес заиста био случајан. Једини начин да се заобиђе овај проблем је да се одабира фреквенција $f_2$ на нижем нивоу у односу на фреквенцију узорковања шума. На пример, $f_2 = f_1/N$, на тај начин долази до асимптотске случајне секвенце битова када $N \rightarrow \infty$. Лоша страна овог начина семпловања јесте ниска ефикасност. Добра страна је да се за било које довољно велико $N$, може добити било који жељени ниво квалитета случајности, барем теоријски [41].




**Слика 4.1.2.1.3 Приказ Багини-Бучи генератора базираног на шуму**

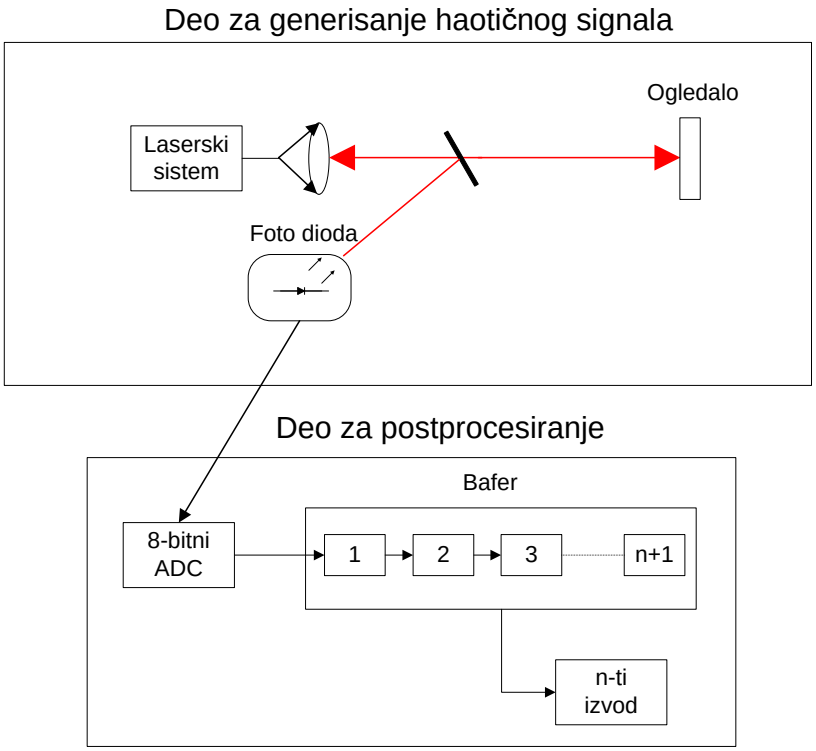
#### 4.1.2.2 Генератори базирани на хаосу

Вероватно најобјективнији принцип за физичко генерисање случајних бројева је примена поновљених мерења физичког система у хаосу. Филозофски проблем је да хаос значи проналажење реда у ономе што је наизглед случајно. Дакле, зашто би се свесно користио детерминистички систем како би се генерисали случајни бројеви? Примена ових генератора се базира на следећим ситуацијама:

- концептуално мешање хаоса и случајности;
- (не)веровање да системи које је тешко описати, нужно имају случајно понашање;
- робусност појединих хаотичних система за производњу макроскопског нивоа шума, и лакоћа искористивости истог у генерисању случајног броја преко метода из генератора базираним на шуму.

Најпогоднији хаотични системи за стварање случајних бројева су оптички, електрични и опто-електрични, премда постоје и механичке конструкције које су такође демонстриране.

Помоћу различитих механизама ласере је могуће довести у стање хаотичне флуктуације снаге [42-43]. Упрошћена шема екстремно брзог самоснабдевајућег хаотичног ласерског система (термин коришћен у страној литератури “ extremely fast self-feedback chaotic laser system”) је приказана на слици 4.1.2.2.1. Хаотично флуктуирање амплитуде светла је могуће детектовати помоћу фотодиоде чија амплитуда је одабирана брзим 8-битним А/Д конвертером и даље процесирана диференцирањем.




**Слика 4.1.2.2.1 Екстремно брзи самоснабдевајући хаотични ласерски систем**

Ласери нуде могућност за реализацију веома брзих хаотичних система и често се користе у генерисању случајних бројева. Због могућности израде малих ласера, резонатора и разних пасивних и активних оптичких елемената на чипу, овакве генераторе је могуће комплетно интегрисати у једном чипу и уједно могу бити енергетски ефикасни.

Генератор случајних бројева приказан на слици 4.1.2.2.2 се састоји од:

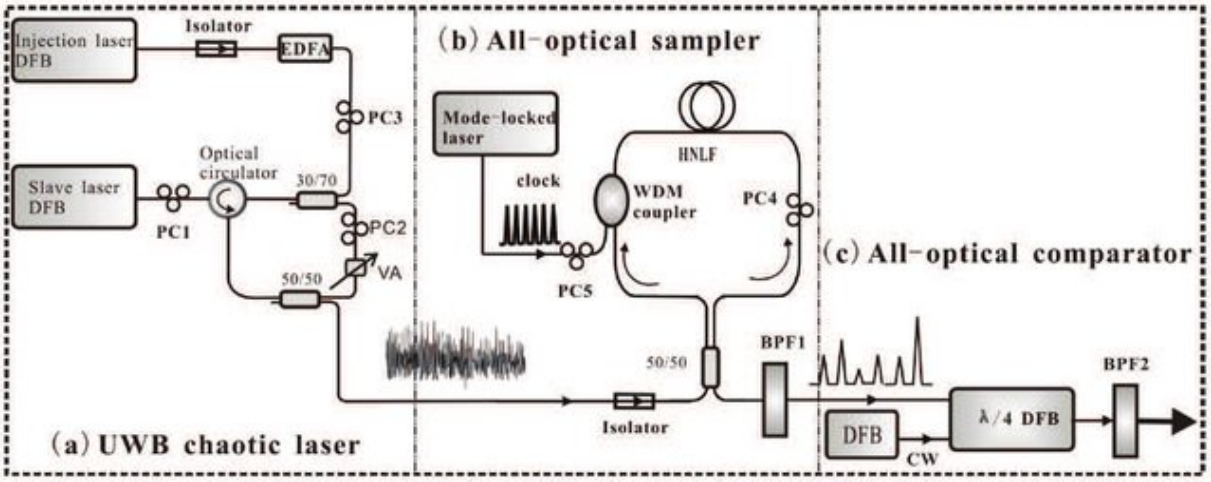
1. хаотичног ласера ултрашироког опсега (ultrawide-band),

2. оптичког семплера и

3. оптичког компаратора.

Пинцип рада је исти као и код претходно описаног "Багини-Бучи" генератора базираног на шуму, са том разликом да уместо електричног шума у овој изведби се користи интезитет светлости хаотичног ласера као извор случајности. Занимљива карактеристика која издваја овај генератор је та што је све оптички изведено, што значи да су сви сигнали као и обрада сигнала на оптичком нивоу. Чак и бројеви на излазу су дигиталне вредности интезитета светлости: низак интезитет светлости

представља логичку "0", док висок интезитет представља логичку "1". Ово је интересантно за коришћење у оптичко процесирајућим чиповима, а у случају потребе, излаз се лако може претворити у електрични сигнал употребом брзих фотодиода и одговарајућег појачавача [44].




**Слика 4.1.2.2.2 Потпуно оптички ласер - генератор базиран на хаосу (слика преузета из [29])**

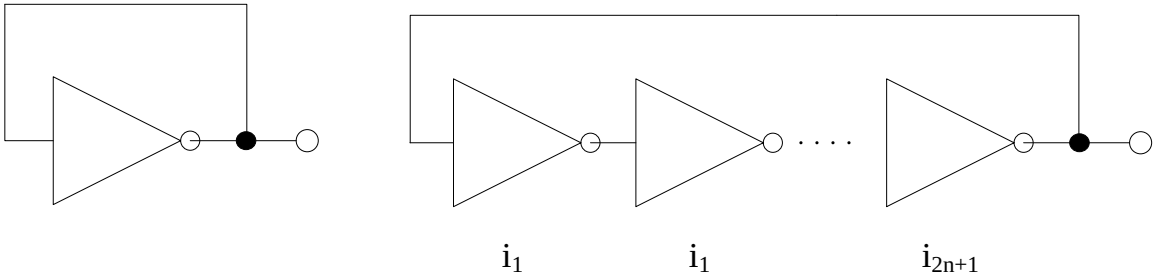
Овај ласер је сачињен од два повратно дистрибуирана ласера, главног (енглески "master") и помоћног (енглески "slave"). Интезитет излаза је екстрактован из повратне петље помоћу разделника зрака и у наставку је узоркован од стране оптичког семплера, на константној фреквенцији диктираној од стране системски закључаног ласера. Свака узоркована вредност интезитета светлости се даље упоређује са подешеним прагом помоћу потпуно оптичког компаратора, што резултира високим интезитетом (1) или ниским интензитетом (0). Случајни битови се производе темпом режимски закључаног ласера.

Мана саме идеје генерисања случајних бројева хаосом је хаотично појачање које је дефинисано као специфично решење диференцијалне једначине која, допуњена почетним условима, описује систем. Због саме једначине тог типа, и подаци садрже ограничену (малу) количину информација. Након што се мерењем добије информација из система, не постоји ни једна нова информација која се може добити из истог. Конкретно то значи да хаотични систем, у теорији, може произвести само ограничен скуп случајних битова и да сви остали морају бити у савршеној или скоро савршеној корелацији са тим скупом. Подразумева се да се реални хаотични системи никад не понашају управо онако како би требало уважавајући "једначину кретања" коју моделују, због случајних квантних и статистичких ефеката. Међутим, ови ефекти нису

основа за ове случајне генераторе и обично су мали и немају значајан утицај на сам систем, чије понашање је углавом одређено макроскопски видљивим хаосом. Са друге стране, основе квантне случајности могу бити искоришћене за производњу доказиво случајних бројева.

### 4.1.2.3 Слободно осцилујући генератори

Када је излаз логичког инвертера доведен на свој улаз, коло се претвара у такозвани слободни осцилатор. (Слика 4.1.2.3.1).




**Слика 4.1.2.3.1 Шематски дијаграм слободних осцилатора (лево брзи и десно спорији – фреквенција осциловања одређена интерним кашњењем и паразитним капацитивностима)**

Повезујући излаз на свој улаз ствара се Зенонов парадокс: ако је на излазу стање логичке "1", уједно ће то стање бити и на улазу. У наставку се инверзијом добија логичка "0", како на излазу, тако и на улазу. Опет инверзијом (NOT операцијом) добија се логичка "1", и тако даље.

Теоријски, излаз је неодређен, али због коначних кашњења простирања NOT логичког кола, коло ће осциловати. Посебност овог осцилатора је у томе што се појављује у колима са негативном повратом спрегом (фазни померај од 180°). У теорији електронике негативна повратна спрега више се везује за "стабилизацију" него за осцилације. Међутим, може се догодити да се коло "закључа" (стабилизује) у неко напонско стање између нуле и јединице, без или са врло малим амплитудама осцилације, и у наставку није у стању да препознаје логичка стања. Да би се побољшале осцилације, може се додати реактанса у повратну спрегу чиме се произведени фазни померај разликује за ± 180°. Исти ефекат се може постићи и паразитним реактансама. У том случају може доћи до задовољавања Баркхаузеновог (Barkhausen) критеријума, самим тим и до појаве осцилација [45]. Због сложеног механизма слободних осцилација, њихова фреквенција је обично веома осетљива на варијације напона напајања и температуре, али ове промене су споре у односу на саму фреквенцију осциловања.

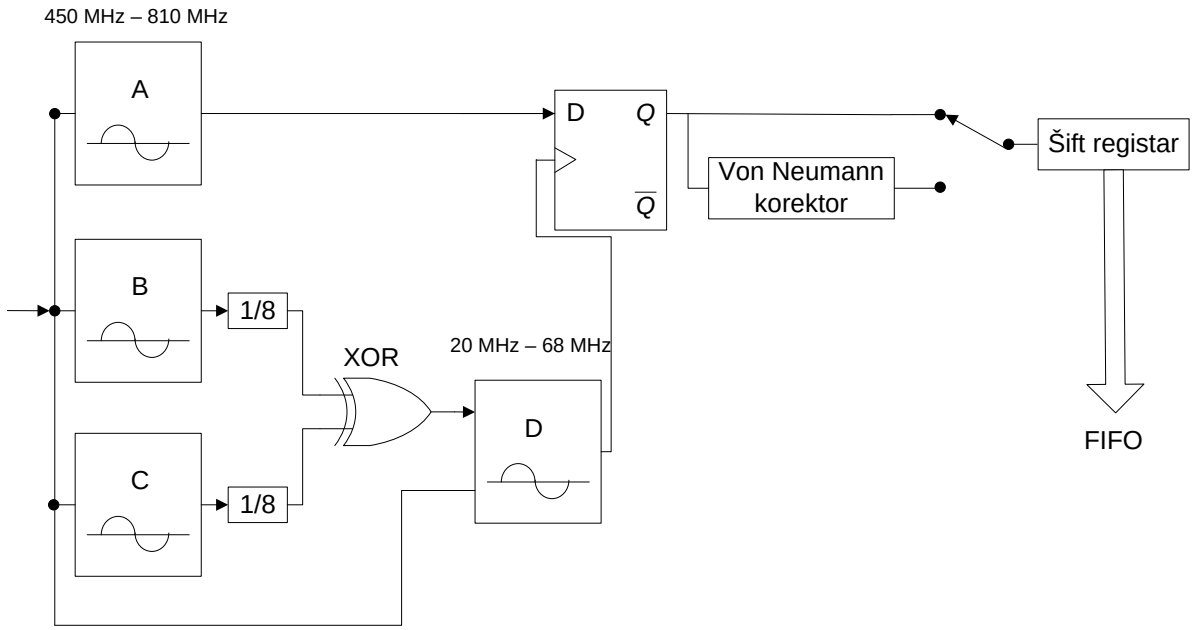
Са друге стране, електрични шум присутан на улазу додаје се на повратни сигнал са излаза и након снажног појачања узрокује веома брзо, случајно осциловање фреквенције и фазе. Овај генератор се може посматрати као посебан случај генератора базираног на шуму. Шум сваког кола је индивидуалан, стога разумна претпоставка је да више осцилатора, иако су на истом чипу, могу имати различите фреквенције и да се њихове међусобне фазе случајно разилазе у времену.

У случају постојања више таквих осцилатора који се налазе у међусобној близини (на пример на чипу), постоји и тенденција да се ускладе (синхронизују) кроз електромагнетне интеракције, олакшане јаким појачањима слободних осцилатора. Потпомогнут околним интерференцијама, велики утицај има и појачање електронског шума на значајан ниво. Овај ефекат може негативно утицати на перформансе дизајна и преставља велики проблем својствен слободним осцилаторима. Тај ефекат великог појачања чини их рањивим на спољашња електромагнетна зрачења.

Основни принцип ових генератора је да је излаз брзог слободног осцилатора узоркован од стране споријег слободног осцилатора. То је еквивалент наглог заустављања "точка среће", јер се он окреће толико "брзо" да се учини заустављеним на "случајним" позицијама. Јасно је да ако не постоји релативно фазно “дрхтање” између осцилатора, ће доћи до понављајућег бинарног шаблона, самим тим и до псеудо-случајног понашања. Још један врло битан проблем код слободно осцилујућих генератора је и да излаз зависи од паразитних реактанси и кашњења кола, и као што је претходно објашњено, за одређена кола постоји могућност да је излазна амплитуда толико мала да није могуће разазнати логичка стања, или је "закључана" у одређеном стању због ослабљеног осциловања. Шмитов тригер на улазу може помоћи у минимизовању овог проблема, али на рачун смањења фреквенције осцилација и усложњавања конструкције генератора.

Слободно-осцилујући приступ се користи у трећој и четвртој генерацији (FPGA, CPLD i ASIC) хардвера за различите криптографске сврхе. Један пример из стварног живота добро илуструје комбинаторику обично потребну за добијање пристојног случајног генератора бројева имплементираним у "VIA C3" процесорима (x86 архитектура, 500 MHz - 1.4 GHz брзина) (Slika 2.2.3.3). Састоји се из четири слободна осцилатора, три брза (450 MHz - 810 MHz) i једног спорог (20 MHz - 68 MHz). Широка

толеранција на фреквенцијама показује претходно описане проблеме: врло тешко контролисање параметара осцилатора приликом саме фабрикације. Најмање један од два осцилатора мора бити задовољавајуће случајности и пошто се то лакше постиже са споријим осцилаторима, инжењери из VIA-е су се и одлучили за ту опцију. Спор генератор је направљен од осцилатора B, C и D. Прво, B и C су успорени за 1/8 периоде и њихов XOR-ован излаз је повезан на D осцилатор (уједно једини који садржи дигитални улаз). Резултујући битови се појављују на излазу Q, D флип-флопа, у синхронизацији са импулсима из D осцилатора [46].



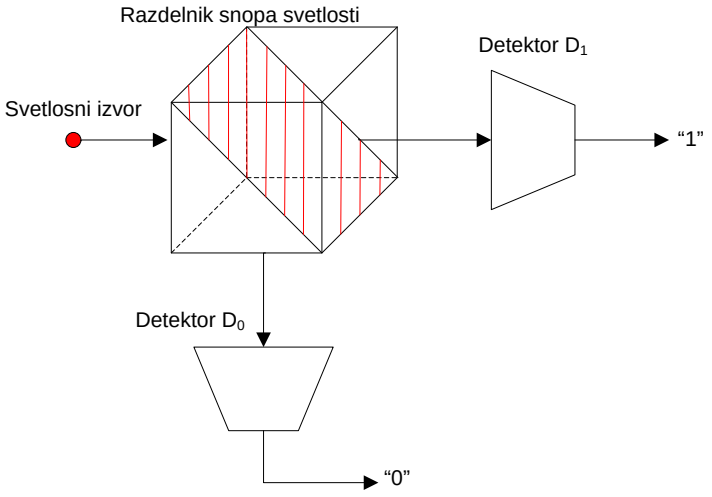

**Слика 4.1.2.3.2 VIA C3 PadLock генератор случајних бројева**

Опционо, излаз је филтриран кроз Фон Нојманов исправљач, који смањује производњу бита. Случајни бројеви на излазу нису најадекватнијег квалитета, и у циљу задовољавања критеријума тестова морају бити исправљени одређеним алгоритмима.

### 4.1.2.4 Квантни генератори

У ширем смислу квант означава елементарну, недељиву, најмању количину енергије која се јавља у неком елементарном процесу. На пример, фотон је квант електромагнетне интеракције, глуон јаке интеракције, З-бозон слабе интеракције, гравитон (експериментално још недетектован) квант гравитационе интеракције. У квантном рачунарству кјубит, или квантни бит је јединица мере квантне информације. Кјубит има сличности са класичним битом, али се у принципу доста разликују. Постоје два могућа исхода мерења кјубита, обично 0 и 1, као и бит. Разлика је у томе што кјубит може бити и суперпозиција оба стања [47].

Будући да живимо у свету у којем владају закони квантне физике, било који истински генератор случајних бројева (на пример окретање коцкице, или бацање новчића) може се назвати "квантним". Међутим, ово име је додељено оним генераторима који користе један истински квантни ефекат, који после сваког мерења, производи нове случајне битове, и то на такав начин да је између било која два мерења систем враћен на исту почетну вредност. Може бити чудно да је такав физички генератор могућ, из разлога што су почетни услови потпуно исти, као и то да је мерење вршено на апсолутно исти начин, а при том добијени резултати се разликују. Ипак, квантна физика ово чини могућим. У овом поглављу ће бити описани и објашњени неки примери из научних радова и патената.




**Слика 4.1.2.4.1 Просторни принцип рада квантног генератора случајних бројева**

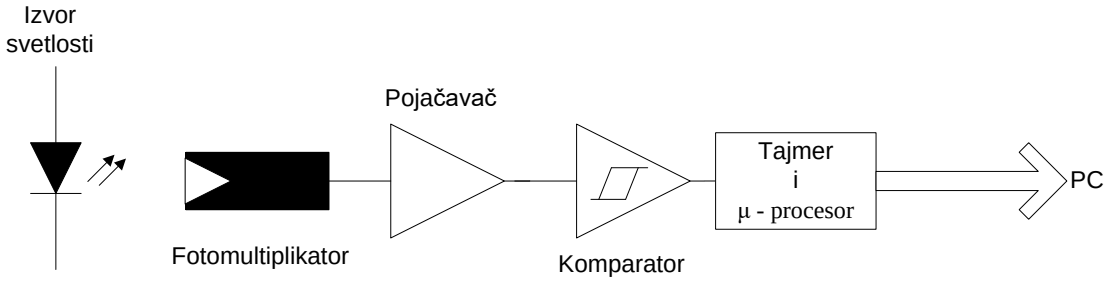
Кружно поларизован фотон има једнак садржај обе линеарне поларизације, али будући да се не може поделити на пола, има тачно 50 % шансе за излазак на било који порт. Ако означимо један од портова са "0", а други са "1", одмах се добија теоретски савршен генератор бројева чија је случајност загарантована законима квантне физике. Понашање таквог система је увек исто, а добијен резултат је увек случајан. Ово је потпуно различито од генератора базираних на хаосу и шуму, где се у циљу добијања различитих резултата систем мењао.

Квантни генератори се на основу овог принципа могу реализовати и несавршености било које врсте (емисија мулти-фотона, несавршена кружна поларизација, несиметрија осе сплитера зрака, мртво време детектора, ефекти меморије и други) се могу мерити независно од процеса генерисања бита, тако да се њихов ефекат на случајне бројеве може прецизно проценити и кориговати постпроцесирањем.

Главни проблем у практичној реализацији поделе светлосног снопа представља потреба за употребом два детектора. Њихове почетне разлике и даље разилажење у времену због старења и (или) температурног ефекта ће имати непосредан утицај на квалитет генерисаних случајних бројева. Овај утицај се може свести на разумну меру употребом једног детектора фотона али однос поделе светлосног снопа се мора прецизно механички подесити. Преостали проблеми настали из временског периода неактивности детектора и накнадног пулсирања доводе до корелације које је немогуће елеминисати у потпуности, али се могу редуковати испод жељеног нивоа.

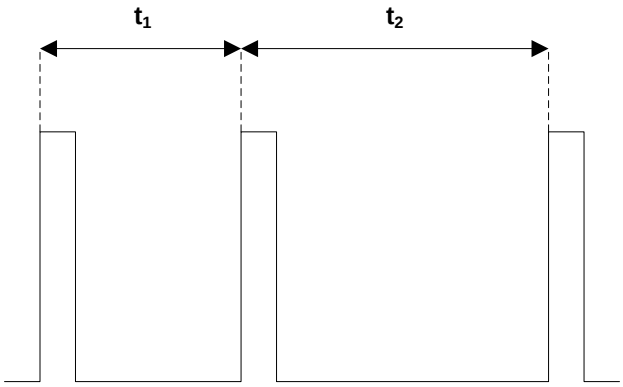
Генератор базиран на дељењу зрака је пример "просторног прицица" у којем је вредност случајног бита 0 или 1, одређена местом на којем фотон заврши.

Пример шематског приказа физичке израде генератора базираног на "временском принципу" је приказан на слици 4.1.2.4.2.




**Слика 4.1.2.4.2 Шема генератора случајних бројева базираног на временском принципу**

Генератори ове врсте уместо просторне информације користе временске. Принцип генерисања бита је следећи. Временски интервали t1 и t2 (слика 3.1.2.4.3) представљају три узастопне детекције фотона. У случају да је време t1> t2 тада се генерише, на пример, логичка "0", док се у супротном случају генерише логичка "1". Ако дође до поклапања временских интервала неће бити генерисана ниједна вредност.




**Слика 4.1.2.4.3 Временски интервали између три узастопне детекције фотона**

У случајним временским моментима фотони падају на детектор који се састоји од фотомултипликатора, појачавача и компаратора, тако да се на основу сваког детектованог фотона генерише један импулс. Импулси се затим обрађују и преносе на рачунар.

# 5. ПРЕДЛОГ НОВЕ МЕТОДЕ ГЕНЕРИСАЊА ДИСКРЕТНОГ АНАЛОГНОГ УНИФОРМНОГ ШУМА

Претпоставимо да имамо тестераст напон *u(t)* периоде *T* и фреквенције *f = 1/T* у опсегу *(-U, +U)*. Ако се изврши одабирање овог периодичног напона фреквенцијом *fs = 2^n f*, добиће се *2^n* различитих вредности напона, униформно распоређених, у оквиру опсега тестерастог напона. На слици 5.1 је приказана једна периода тестерастог напона у којој постоји $2^3 = 8$ дигиталних импулса. Ако се одабирање тестерастог напона врши у тренутку узлазне ивице дигиталних импулса, добиће се 8 дискретних аналогних вредности. Статистички посматрано, на већем броју периода свака дискретна вредност се појављује са једнаком вероватноћом *p(u)*. У овом примеру нема истинске случајности, напротив постоји потпуна предвидивост [12] .

Претпоставимо да имамо напон који се мења линеарно у опсегу *-U* до *+U* у временском периоду $0 \le t < T$. Напон је тада дефинисан изразом (5.1).

$$u(t) = U\left(\frac{2}{T}t - 1\right), \quad 0 \le t < T \tag{5.1}$$

Применом периодичног проширења на интервалу $0 \le t < T$, важиће израз:

$$u(t) = u(t + kT), \quad k \in Z \tag{5.2}$$

Одабирањем тестерастог сигнала *u(t)* у свакој периоди $T_S$, где је периода тестерастог напона N пута већа од периоде одабирања , $T = NT_S$. Уколико се прво одабирање изврши у моменту $\tau$, $0 \le \tau < T_S$, сви моменти одабирања су дефинисани изразом:

$$T_i = \tau + i \cdot T_S, \quad i = 0,1,...,N-1$$

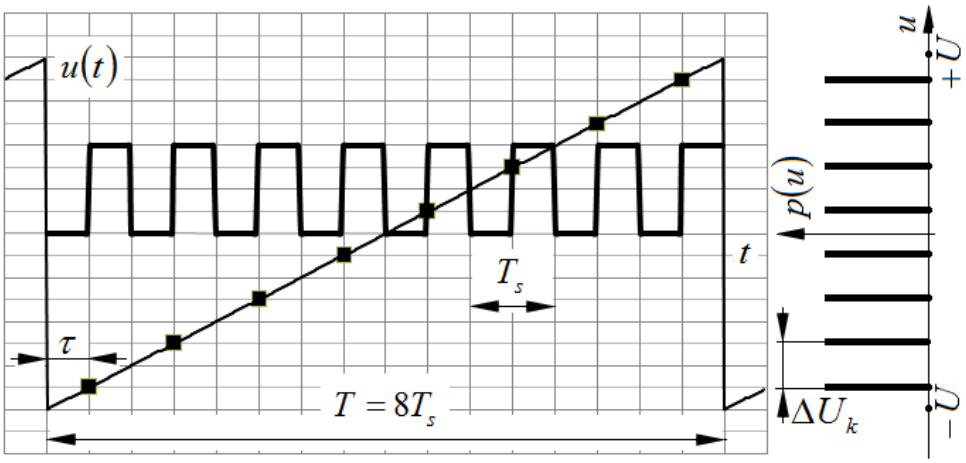
Вредности одбирака су дефинисане изразом:

$$U_i = u(T_i) = U\left[\frac{2}{N \cdot T_S}(\tau + i \cdot T_S) - 1\right] \tag{5.3}$$

Вредности $U_i$, i = 0,1, ...,N-1 формирају низ. Може се одредити размак између два суседна члана овог низа:

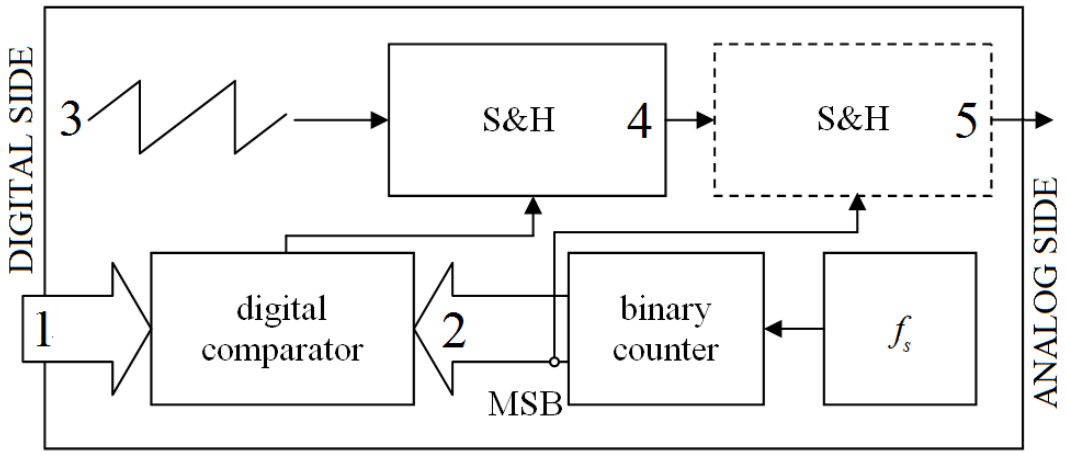
$$\Delta U_k = U_k - U_{k-1} = U \cdot 2\frac{f}{f_S} = const \tag{5.4}$$

За било коју вредност $\tau$, $0 \le \tau < T$, док је $T = NT_S$, у свакој периоди $T_S$, добија се сет од $N$ вредности код којих је разлика између суседних чланова константна у опсегу $-U$ до $+U$. Вредност било ког елемента низа зависи од $\tau$ - момента првог одабирања.



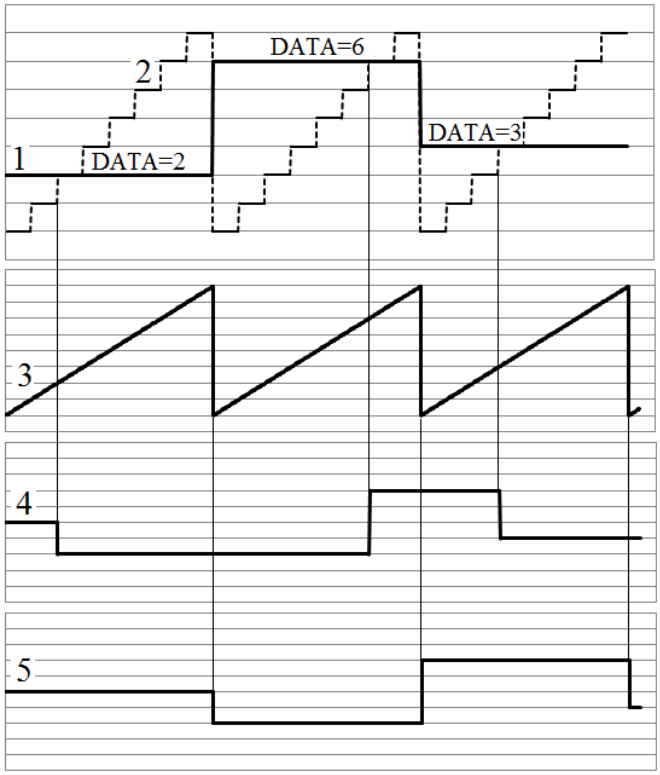

**Слика 5.1 Приказ тестерастог напона и дигиталног сигнала осам пута веће фреквенције којим се врши одабирање и добијених 8 једнако вероватних дискретних вредности**

Ово би практично могло да се искористи за реализацију Д/А конвертора. На слици 5.2 је приказан блок дијаграм Д/А конвертора који ради на овом принципу.




**Слика 5.2 Блок дијаграм Д/А конвертора**

На слици 5.3 су приказани карактеристични таласни облици сигнала.



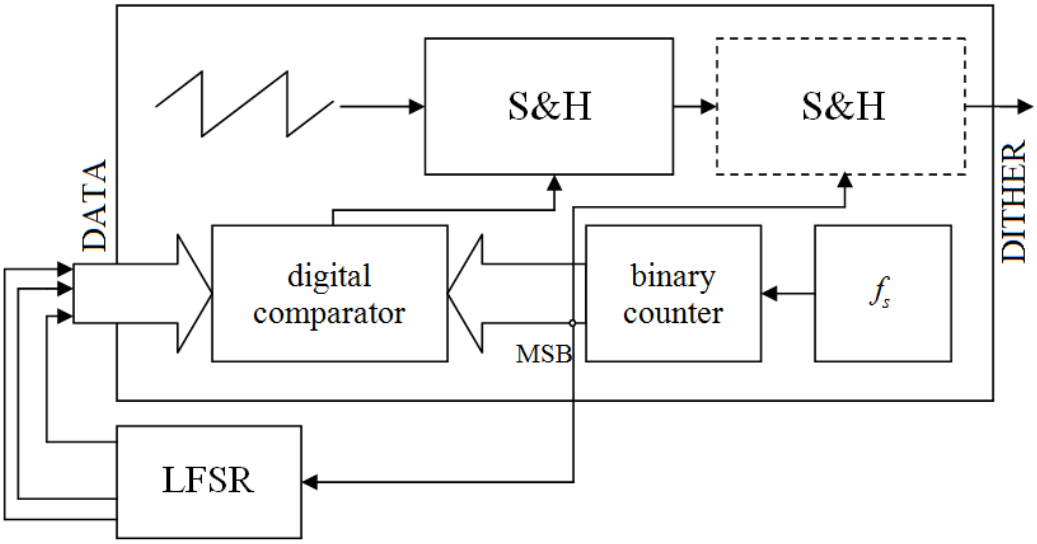

**Слика 5.3 Карактеристични таласни облици сигнала за време од три пуна циклуса бројача**

Употребом дигиталног компаратора, улазни дигитални податак (таласни облик 1) се пореди са стањем n-битног бинарног бројача (таласни облик 2). Бројач ради на

фреквенцији $f_s = 2^n f$, што значи да у једној периоди тестерастог сигнала $T$ прође кроз свих $2^n$ вредности, доводећи до обртања његовог стања (енглески - overflow). Периода тестерастог сигнала (таласни облик 3) се поклапа са једним циклусом бинарног бројача. За ово време бројач прође кроз свих $2^n$ стања почевши од $0$ до $2^n - 1$.

Одабирање тестерастог сигнала се врши у моменту поклапања садржаја бројача и улазног дигиталног податка (таласни облик 4). Малим вредностима улазног дигиталног сигнала одговара краће време Д/А конверзије, док је за веће вредности потребно дуже време за конверзију. Додавањем још једног семплинг кола (означено испрекиданом линијом на слици 5.2) одабирање се врши у моменту обртања стања бинарног бројача (таласни облик 5). На овај начин је време конверзије једнако периоди $T$, без обзира на вредност улазног дигиталног податка. Излазни опсег оваквог Д/А конвертора би био једнак опсегу тестерастог напона, а број могућих стања $2^n$, односно имао би n-битну резолуцију.

Ова идеја представља основу за генерисање псеудослучајног напона са униформном функцијом густине расподеле вероватноће. Дигитални подаци са излаза LFSR-а се доводе на улаз таквог Д/А конвертора, који је приказан на слици 5.4.




**Слика 5.4 LFSR и нееквидистантно одабирање тестерастог сигнала**

Садржај LFSR-а се мења у тренутку обртања стања бројача, што значи да би садржај LFSR-а био константан током једне периоде тестерастог сигнала, или времена за које бројач прође кроз свих $2^n$ стања. У моменту када се вредности бројача и LFSR-а изједначе долази до одабирања тестерастог напона.

Да бисмо на овај начин добили понашање као да имамо 12 битни ДА конвертор, морали бисмо обезбедити да је фреквенција у дигиталном делу $f_s$ већа од фреквенције тестерастог напона $2^{12} = 4096$ пута. При фреквенцији тестерастог напона од 100 kHz, требали бисмо обезбедити да је $f_s = 2^{12} \cdot 100\,\text{kHz} = 409.6\,\text{MHz}$. Ово је неприхватљиво велика вредност фреквенције. У даљем тексту ће бити приказана могућност добијања већег броја стања, при незнатном повећању фреквенције $f_s$ .

Посматрајмо случај у којем однос двеју фреквенција није целобројан, односно $f_s / f = 2^n \pm 1/2$. У овом случају ће за две периоде тестерастог напона $(2T)$ да се деси цео број дигиталних импулса $N = 2T/T_s = 2^{n+1} \pm 1$. $N$ истовремено представља број могућих дискретних вредности. Оваквим избором односа двеју фреквенција могли

бисмо добити приближно дупло повећање броја дискретних вредности при скоро истој фреквенцији $f_s = f\left(2^n \pm 1\right)/2 \approx 2^n f$ .

У терминима ДА конвертора, то би било аналогно добитку од 1 бита. На слици 5.5 су приказане две периоде тестерастог напона и 15 импулса који дефинишу тренутке одабирања. Са стране је приказана расподела, где се види (скоро) дупло повећање броја дискретних вредности.

Претпоставимо да у две периоде тестерастог напона *2T* дође до непарног броја одбирака *N = 2k-1*.

$$2T = N \cdot T_S = \left(2k-1\right) T_S \Rightarrow T = \left(k-1/2\right) T_S \tag{5.5}$$

Нека до првог одабирања у првој периоди дође у тренутку $0 \le \tau_0 < T_S/2$. Тада ће до првог одабирања у следећој периоди доћи у тренутку $\tau_1 = \tau_0 + (k+1)T_S$.

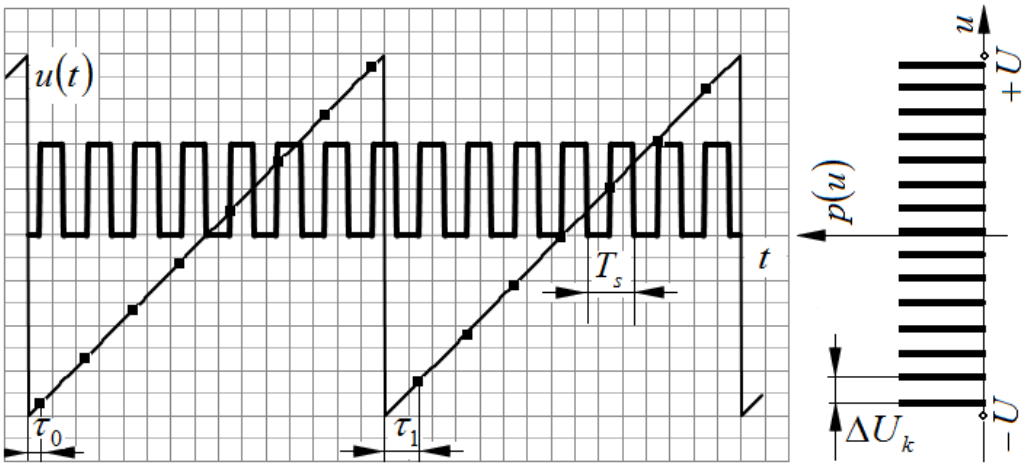
Услед периодичности тестерастог напона важи:

$$u\left(\tau_1\right) = u\left(\tau_1 - T\right) = u\left(\tau_0 + T_S/2\right) \tag{5.6}$$

Размак између суседних могућих вредности напона је дефинисан изразом:

$$u\left(\tau_1\right) - u\left(\tau_0\right) = U\frac{f}{f_S} \tag{5.7}$$

Слика 5.5 приказује две периоде тестерастог напона и 15 импулса који дефинишу тренутке одабирања. Са стране се може видети функција густине расподеле вероватноће са приближно дупло више дискретних вредности.




**Слика 5.5 Приказ две периоде, за однос фреквенција fs/f=15/2 и добијених 15 једнако вероватних дискретних вредности.**

Ако би се у разматрање узео однос $f_s/f = 2^n \pm 1/2 \pm 1/4$, за четири периоде тестерастог напона дошло би до појаве целобројног броја импулса $N = 4T/T_s = 4 f_s/f = 2^{n+2} \pm 2^1 \pm 2^0$.

На овај начин се са приближно истом фреквенцијом одабирања $fs = f\cdot(2^{n+2} \pm 2^1 \pm 2^0) / 2^2 \approx 2^n \cdot f$ добија четири пута више могућих стања него раније, што одговара добити у резолуцији од 2 бита. Могло би се наставити даље са оваквом генерализацијом и у табели 5.1 је приказано неколико таквих ситуација.

Овим поступком би се, барем теоретски, повећавањем вредности параметра k, могао бесконачно повећати број могућих напонских вредности на излазу.

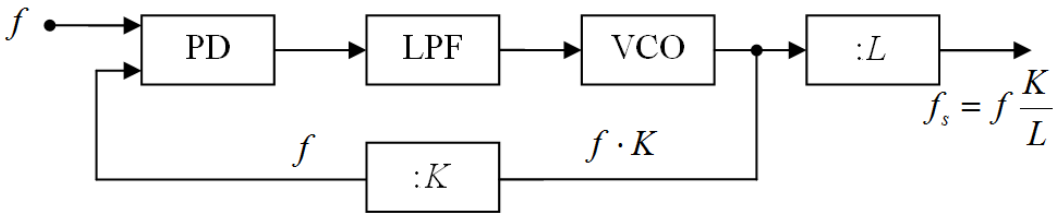
**Табела 5.1 Број могућих дискретних вредности у зависности од односа фреквенција**

| | Однос фреквенција | Број могућих стања |
|---|---|---|
| $k$ | $f_s/f$ | $N$ |
| 2 | $2^n \pm 1/2$ | $2^{n+1} \pm 2^0$ |
| 3 | $2^n \pm 1/2 \pm 1/4$ | $2^{n+2} \pm 2^1 \pm 2^0$ |
| 4 | $2^n \pm 1/2 \pm 1/4 \pm 1/8$ | $2^{n+3} \pm 2^2 \pm 2^1 \pm 2^0$ |
| 5 | $2^n \pm 1/2 \pm 1/4 \pm 1/8 \pm 1/16$ | $2^{n+4} \pm 2^3 \pm 2^2 \pm 2^1 \pm 2^0$ |

Без обзира колико се повећава параметар k, увек се добија коначан број стања N.

Намеће се питање, како практично обезбедити да се однос двеју фреквенција $f_s/f$ зада баш по тачно жељеној формули. Као логично решење се јавља примена фазно закључане петље (phase locked loop - PLL). Улазна фреквенција у PLL би била фреквенција тестерастог напона $f$, а повратном спрегом би се обезбедило множење ове фреквенције жељеним коефицијентом ради добијања импулса фреквенције $f_s$. У свакој од претходних формула је фреквенција одабирања исказана у облику $f_s = f \cdot K / L$, при чему су $K$ и $L$ цели бројеви, а $L$ је облика $2^k$.

Слика 5.6 представља блок дијаграм PLL структуре која се користи да се обезбеди фреквенција *fs* за дигитални део на основу фреквенције тестерастог напона *f*.

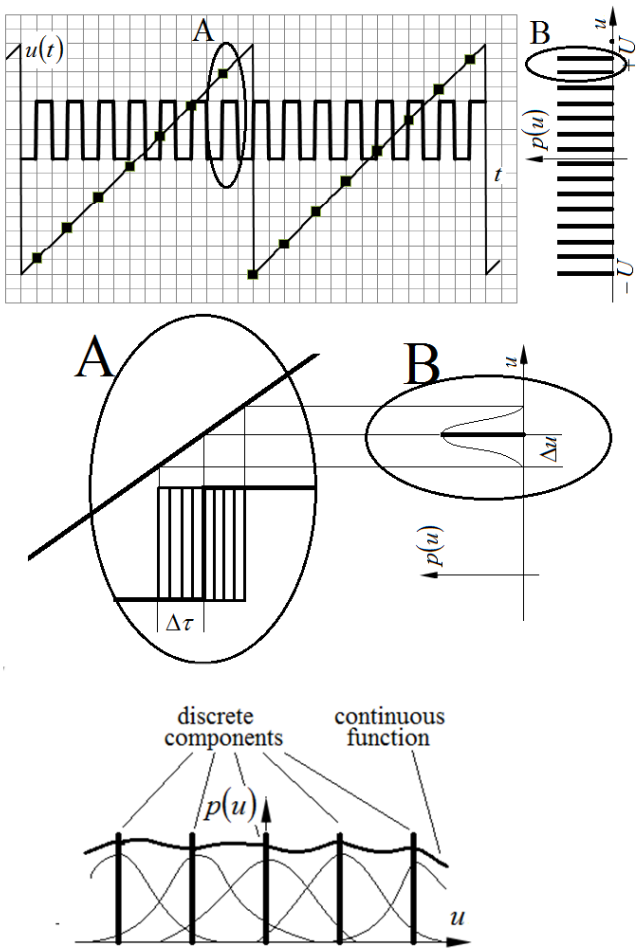



**Слика 5.6 PLL структура за генерисање фреквенције fs**

На улаз фазног детектора (phase detector PD) долази тестерасти сигнал фреквенције *f* и сигнал из повратне спреге. Задатак петље је да изједначи ове две фреквенције. Излаз фазног детектора је поворка импулса која се води на улаз НФ филтра. НФ филтер има задатак да издвоји једносмерну компоненту која управља радом напонски контролисаног осцилатора (VCO). Импулси са излаза VCO-а се повратном спрегом преко делитеља фактором *K* враћају на фазни детектор. Делитељ фактором *K* практично дефинише фактор којим се множи улазна фреквенција *f*. Делитељ фактором *L* дели фреквенцију са излаза VCO-а.

При пројектовању НФ филтера, покушава се задовољити компромис у брзини одзива НФ филтра и величине рипла (нежељена наизменична компонента додата жељеној једносмерној вредности). Код пасивног RC филтра, малој граничној учестаности одговара прихватљиво мали рипл, односно нестабилност напона на улазу VCO-а, а тиме и jitter у фреквенцији на излазу VCO-а. Нажалост, овим се добија дугачко време успостављања, односно спор одзив на промену улазне фреквенције. Избором мале граничне учестаности НФ филтера би се обезбедило довољно велико потискивање наизменичне компоненте, односно мали рипл.

У овом случају би параметре НФ филтра намерно одабрали тако да се добије у извесној мери нестабилна вредност на излазу, па би на улазу VCO-а postojao рипл. Због постојања рипла на улазу у VCO, на излазу ће се добити импулси чија ће фреквенција бити модулисана око средње вредности, може се рећи око називне фреквенције. Услед модулисане фреквенције импулса који окидају бројач, добило би се модулисање могућих тренутака одабирања тестерастог сигнала. На слици 5.7 је приказан детаљ који илуструје расипање амплитуда напона $\Delta u$ услед jittera $\Delta\tau$ імпулса који дефинише тренутак одабирања тестерастог напона.




**Слика 5.7 Детаљ тестерастог напона и сигнала за одабирање са узлазном ивицом jitter-а (испод: дискретна функција расподеле густине вероватноће постаје континуална)**

Ово би за последицу имало добијање нових вредности семплованог напона мало мањих или мало већих од очекиваних вредности (које би се добиле када рипла не би било). На основу овога би се, уместо јединствене вредности добијао читав скуп различитих и приближно истих вредности. Ако се посматра цео опсег, онда би се уместо дискретне функције расподеле вероватноће амплитуда, добила континуална расподела. Односно, добио би се шум који може да поприми било коју вредност у жељеном опсегу, не само коначан скуп дискретних вредности.

# 6. СИМУЛАЦИОНИ МОДЕЛ ГЕНЕРАТОРА ДИСКРЕТНОГ АНАЛОГНОГ УНИФОРМНОГ ШУМА

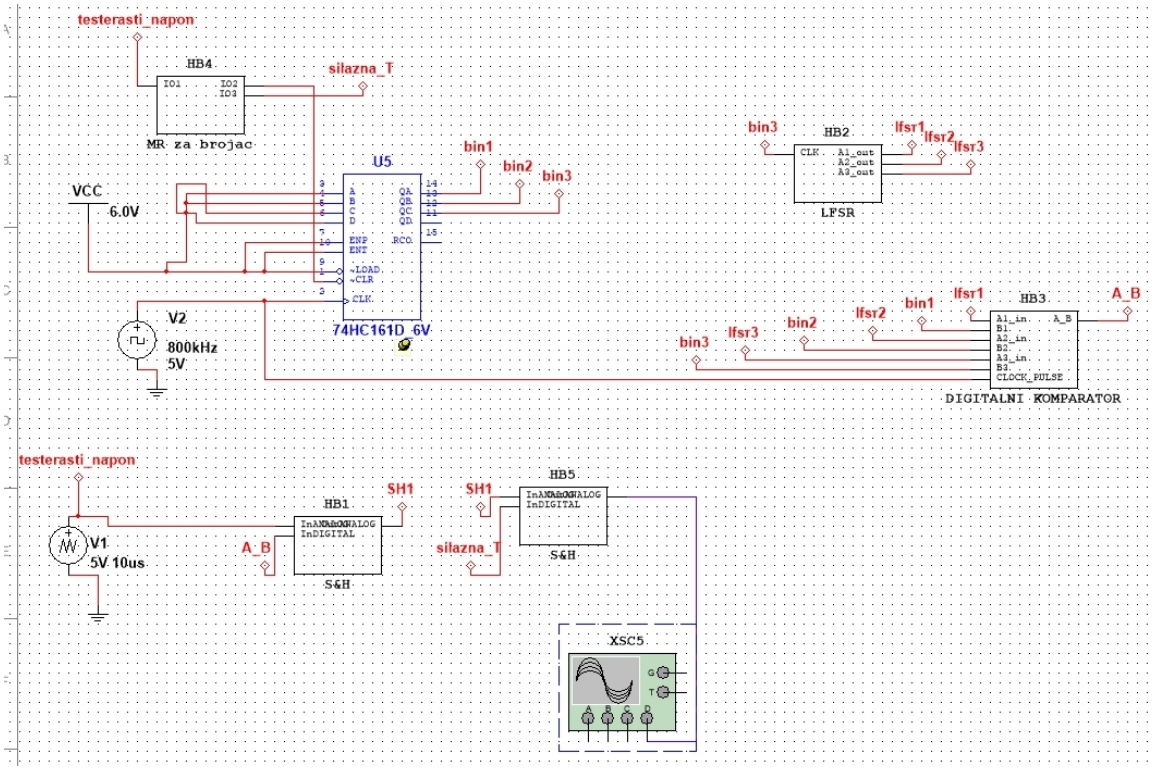
Софтверски симулациони модел је развијен са циљем да се провери адекватност предложене методе.

Након тога је развијен хардверски генератор дискретног аналогног шума који је детаљно описан у прилогу: "Хардверско решење генератора дискретног аналогног униформног шума". Хардверско решење је развијено у сврху провере концепта. Његове перформансе су лошије од перформанси најбољих доступних комерцијалних Д/А конвертора, пре свега јер су они активно развијани последњих педесет година уз ангажовање огромног броја истраживача широм света.

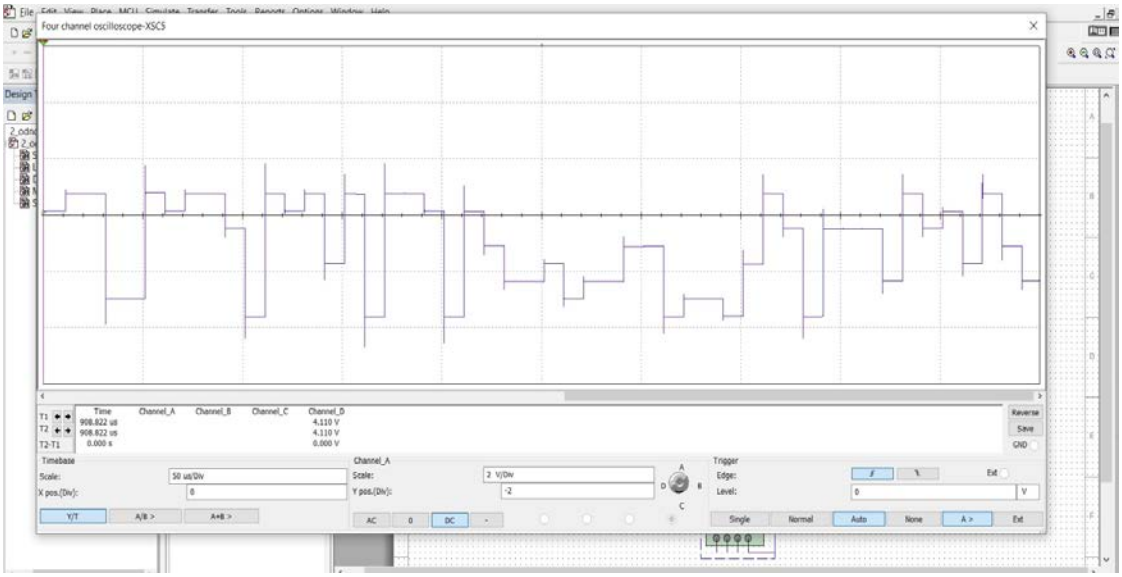
Ограничења реализованог генератора су се односила на немогућност подешавања параметара при генерисању дитера и пре свега на одсуство комерцијалног хардвера којим би се могао валидовати реализовани генератор.

Због тога се приступило изради детаљнијег и реалнијег симулационог модела, како би се касније резултати добијени истим могли валидовати једним од доступних комерцијалних софтверских пакета за валидацију генератора случајних бројева (Diehard, TestU01, ENT, NIST пакет статистичких тестова).

За потребе реализације новог симулационог модела генератора коришћен је SPICE (Simulation Program with Integrated Circuit Emphasis) софтверски пакет NI Multisim.




**Слика 6.1 Приказ шеме симулационог модела реализованог у NI Multisim софтверском пакету**




**Слика 6.2 Приказ резултата симулације тестерастог напона на екрану виртуелног осцилоскопа у случају нецелобројног односа фреквенција $f_s/f$**

Иако је поменути SPICE софтвер био подобан за израду симулационог модела, показало се да као и други SPICE софтвери има битно ограничење у погледу могућности генерисања значајнијег броја вредности на излазу. Како је наредни корак

поступак валидације, за статистички значајну анализу излазних података из симулације потребно је генерисати фајл величине од најмање 100000 вредности.

Новореализовани симулациони модел је упрошћен, са идеализованим компонентама уместо врло детаљног и реалног модела који је реализован у NI Multisim софтверском пакету. Ово је омогућило добијање довољног броја вредности симулацијом у разумном времену.

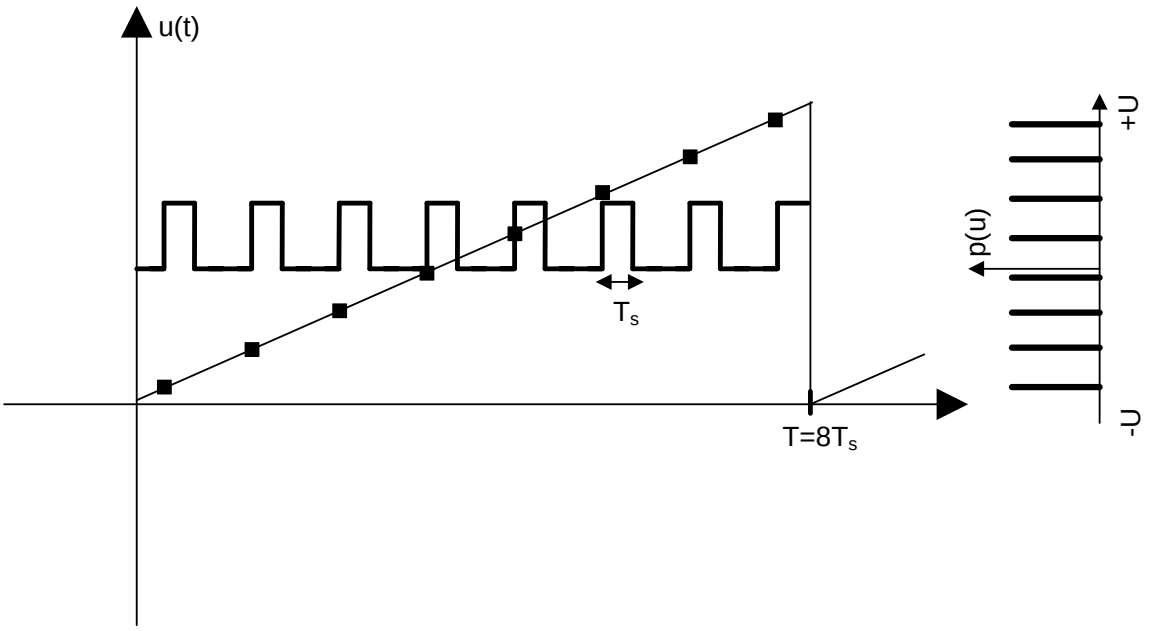
Параметри које је могуће варирати у новом симулационом моделу су:

- одабир таласног облика напона (тестера или троугао)
- периода тестерастог (троугаоног) напона,
- амплитудски опсег тестерастог (троугаоног) напона,
- број бита LFSR-а (8, 16 и 32 бита),
- одабир типа провере парности у повратној спрези LFSR-а ( ексклузивно или (XOR) или ексклузивно нили (XNOR) ),
- постављање иницијалне вредности регистра како не би дошло до недозвољених стања,
- одабир места са којих се узима сигнал за повратну спрегу за разне дужине померачког регистра, а које обезбеђују максималну дужину секвенце,
- одабир конкретних бита са излаза LFSR-а на основу којих се формира дигитални излаз,
- однос фреквенција тестерастог (троугаоног) напона и фреквенције дигиталног сигнала којим се врши одабирање,
- периода jitter-а и
- индекс модулације jitter-а у релативном облику.

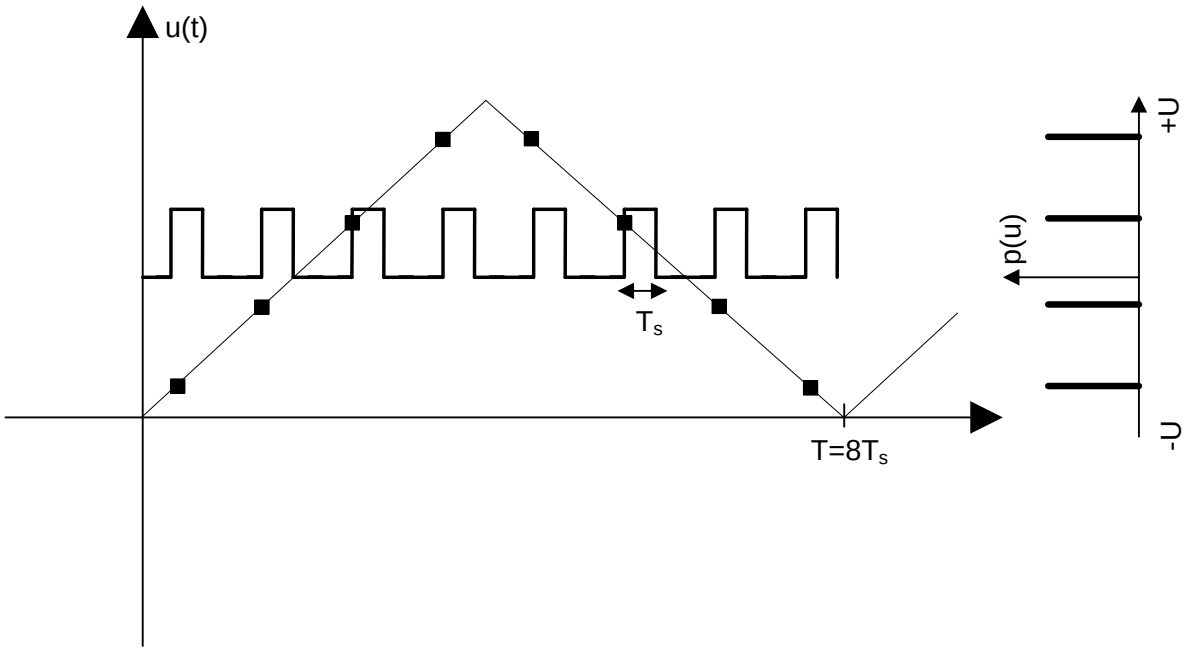
## 6.1 Резултати симулације

У симулацији је разматран тестерасти и троугаони таласни облик напона. Тестерасти напон је од интереса за теоријску анализу. У хардверском генератору је коришћен троугаони напон, из разлога његове лакше реализације у односу на тестерасти напон. Предложена метода је примењива на оба таласна облика напона, уз напомену да се за троугаони напон добија дупло мањи број дискретних вредности.

На слици 6.1.1 и 6.1.2 је приказан случај одабирања тестерастог и троугаоног напона дигиталним сигналом 8 пута веће учестаности и добијених 8 дискретних вредности у случају тестерастог напона и 4 дискретне вредности у случају троугаоног напона.




**Слика 6.1.1 Приказ тестерастог напона и дигиталног сигнала осам пута веће фреквенције којим се врши одабирање**



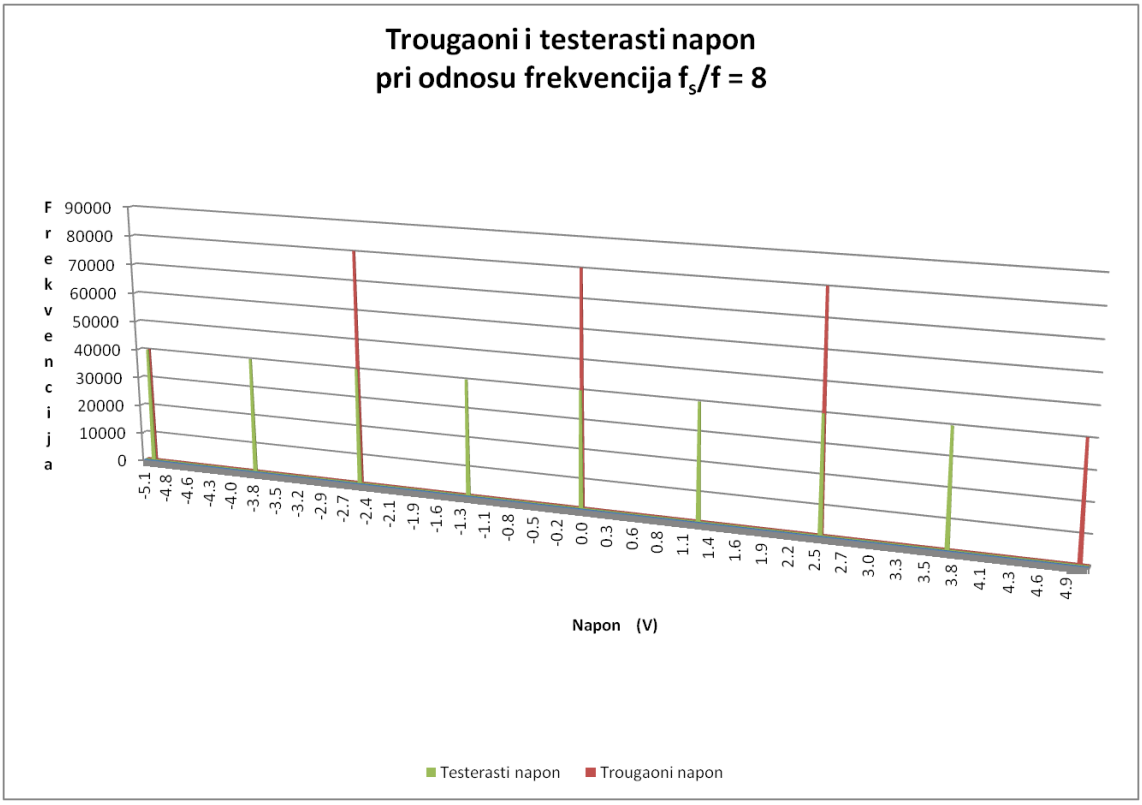

**Слика 6.1.2 Приказ троугаоног напона и дигиталног сигнала осам пута веће фреквенције којим се врши одабирање**

У наставку су приказани резултати симулација уз варирање неколико параметара:

- Однос фреквенција тестерастог (троугаоног) сигнала и дигиталног сигнала којим се врши одабирање,
- вредност jittera-а (расипање услед раздешености фазно закључане петље ) ,
- однос периода тестерастог (троугаоног) сигнала и периоде jitter-а.

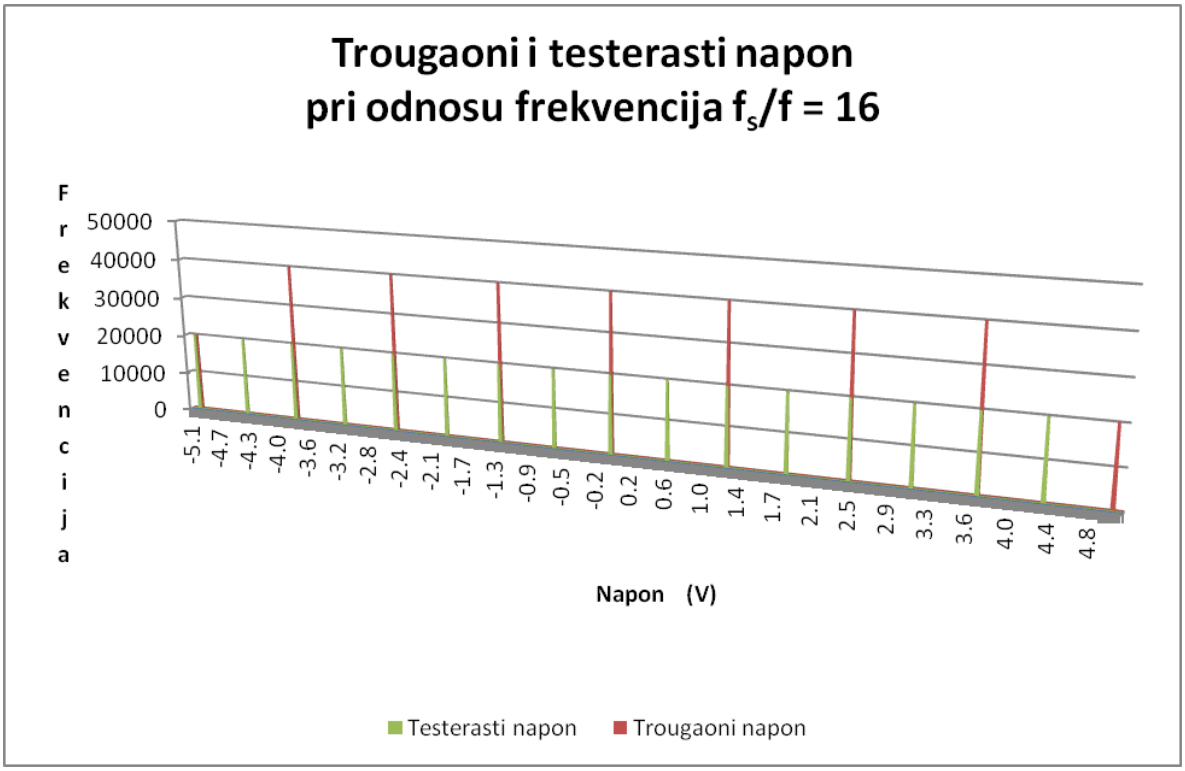
За све приказане резултате генерисано је 320000 излазних вредности.

Као што је у предложеној методи наглашено на самом старту постоји могућност да је однос фреквенције тестерастог (троугаоног) напона и фреквенције дигиталног сигнала $f_s/f$ којим се овај напон одабира целобројан. У овом случају број излазних вредности $N$ се може повећати једино ако се повећа вредност фреквенције дигиталног сигнала (велике вредности фреквенције $f_s$ представљају значајан проблем при практичној реализацији), што је илустровано на сликама 6.1.3 , 6.1.4 и 6.1.5.



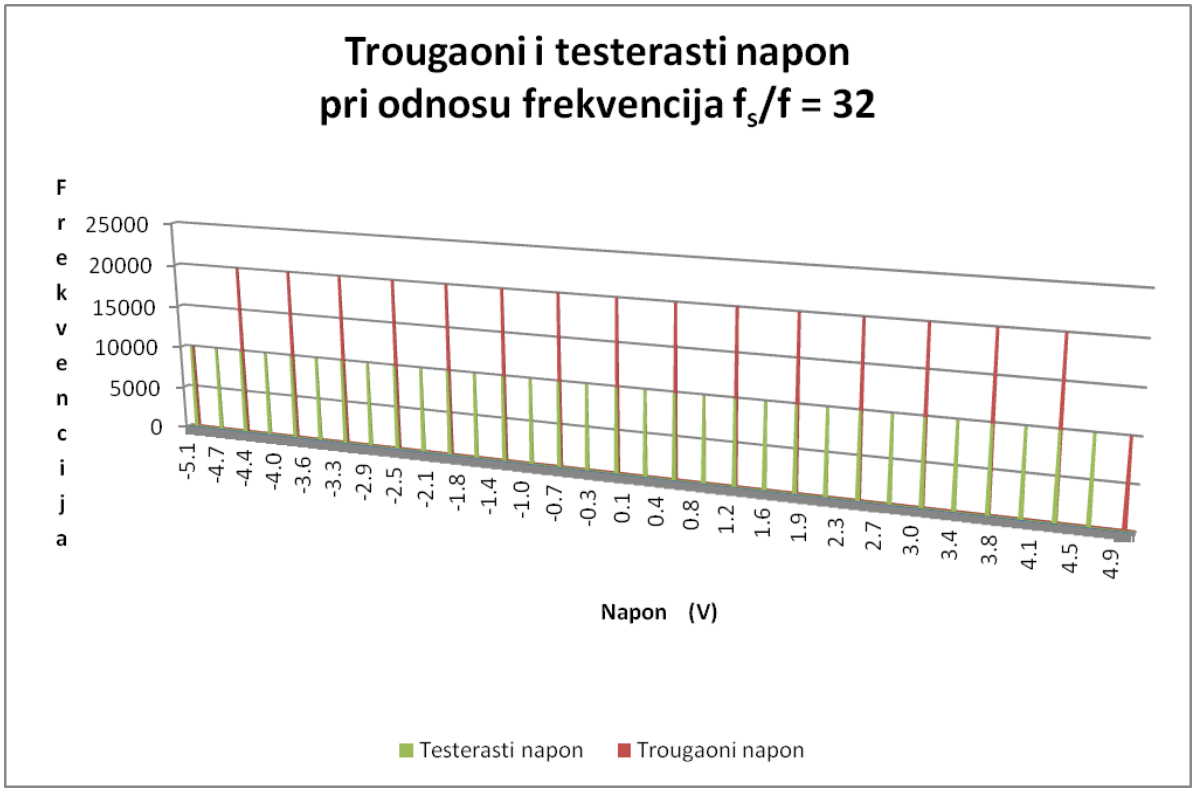

**Слика 6.1.3 Хистограм вредности троугаоног и тестерастог напона у случају целобројног односа фреквенција $f_s/f$ =8 за симулираних 320000 резултата**

На слици 6.1.3 је приказано 8 дискретних вредности за тестерасти напон (иста фреквенција понављања, али су на 5 места прекривени вредностима троугаоног напона) и 5 дискретних вредности троугаоног напона.




**Слика 6.1.4 Хистограм вредности троугаоног и тестерастог напона у случају целобројног односа фреквенција $f_s/f$ =16 за симулираних 320000 резултата**

На слици 6.1.4 је приказано 16 дискретних вредности за тестерасти напон и 9 дискретних вредности троугаоног напона.

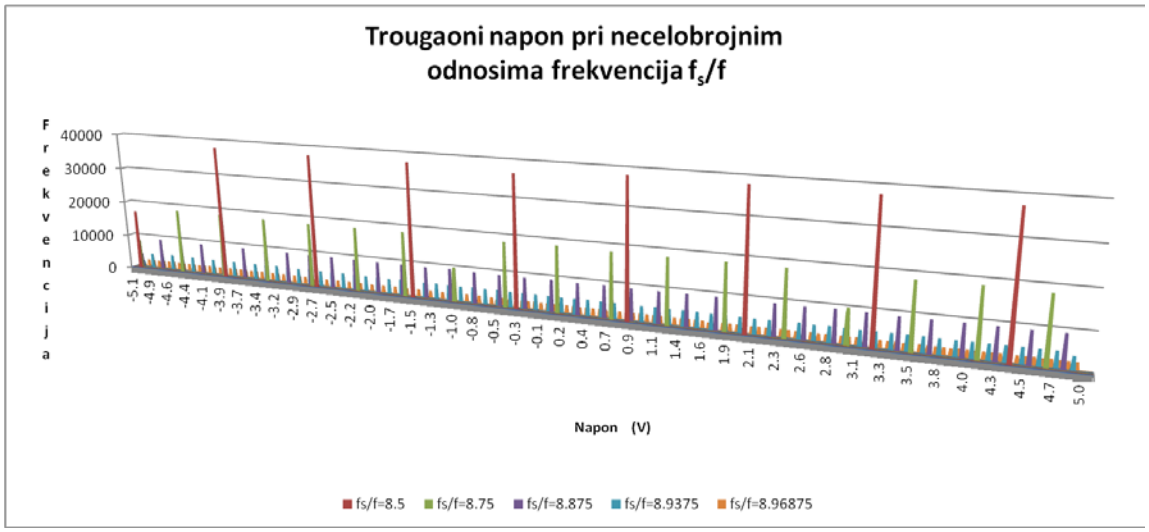



**Слика 6.1.5 Хистограм вредности троугаоног и тестерастог напона у случају целобројног односа фреквенција $f_s/f$ =32 за симулираних 320000 резултата**

На слици 6.1.5 су приказане 32 дискретне вредности за тестерасти напон и 17 дискретних вредности троугаоног напона.

Прво побољшање предложено у новој методи, које доводи до повећања броја могућих дискретних вредности при незнатном повећању фреквенције дигиталног сигнала *fs* јесте одабир нецелобројног односа фреквенција *f* и $f_s$. Примери различитих односа фреквенција и одговарајућег-повећаног броја дискретних вредности које се добијају је дат у поглављу 5 у табели 5.1.

На слици 6.1.6 је приказано поређење хистограма троугаоног напона за нецелобројне вредности односа фреквенција $f_s/f$ из скупа (8.5, 8.75, 8.875, 8.9375, 8,96875).

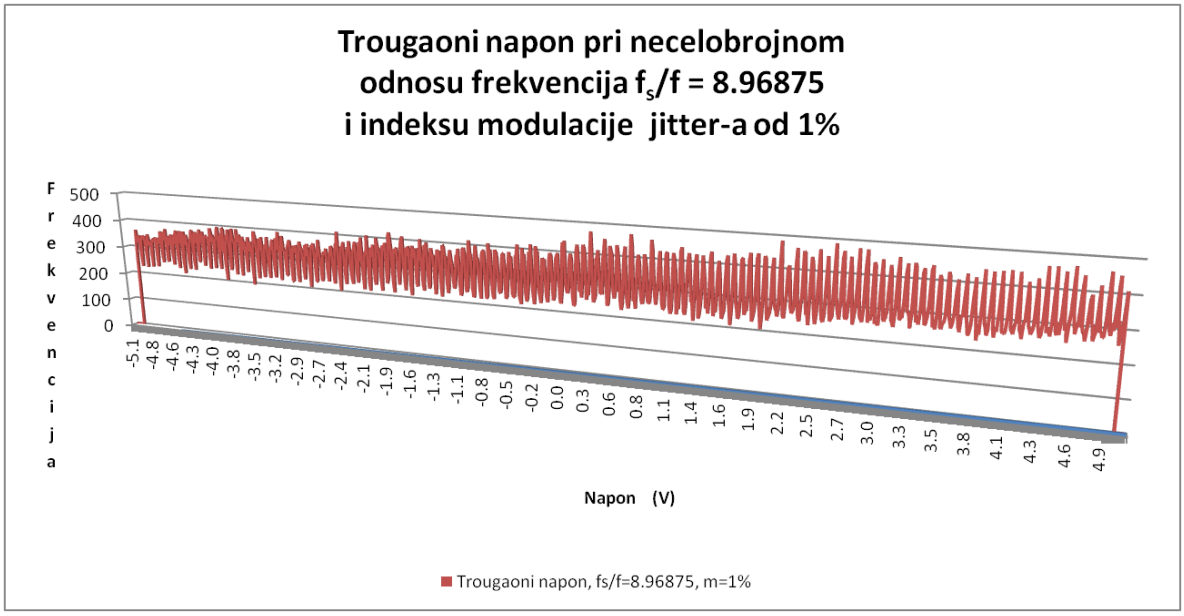



**Слика 6.1.6 Поређење хистограма вредности троугаоног напона у случају нецелобројног односа фреквенција $f_s/f$ за симулираних 320000 резултата**

Уочљиво је да се са повећањем нецелобројног односа фреквенција *f* и $f_s$ (како тај односи тежи $f_s/f = 9$) повећава и број добијених дискретних вредности. У поглављу 4 је показано да се са сваком следећом нецелобројном вредности број могућих вредности приближно дуплира, што је аналогно добитку од 1 бита.

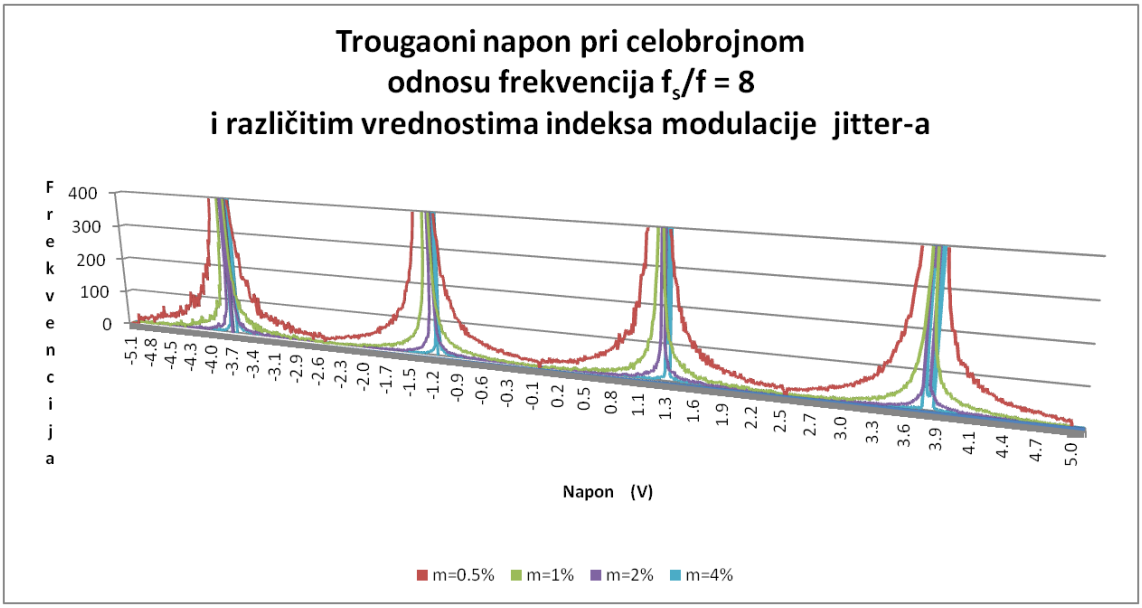
Друго побољшање се односи на увођење jitter- а, чиме се омогућава модулисање могућих тренутака одабирања тестерастог сигнала и као резултат се добија теоретски неограничен број добијених дискретних вредности.

На слици 6.1.7 је приказан хистограм троугаоног напона са нецелобројним односом фреквенција $f_s/f$=8.96875 и индексом модулације jitter-а *m* од 1%.




**Слика 6.1.7 Хистограм вредности троугаоног напона у случају нецелобројног односа фреквенција $f_s/f$ = 8.96875 и вредности индекса модулације jitter-a од 1 % за симулираних 320000 резултата**

У циљу јасног приказа утицаја вредности индекса модулације jitter-a на слици 6.1.8 је дато поређење хистограма троугаоног напона за целобројни однос фреквенција $f_s/f$=8 и четири различите вредности индекса модулације jitter-a $m$. Слика показује добијање читавог опсега уместо једне дискретне вредности, како то теоријско разматрање предвиђа. У зависности од индекса модулације jitter-a, приказани су опсези у којима се расипају одбирци. Намерно је узета ситуација где је однос учестаности целобројан и износи 8, те се добија мали број дискретних вредности. При односима учестаности које производе већи број дискретних вредности долази до преклапања опсега и на тај начин до уједначавања хистограма.




**Слика 6.1.8 Поређење хистограма вредности троугаоног напона у случају целобројног односа фреквенција $f_s/f$ = 8 и различитих вредности индекса модулације jitter-а за симулираних 320000 резултата**

# 7. ВАЛИДАЦИЈА СИМУЛАЦИОНОГ МОДЕЛА ГЕНЕРАТОРА ДИСКРЕТНОГ АНАЛОГНОГ УНИФОРМНОГ ШУМА

У циљу валидације реализованог симулационог модела генератора дискретног аналогног униформног шума искоришћен је општеприхваћени и најчешће коришћени софтверски пакет развијен од стране Америчког националног Института за стандарде и технологију (NIST).

Овај софтверски пакет садржи сет од петнаест наменски развијених статистичких тестова који се користе како би се добила информација о квалитету реализованог генератора случајних бројева. Циљ је утврђивање постојања девијације у односу на праву случајност у бинарним секвенцама генерисаних података.

Да би се поменути софтверски пакет могао искористити, генератор случајних бројева мора на свом излазу генерисати бинарни низ нула и јединица одговарајуће дужине.

Прегледом литературе посвећене тестирању генератора случајних бројева [48-56], одлучено је да се за валидацију реализованог симулационог модела користи 6 тестова.

Примењени су следећи статистички тестови:

- Frequency (Monobit) Test,
- Frequency Test Within a Block,
- Runs Test (Oscillation Test),
- Longest Run of Ones in Block,
- Binary Matrix Rank Test и
- Discrete Fourier Transform Test.

Опис сваког од коришћених тестова, као и препоручени начини за тумачење резултата добијених њиховом применом су дати у Прилогу "Преглед коришћених статистичких тестова у оквиру NIST софтверског пакета".

## 7.1 Приказ резултата валидације

За валидацију предложене методе и развијеног симулационог модела искоришћена је верзија NIST SP 800-22 софтверског пакета статистичких тестова са графичким интерфејсом у оквиру Windows оперативног система.

Имајући у виду 6 одабраних тестова и захтеве који сваки од њих намеће, симулацијом је креиран фајл са 1000 бинарних секвенци, од којих је свака дужине 1024 бита (1024000 вредности). Над ових 1024000 вредности су спроведени сви статистички тестови и добијени резултати су приказани сумарно у табели 7.1.

**Табела 7.1 Сумарни приказ резултата статистичких тестова**

| Назив статистичког теста | P вредност | % од укупног броја бинарних секвенци које су прошле дати тест |
|---|---|---|
| Frequency (Monobit) Test | 0.950165 | 98.9 |
| Frequency Test Within a Block | 0.983752 | 99.5 |
| Runs Test | 0.952591 | 97.1 |
| Longest Run of Ones in Block | 1 | 100 |
| Binary Matrix Rank Test | 0.69372 | 100 |
| Discrete Fourier Transform Test | 0.935354 | 100 |

Сви статистички тестови су формулисани тако да проверавају нулту хипотезу $H_0$. Нулта хипотеза у свим спроведеним тестовима је формулисана као претпоставка да је испитивана бинарна секвенца случајна. Алтернативна хипотеза $H_A$ претпоставља да испитива бинарна секвенца није случајна. Након сваког теста се доноси одлука да ли се нулта хипотеза прихвата или одбацује. За предефинисани ниво поверења у свим тестовима $\alpha = 0.01$ очекује се да се код стварно случајних генератора одбаци 1 у 100 тестираних секвенци. *P* вредност представља параметар чија вредност се користи како би се прихватила или одбацила нулта хипотеза. Што је мања вредност параметра *P* то се сматра да је већа оправданост одбацивања нулте хипотезе. При тестирању хипотезе

се вредност параметра $P$ пореди са одабраном вредности нивоа поверења α и уколико је $P \leq \alpha$ нулта хипотеза се одбацује, а уколико је $P > \alpha$ нулта хипотеза се прихвата.

То значи да је при тестирању хипотезе у описаном тестирању потребно да вредност параметра $P$ буде већа од нивоа поверења $\alpha$, како би нулта хипотеза - да је тестирана секвенца заиста случајна, била прихваћена.

У табели 7.1 су приказане вредности параметра $P$ за све тестове. Поређењем са одабраним новом поверења који за све тестове износи $\alpha = 0.01$ констатује се да се са великом вероватноћом у свим тестовима прихвата нулта хипотеза, тј. да је испитивана секвенца генерисаних вредности заиста случајна.

Други параметар који је приказан у табели је однос у процентима секвенци (од тестираних 1000) које су прошле и оних које нису прошле дати тест.

# 8. РЕКАПИТУЛАЦИЈА РАДА

У уводном поглављу је описан проблем који је био тема истраживања. Наведени су тренутно актуелни начини генерисања дитерских сигнала и сагледане су њихове предности и мане. Наглашено је да од квалитета генерисаног дитерског сигнала директно зависи квалитет конверзије аналогне у стохастичку величину. Дефинисан је циљ истраживања и формулисана је хипотеза.

У другом поглављу су приказане предности мерења на интервалу у односу на мерење у тачки. Дат је преглед стохастичке дигиталне мерне методе уз осврт на значај примене дитерских сигнала. Наведена су и описана досадашња решења базирана на стохастичкој мерној методи.

Треће поглаље се бави дефиницијом појма ефективне резолуције стохастичких мерних инструмената. Објашњена је веза између ефективне резолуције стохастичког А/Д конвертора и примењеног дитера (дискретног аналогног шума унифромне расподеле). У другом делу поглавља је приказана анализа утицаја једне систематске грешке на резултат мерења: коначне резолуције Д/А конвертора којим се генерише дитерски сигнал. Ова анализа је послужила као мотив за формулисање нове методе за генерисање дитерских сигнала који немају коначну резолуцију.

У четвртом поглављу је описан значај употребе дитерских сигнала у оквиру стохастичке дигиталне мерне методе. Дат је приказ најзначајнијих метода за реализацију псеудослучајних и истински случајних генератора шума са посебним освртом на померачке регистре са линеарном повратном спрегом.

Пето поглавље се бави формулацијом нове, оригиналне методе за генерисање дитерских сигнала. Нова метода је заснована на асинхроном одабирању тестерастог или троугаоног напона. Теоријски је показано да предложена метода генерисања обезбеђује дитерски сигнал бесконачне резолуције. Директна последица је повећање ефективне резолуције стохастичких мерних инструмената.

У шестом поглављу је описан нови симулациони модел, као и претходни кораци у истраживању који су довели до његовог развоја. Приказана је анализа резултата добијених симулацијом и наглашен је значај могућности варирања низа параметара приликом симулације којима се директно утиче на квалитет рада генератора дитерског сигнала. Резултати добијени симулацијом потврђују могућност генерисања дитерских сигнала практично бесконачне резолуције.

Седмо поглавље је посвећено валидацији реализованог симулационог модела. Како би се добила представа о квалитету предложеног генератора, искоришћен је софтверски пакет статистичких тестова NIST SP 800-22. Презентовани су подаци добијени валидацијом и на основу резултата статистичких тестова закључено је да је испитивана секвенца вредности генерисаних од стране предложеног генератора заиста случајна.

У прилогу је описан реализовани хардверски прототип генератора дискретног аналогног униформног шума(дитерског сигнала). Прототип је развијен са циљем провере предложене методе. Приказани резултати потврђују да је могућ развој хардверског генератора дискретног аналогног униформног шума заснованог на теоријским принципима приказаним у дисертацији.

# 9. ЗАКЉУЧАК

У оквиру истраживања тезе "Нова метода за повећање ефективне резолуције стохастичких мерних инструмената високих перформанси" анализиран је математички модел стохастичког адиционог А/Д конвертора, развијене су две врсте симулационих модела и анализирано је хардверско решење генератора ради провере исправности предложене методе.

Прве симулације су реализоване са циљем да се моделује понашање стохастичког адиционог флеш А/Д конвертора са два генератора дитера (СААДК2Г) у зависности од резолуције употребљеног Д/А конвертора.

Мотивација за формулисање нове методе генерисања дитерских сигнала је добијена узимањем у обзир анализе утицаја систематских грешака на грешку мерења стохастичког адиционог А/Д конвертора приказане у трећем поглављу тезе.

У тези је дат предлог нове методе генерисања дитера (дискретног аналогног униформног шума) засноване на примени LFSR структуре и нееквидистантном одабирању тестерастог напона.

Главна добит предложене методе јесте избегавање коришћења Д/А конвертора, што поједностављује и чини економски приступачнијом изведбу генератора дитерског сигнала неопходног у стохастичкој дигиталној мерној методи. Такође предност је што се применом предложене методе добијају вредности напона из континуалног уместо дискретног скупа.

Након провере предложене методе симулационим путем реализовано је хардверско решење генератора дискретног аналогног шума описаног у прилогу: "Хардверско решење генератора дискретног аналогног униформног шума". Хардверско решење је развијено у сврху провере концепта.

Услед немогућности подешавања довољног броја параметара при генерисању дитера и одсуства комерцијалног хардвера којим би се могао валидовати реализовани

генератор одлучено је да се приступи изради новог, детаљнијег и реалистичнијег симулационог модела.

У новом симулационом моделу је дата могућност варијације великог броја параметара. Добијени су резултати уз варирање неколицине доступних параметара. Графички приказани резултати симулације су потврдили хипотезу изнесену у уводу, да је употребом предложене методе за генерисање дитерских сигнала могуће постићи повећање ефективне резолуције инструмената базираних на стохастичкој дигиталној мерној методи.

На крају је спроведена валидација резултата добијених симулацијом применом општеприхваћеног софтверског пакета статистичких тестова за тестирање квалитета случајних и псеудослучајних генератора случајних бројева, развијеног од стране Америчког националног Института за стандарде и технологију (NIST).

Резултати валидације су потврдили да се симулацијом заснованом на предложеној методи добијају вредности које се могу сматрати случајним.

Логични правци даљег истраживања су даљи рад на симулацији варирањем преосталих параметара, затим евалуацији резултата и израда новог хардверског генератора дитерског сигнала. У сврху коначне потврде валидности предложене методе било би потребно реализовати два засебна генератора дитерског сигнала и спровести њихову интеграцију у реализовани хардвер двобитног стохастичког бројила електричне енергије, описан у [11], како би се могли поредити резултати мерења добијени уз употребу дитерских сигнала генерисаних стандардном методом и дитера генерисаних хардвером заснованим на методи предложеној у тези.

# 10. ЛИТЕРАТУРА

[1] J. Neškudla, J. Vedral, "Digitaly controlled white noise generator", 2006. URL:http://www.imeko.org/publications/wc-2006/PWC-2006-TC4-IWADC-008u.pdf (31.01.2016.).

[2] S. L. Toral, J. M. Quero, L. G. Franquelo, "Stochastic pulse coded arithmetic", Circuits and Systems, Proceedings ISCAS 2000. The 2000 IEEE International Symposium (Volume:1), Geneva, pp 599 - 602.

[3] J. Vedral, J. Holub, "Oscilloscope testing by means of stochastical signal", URL: http://www.measurement.sk/PAPERS/Vedral.pdf (31.01.2016.)

[4] D. Pejic, V. Vujicic, "Accuracy limit of high precision stochastic watt-hour meter", Instrumentation and Measurement, IEEE Transactions (Volume: 49, Issue: 3), June 2000, pp. 617-620, doi: 10.1109/19.850404.

[5] G. D'Antona, A. Ferrero, " Digital Signal Processing for Measurement Systems", Springer US, 2006.

[6] V.Vujičić, I. Župunski, Z. Mitrović, M. Sokola, "Measurement in a point versus measurement over an interval", Proceedings of the IMEKO XIX World Congress, Lisbon, Portugal, 2009, pp. 1128-1132.

[7] H. Nyquist, "Certain topics in telegraph transmission theory". Trans. AIEE. 47: 617–644,doi:10.1109/t-aiee.1928.5055024, April 1928.

[8] C.E. Shannon, "Communication in the presence of noise". Proceedings of the Institute of Radio Engineers, 37 (1): 10-21. doi:10.1109/jproc.1949.232969, January 1949.

[9] P. Poljak, " Prilog razvoju i standardizaciji mernih metoda u merenjima u tački i merenjima na intervalu", doktorska disertacija, Fakultet tehničkih nauka, Novi Sad, 2013.

[10] B. Widrow, "Statistical Analysis of Amplitude-Quantized Sampled -Data Systems", Trans. AIEE (Applications and Industry), vol. 79, pp. 555-568, 1960.

[11] D. Pejić, "Stohastičko merenje električne snage i energije ", doktorska disertacija, Fakultet tehničkih nauka, Novi Sad, 2010.

[12] D. Pejić, N. Gazivoda, B. Ličina, M. Urekar, P. Sovilj, B. Vujičić, "A Proposal of a Novel Method for GeneratingDiscrete Analog Uniform Noise", Advances in Electrical and Computer Engineering, Vol. 18, No. 3, doi: 10.4316/AECE.2018.03009, 2018.

[13] N. Pjevalica, "Merenja u elektrodistributivnoj mreži u frekvencijskom domenu", doktorska disertacija, Fakultet tehničkih nauka, Novi Sad, 2007.

[14] J. Tomić, "Integrisano merilo harmonika", magistarski rad, Fakultet tehničkih nauka, Novi Sad, 2004.

[15] В. Пјевалица, "Стохастички дигитални процесор ортогоналних трансформација", докторска дисертација, Факултет техничких наука, Нови Сад, 2008.

[16] Park, S.K. and Miller, K.W., 1988. Random number generators: good ones are hard to find. Communications of the ACM, 31(10), pp.1192-1201.

[17] L'ecuyer, P., 1988. Efficient and portable combined random number generators. Communications of the ACM, 31(6), pp.742-751.

[18] MacLaren, M.D. and Marsaglia, G., 1965. Uniform random number generators. Journal of the ACM (JACM), 12(1), pp.83-89.

[19] L'ecuyer, P., 1999. Good parameters and implementations for combined multiple recursive random number generators. Operations Research, 47(1), pp.159-164.

[20] Hull, T.E. and Dobell, A.R., 1962. Random number generators. SIAM review, 4(3), pp.230-254.

[21] Marsaglia, G., Zaman, A. and Tsang, W.W., 1990. Toward a universal random number generator. Stat. Prob. Lett., 9(1), pp.35-39.

[22] Jun, B. and Kocher, P., 1999. The Intel random number generator. Cryptography Research Inc. white paper, 27, pp.1-8.

[23] Blum, L., Blum, M. and Shub, M., 1986. A simple unpredictable pseudo-random number generator. SIAM Journal on computing, 15(2), pp.364-383.

[24] Hellekalek P. Good random number generators are (not so) easy to find. Mathematics and Computers in Simulation. 1998 Jun 1;46(5-6):485-505.

[25] OISHI, S.I. and INOUE, H., 1982. Pseudo-random number generators and chaos. IEICE TRANSACTIONS (1976-1990), 65(9), pp.534-541.

[26] Kelsey, J., Schneier, B. and Ferguson, N., 1999, August. Yarrow-160: Notes on the design and analysis of the yarrow cryptographic pseudorandom number generator. In International Workshop on Selected Areas in Cryptography(pp. 13-33). Springer, Berlin, Heidelberg.

[27] McEvoy, R., Curran, J., Cotter, P. and Murphy, C., 2006. Fortuna: cryptographically secure pseudo-random number generation in software and hardware.

[28] Rose, G.G., Gantman, A. and Xiao, L., Qualcomm Inc, 2011. Cryptographically secure pseudo-random number generator. U.S. Patent 8,019,802.

[29] M. Stipčević, C. K. Koc,"True Random Number Generators", Open Problems in Mathematics and Computational Science,University of California Santa Barbara, DOI: 10.1007/978-3-319-10683-0_12, 2014.

[30] A. Peinado, A. Fúster-Sabater, "Generation of pseudorandom binary sequences by means of linear feedback shift registers (LFSRs) with dynamic feedback", Mathematical and Computer Modelling, Vol. 57, pp.2596-2604, 2013.

[31] Donald E. Knuth, The Art of Computer Programming, Volume 3, Sorting and Searching.

[32] A. Kerckhoffs. La cryptographie militaire. Journal des sciences militaires, IX, 1883.

[33] J. B. Johnson, "Thermal Agitation of Electricity in Conductors", Nature, Vol. 119, pp. 50–51, 1927.

[34] J.B. Johnson, "Thermal Agitation of Electricity in Conductors", Physics Review, Vol. 32, pp. 97-109, 1928.

[35] H. Nyquist, “Thermal agitation of electric charge in conductor,” Physics Review, Vol. 32, , pp. 110-113, 1928.

[36] P.I. Somlo, "Zener-diode noise generators", Electronics Letters,DOI: 10.1049/el:19750219, 1975.

[37] C. D. Motchenbacher, F. C. Fitchen, "Low-Noise Electronic Design", New York:Wiley, 1973.

[38] A. Konczakowska, B. M. Wilamowski, "Noise in Semiconductor Devices", Gdansk University of Technology, Auburn University, 2010.

[39] F.N. Hooge, "1/f noise sources", IEEE Transactions on Electron Devices, Vol. 41, pp.1926-1935, 1994.

[40] A. Abdipour, G. Moradi, S. Saboktakin, "Design and implementation of a noise generator" RF and Microwave Conference, pp. 472-474, 2008.

[41] V. Bagini, M. Bucci, "A design of reliable true random number generator for cryptographic applications" International Workshop on Cryptographic Hardware and Embedded Systems, pp. 204-218, Springer, Berlin, Heidelberg, 1999.

[42] T. Stojanovski, L. Kocarev, "Chaos-based random number generators-part I: analysis [cryptography]", IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, Vol. 48, pp.281-288, 2001.

[43] T. Stojanovski, L. Kocarev, "Chaos-based random number generators. Part II: practical realization", IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, Vol. 48, pp.382-385, 2001.

[44] Y. Wang, P. Li, J. Zhang, "Fast random bit generation in optical domain with ultrawide bandwidth chaotic laser", IEEE Photonics Technology Letters, Vol. 22, pp.1680-1682, 2010.

[44] R.S. Tebble, I.C. Skidmore, W.D. Corner, "The Barkhausen effect", Proceedings of the Physical Society. Section A, Vol. 63, p.739, 1950.

[46] F. Pareschi, G. Setti, R. Rovatti, "Implementation and testing of high-speed CMOS true random number generators based on chaotic systems", IEEE transactions on circuits and systems I: regular papers, Vol. 57, pp.3124-3137, 2010.

[47] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, A. Zeilinger, "A fast and compact quantum random number generator", Review of Scientific Instruments, Vol. 71, pp. 1675-1680, 2000.

[48] J. Soto, "Statistical testing of random number generators",In *Proceedings of the 22nd National Information Systems Security Conference* ,Vol. 10, No. 99, p. 12, Gaithersburg, 1999.

[49] S.J. Kim, K. Umeno, A. Hasegawa, "Corrections of the NIST statistical test suite for randomness".,*arXiv preprint nlin/0401040*, 2004.

[50] F. Pareschi, R. Rovatti, G. Setti, "Second-level NIST randomness tests for improving test reliability", IEEE International Symposium on Circuits and Systems, pp. 1437-1440), 2007.

[51] F. Pareschi, R. Rovatti, G. Setti, "On statistical tests for randomness included in the NIST SP800-22 test suite and based on the binomial distribution", IEEE Transactions on Information Forensics and Security, *7*(2), pp.491-505, 2012.

[52] L.E. Bassham III, A.L. Rukhin, J. Soto, J.R. Nechvatal, M.E. Smid, E.B. Barker, S.D. Leigh, M. Levenson, M. Vangel, D.L. Banks, N.A. Heckert, "Sp 800-22 rev. 1a. a statistical test suite for random and pseudorandom number generators for cryptographic applications", 2010.

[53] E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications", National Institute of Standards and Technology, 2000.

[54] K. Hamano, T. Kaneko, "Correction of overlapping template matching test included in NIST randomness test suite", IEICE transactions on fundamentals of electronics, communications and computer sciences, 90(9), pp.1788-1792, 2007.

[55] S. Murphy, "The power of NIST's statistical testing of AES candidates", Preprint. January, 17, 2000.

[56] K. Marton, A. Suciu, "On the interpretation of results from the NIST statistical test suite", Science and Technology, 18(1), pp.18-32, 2015.

[57] K. L. Chung, "Elementary Probability Theory with Stochastic Processes", New York: SpringerVerlag, 1979.

[58] J. Pitman, "Probability", New York: Springer-Verlag, 1993.

[59] N. Maclaren, "Cryptographic Pseudo-random Numbers in Simulation," Cambridge Security Workshop on Fast Software Encryption. Dec. 1993.

[60] D. E. Knuth, "The Art of Computer Programming. Vol 2: Seminumerical Algorithms", 3rd ed. Reading, Mass: Addison-Wesley, 1998.

[61] M. Abramowitz, I. Stegun, "Handbook of Mathematical Functions: NBS Applied Mathematics Series 55", Washington, D.C.: U.S. Government Printing Office, 1967.

[62] J. D. Gibbons, "Nonparametric Statistical Inference", 2nd ed. New York: Marcel Dekker, 1985.

[63] A. P. Godbole, S. G. Papastavridis, "Runs and patterns in probability: Selected papers", Dordrecht: Kluwer Academic, 1994.

[64] F. N. David, D. E. Barton, "Combinatorial Chance", New York: Hafner Publishing Co., 1962.

[65] P. Revesz, "Random Walk in Random and Non-Random Environments", Singapore: World Scientific, 1990.

[66] G. Marsaglia, "DIEHARD: a battery of tests of randomness", http://www.stat.fsu.edu/pub/diehard/.

[67] I. N. Kovalenko, “Distribution of the linear rank of a random matrix”, Theory of Probability and its Applications. 17, pp. 342-346, 1972.

[68] G. Marsaglia, L. H. Tsay, “Matrices and the structure of random number sequences”, Linear Algebra and its Applications. Vol. 67, pp. 147-156, 1985.

[69] R. N. Bracewell, "The Fourier Transform and Its Applications", New York: McGraw-Hill, 1986.

[70] W. Killman, J. Schüth, W. Thumser, I. Uludag, "A Note Concerning the DFT Test in NIST Special Publication 800-22", T-Systems, Systems Integration, July 2004.

[71] Đ. Novaković, "Generator pseudoslučajnog napona", projektni rad, Fakultet tehničkih nauka, 2017.

# ПРИЛОЗИ

# 1. Преглед коришћених статистичких тестова у оквиру NIST софтверског пакета

### 1. Frequency (Monobit) Test

Фокус овог теста је на пропорцији нула и јединица у целој секвенци. Сврха овог теста је одређивање да ли је број јединица и нула у секвенци приближно исти, као што би се очекивало од истински случајне секвенце. Тест процењује у којој мери је удео јединица у секвенци близак вредности од 50%. Како би хипотеза да се ради о стварно случајној секвенци била потврђена број јединица и нула у секвенци треба да буду приближно исти. Сви наредни тестови се ослањају на овај и ако тестирана секвенца не прође тест остали се ни не извршавају и аутоматски се генерише извештај да је пала и на свим осталим тестовима.

Тест се извршава тако што се битови који имају вредност 0 претварају у вредност -1, док се јединице претварају у вредност +1 и врши се сумирање свих добијених вредности.

$$S_n = X_1 + X_2 + ... + X_n$$

Затим се резултат теста израчунава као количник апсолутне вредности суме $S_n$ и квадратног корена из броја $n$ који представља дужину испитиване секвенце.

$$S_{obs} = \frac{|S_n|}{\sqrt{n}}$$

На основу испитивања хипотезе и посматране вредности се прорачунава $P$ вредност.

Уколико је вредност *P* мања од нивоа поверења $\alpha$ (предефинисана вредност је увек $\alpha$=0.01) закључује се да секвенца није случајна.

Препорука је да се за овај тест користи секвенца дужине најмање 100 бита.

Узевши у обзир да је ниво поверења $\alpha$=0.01, потребно је за сваки тест урадити 100 различитих секвенци [57-58].

## 2. Frequency Test within a Block

Фокус овог теста је на пропорцији јединица унутар M-битног блока. Проверава се да ли је број понављања јединица унутар блока M приближно једнак M/2, као што би се очекивало под претпоставком случајности испитиване секвенце.

Улазна секвенца дужине n се дели у N непреклапајућих блокова, где је $N = \left\lfloor \frac{n}{M} \right\rfloor$.

Пропорција јединица унутар M-битног блока се добија применим $\chi^2$ теста. На основу пропорције се прорачунава *P* вредност.

Уколико је вредност *P* мања од нивоа поверења $\alpha$ закључује се да секвенца није случајна.

Препорука је да се за овај тест користи секвенца дужине најмање 100 бита уз услов да је $n \geq NM$ [59-61].

### 3. Runs Test

У овом тесту је фокус на проналажењу укупног броја секвенци бита исте вредности унутар испитиване секвенце. Проверава се да ли је број оваквих секвенци бита истих вредности различитих дужина за јединице и нуле одговара очекиваном броју за истински случајну секвенцу.

Да би тест започео секвенца прво мора на почетку проћи Frequency (Monobit) тест. Уколико је овај услов задовољен прорачунава се *P* вредност.

Уколико је вредност *P* мања од нивоа поверења $\alpha$ закључује се да секвенца није случајна.

Препорука је да се за овај тест користи секвенца дужине најмање 100 бита.

Очекивана је ситуација да унутар испитиване секвенце долази до што чешће осцилације секвенци бита исте вредности [62-63].

### 4. Test for the Longest Run of Ones in a Block

Овај тест се своди на проналажење најдуже секвенце јединица унутар M-битног блока у испитиваној секвенци. Проверава се да ли дужина најдуже секвенце јединица унутар испитиване секвенце одговара вредности која се очекује за истински случајну секвенцу. Уколико се констатује нерегуларност везана за најдужу секвенцу јединица иста нерегуларност аутоматски важи и за најдужу секвенцу нула унутар испитиване секвенце.

Тест има три предефинисане вредности за број бита од којих се може састојати блок M : 8, 128 и 10000. У складу са тим се мора одабрати и једна од три вредности за број бита испитиване секвенце: 128, 6272 или 750000.

Након проналажења фреквенције понављања јединица у секвенцама унутар сваког блока одређује се пропорција јединица унутар M-битног блока применим $\chi^2$ теста. На основу пропорције се прорачунава *P* вредност.

Уколико је вредност $P$ мања од нивоа поверења $\alpha$ закључује се да секвенца није случајна.

Велике вредности добијене $\chi^2$ тестом индикују да се унутар испитиване секвенце налазе предугачки кластери јединица [64-65].

### 5. Test for the Longest Run of Ones in a Block

Тест се своди на проналажење ранга дисјунктних под-матрица целокупне секвенце. Тражи се линеарна зависност између поднизова фиксне дужине унутар испитиване секвенце.

Улазна секвенца дужине n се дели у MxQ-битних непреклапајућих блокова, где је број резултујућих блокова $N = \left[ \frac{n}{MQ} \right]$. M представља број редова унутар сваке MxQ матрице и у овом тесту има предефинисану вредност M=32. Q представља број колона унутар сваке MxQ матрице и у овом тесту има предефинисану вредност Q=32.

Одређује се ранг сваке формиране матрице и те вредности се користе као улазни параметри за $\chi^2$ тест.

Прорачунава се $P$ вредност и уколико је она мања од нивоа поверења $\alpha$ закључује се да секвенца није случајна [66-68].

## 6. Discrete Fourier Transform (Spectral) Test

Фокус овог теста је на проналажењу екстремних вредности у спектру добијеном применом дискретне Фуријеове трансформације на испитивану секвенцу.

Тест се извршава тако што се битови који имају вредност 0 претварају у вредност -1, док се јединице претварају у вредност +1 и на тај начин се добија нова секвенца бројева. На ову нову секвенцу се примени дискретна Фуријеова трансформација.

Добија се секвенца комплексних променљивих које репрезентују периодичне компоненте секвенце бита на различитим фреквенцијама.

Ако претпоставимо да $x_k$ представља *k*-ти бит секвенце, где је $k = 1, ..., n$. Након кодовања свих бита са +1 и -1 следи:

$$f_j = \sum_{k-1}^{n} x_k \exp(2\pi_i (k-1)\, j / n)$$

где је:

$$\exp(2\pi ikj / \mathrm{n}) = \cos(2\pi kj / n) + i \sin(2\pi kj / n),$$
$$j = 0, ..., n-1,$$
$$i = \sqrt{-1}$$

Због симетрије приликом трансформације из реалних вредности у комплексне разматрају се само вредности од *0* до *(n/2-1)*. Нека је $mod_j$ модуо комплексног броја $f_j$.

Под претпоставком да је тестирана секвенца заиста случајна тест да 95% вредности $mod_j$ мора бити мање од вредности параметра *h*, који је једнак: $h = \sqrt{(\log \frac{1}{0.05})\,\mathrm{n}}$ .

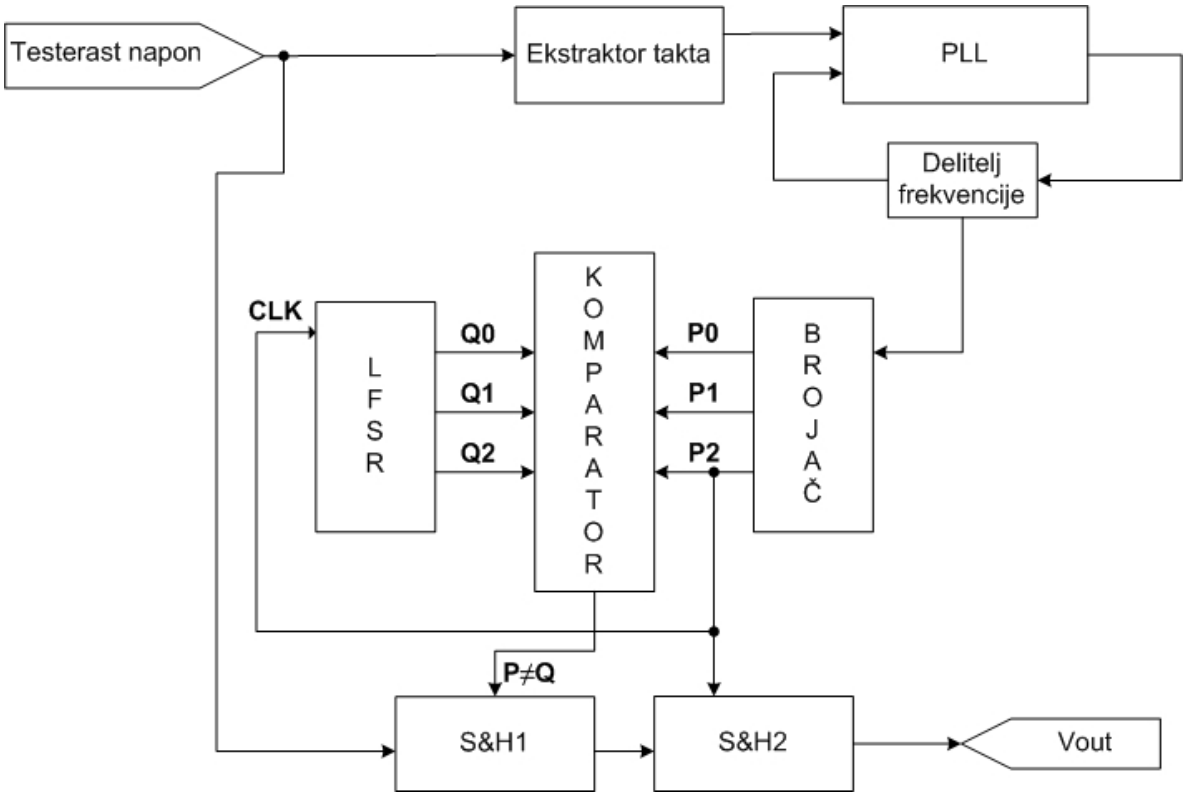
P вредност се прорачунава на основу биномне расподеле и уколико је она мања од нивоа поверења $\alpha$ закључује се да секвенца није случајна.

Препорука је да се за овај тест користи секвенца дужине најмање 1000 бита [69-70].

# 2. Хардверско решење генератора дискретног аналогног униформног шума

У [71] је описан реализовани хардверски генератор дискретног аналогног униформног шума.

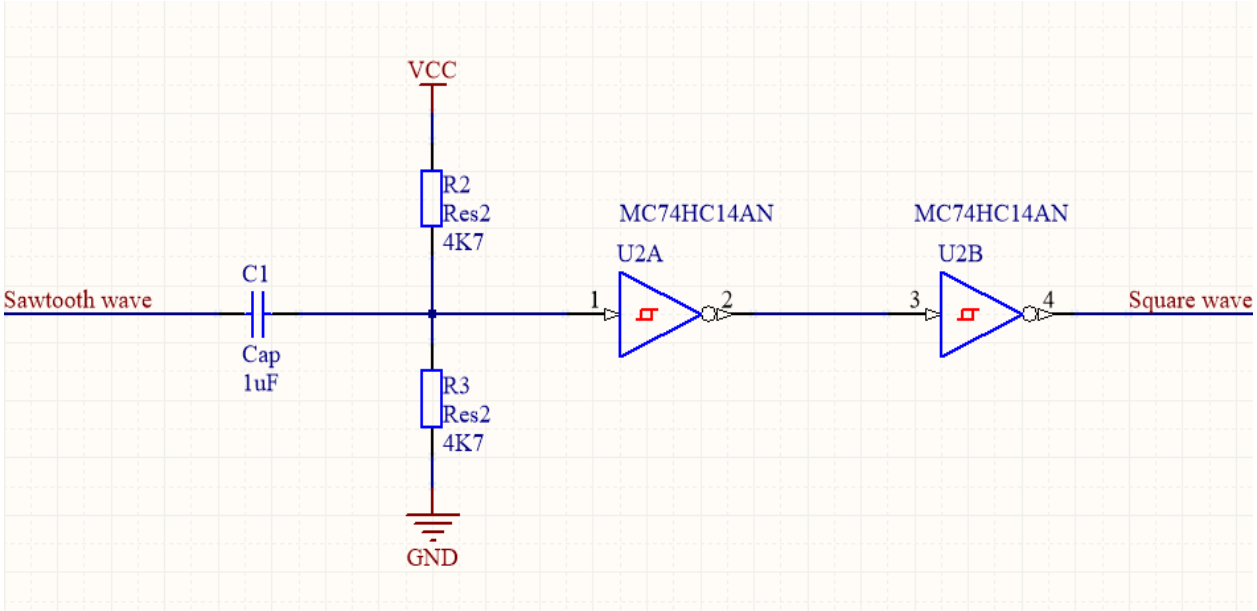
Блок шема уређаја дата је на слици 1.




**Слика 1 Блок шема генератора**

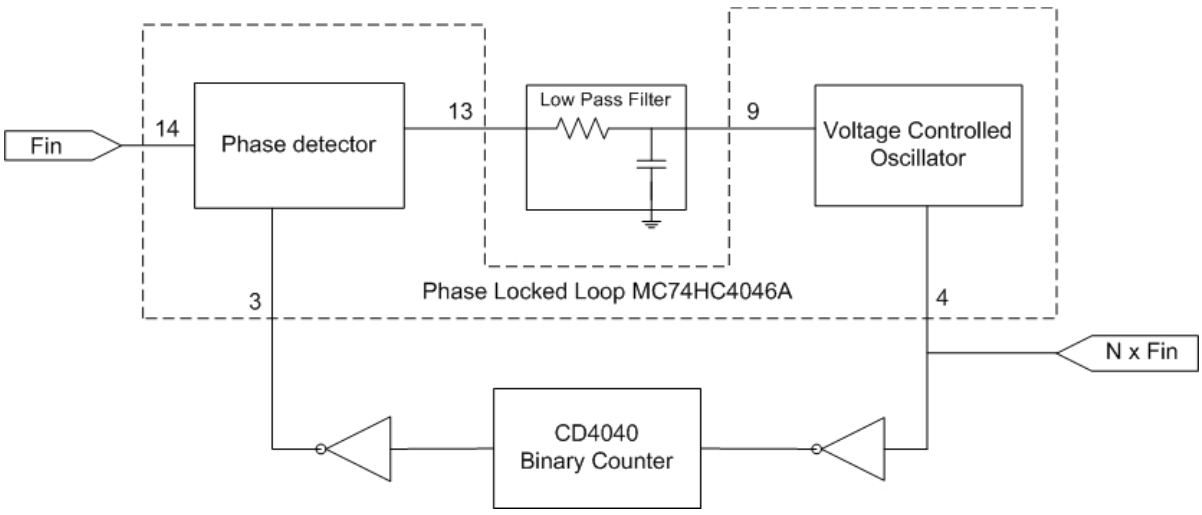
Екстрактор такта представља склоп који од улазног, наизменичног, тестерастог напонског сигнала генерише дигитални напонски сигнал у виду четвртки. Амплитуда улазног тестерастог напонског сигнала износи ±2,5 V, док амплитуда дигиталног напонског сигнала износи 5 V. Зато се тестерастом сигналу мора суперпонирати напонски офсет од 2,5 V што се постиже напонским разделником од 5 V. Тестерасти напон се преко кондензатора доводи на чип MC74HC14 - инвертујући Шмитов тригер,

а затим се још једном добијени сигнал провлачи кроз инвертујући Шмитов тригер. Разлог пролаза кроз два Шмитова тригера је добијање што је могуће оштрије ивице дигиталног сигнала који се користи као такт сигнал дигиталног дела кола. Шема екстрактора такта дата је на слици 2.




**Слика 2. Шема екстрактора такта**

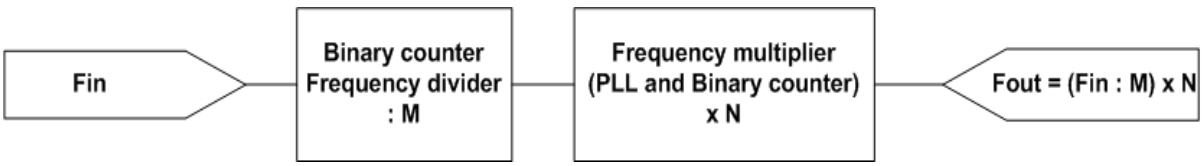
PLL представља дигитални склоп који се у овом случају користи као множач фреквенције. Блок шема на којој је приказано функционисање множача фреквенције дата је на слици 3.




**Слика 3. Множач фреквенције**

Коришћен је PLL чип MC74HC4046A који у себи садржи фазне детекторе, чију кључну компоненту представља фазни компаратор. Могуће је извршити одабир између три фазна компаратора. Улога фазног компаратора је да на основу два напона која се пореде генерише импулсе у складу са разликом у фазама улазних сигнала. Ови импулси се филтрирају уз помоћ пасивног НФ филтра, да би се добила што стабилнија вредност сигнала који се даље води на напоном контролисани осцилатор (VCO). Да би се добила што стабилнија вредност потребно је употребити што квалитетнији НФ филтар. У овој шеми је намерно коришћен лош НФ филтар што доприноси случајности целокупног система. VCO генерише импулсе у зависности од вредности напона на осцилатору. Да би се извршило множење сигнала потребно је у повратну спрегу чипа поставити бинарни бројач (чип CD4040), чији је задатак да подели фреквенцију одговарајућом целобројном вредношћу. Важно је напоменути да се због убрзавања транзиције са једног на други логички ниво додају Шмитови тригери, пре и после бинарног бројача. Сигнал фреквенције која је подељена бинарним бројачем, доводи се на други улаз детектора фазе, те на тај начин PLL петља покушава да изједначи фреквенције сигнала на оба улаза, а то је могуће остварити само ако је фреквенција на излазу VCO онолико пута већа колико износи фактор дељења бинарног бројача.

На излазу PLL-а су реализоване фреквенције помножене 8 пута, 8,5 пута као и 8,25 пута. Пошто је PLL-ом и бинарним бројачем могуће множити само целобројном вредношћу, идеја је да се сигнал прво помножи 8, 17 и 33 пута овом петљом, а затим додатним бинарним бројачем подели 1, 2 и 4 пута, респективно. Проблем који се уочава при оваквој конфигурацији јесте фреквенција која ће, ако је на улаз доведен сигнал фреквенције 100 kHz, на излазу множача фреквенције бити у распону од 800 kHz до 3,3 MHz што може представљати велики проблем због генерисања шума на високим учестаностима, као и велики распон фреквенција које мора генерисати VCO. Из тих разлога је поменути делилац фреквенције након множача фреквенције, постављен испред множача као што је приказано на слици 4.




**Слика 4. Блок шема множача фреквенције са вредностима 8, 8,5 и 8,25 пута**

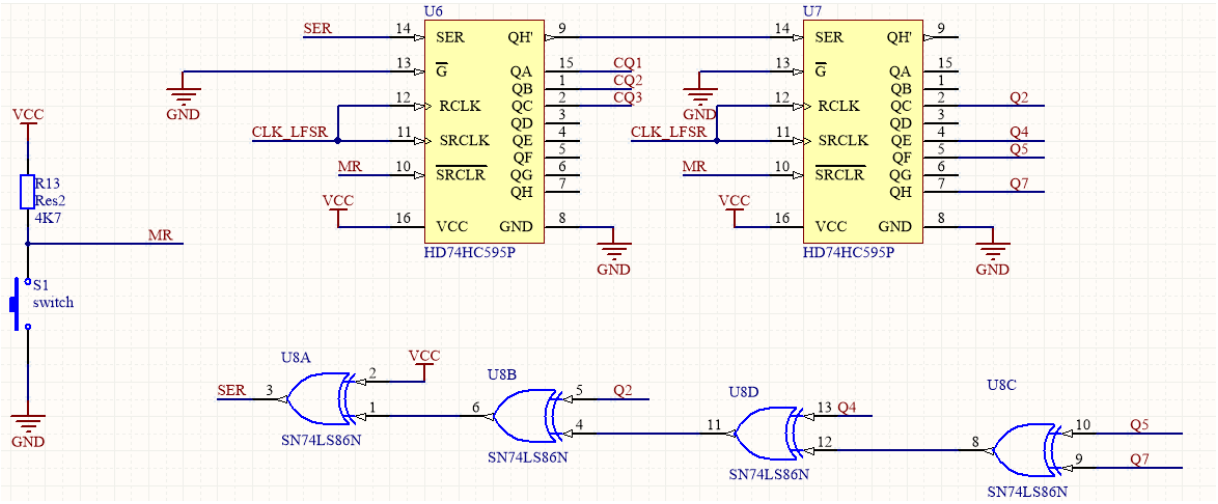
Вредности за коефицијенте M и N су дате у табели 1, за улазну фреквенцију од 100 kHz.

**Табела 1. Вредности за коефицијенте множача**

| Коефицијент множења | M | N | Fout [kHz] |
|---|---|---|---|
| 8 | 1 | 8 | 800 |
| 8,5 | 2 | 17 | 850 |
| 8,25 | 4 | 33 | 825 |

LFSR структура се састоји из померачког регистра и повратне спреге остварене уз помоћ XOR логичких кола. Улаз у померачки регистар представља комбинацију полиномне функције повратне спреге и претходног стања регистра. Коришћена полиномна функција у овом случају је X16 + X14+X13+X11+1, јер она даје најдужу могућу секвенцу различитих битова. Пошто су два померачка осмобитна регистра везана редно, онда је резултујући шифт регистар шеснаестобитни. Рад регистра је одређен и у потпуности предвидив јер ради са претходним стањима у регистру, а поред тога још једно ограничење представља и коначна величина регистра, па је могуће уписати максимално 65535 различитих секвенци битова за већ наведену функцију након чега се циклус понавља. Прва три бита регистра се воде на компаратор. Брзина убацивања бита у шифт регистар је одређена брзином такта коју генерише бројач. Неповољна ситуација која се може десити је да се цео шеснаестобитни регистар попуни јединицама што представља нежељено стање, јер ће регистар у себе континуално уписивати јединицу, те се на тај начин добија ефекат бесконачне петље. Да би се ово избегло додат је тастер за ресетовање, који корисник треба да притисне ако дође до описане ситуације

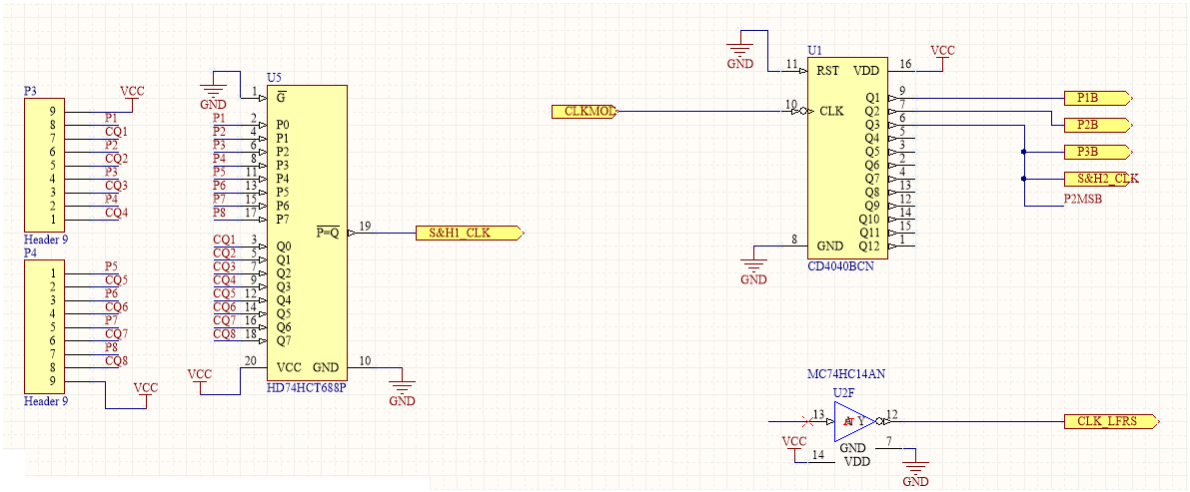
Као осмобитни шифт регистри користе се два кола 74HC595, а као XOR логичко коло се користи SN74LS86. На слици 5 дата је шема описаног система.




**Слика 5. LFSR структура**

Улога бројача је да генерише битове који ће се поредити на компаратору са битовима LFSR-а, затим да генерише такт за LFSR као и да генерише такт одабирања за S&H2 кола. Бит који дели улазну фреквенцију са два, четири и осам се доводи на улазе компаратора, док се фреквенција подељена са осам поставља за такт LFSR, али се претходно провуче кроз инвертовани Шмитов тригер из два разлога. Први разлог представља дефинисање што је могуће стрмије ивице сигнала, док други разлог представља синхронизацију такта са бројачем, јер се окидање врши на различите ивице транзиције сигнала. Улога компаратора је да проверава вредности на улазима од стране LFSR-а и бројача, и ако су они исти извршиће се одабирање уз помоћ S&H1 кола. Проблем који се јавља у овом случају је што коришћени компаратор (74HCT688) испитује $\overline{P = Q}$ што је управо супротно од онога што се жели испитати. Проблем се превазилази постављањем инвертора уз помоћ транзистора који има улогу и да помери напонски ниво на ±5 V, са ког се даље сигнал води на такт одабирања S&H1. Суштина рада целог блока се заснива на томе да када се у LFSR упише одређена вредност (осмина такта бројача), бројач пролази кроз све могуће комбинације три бита (бинарно од 0 до 7) које се пореде на компаратору са већ задатом вредношћу на LFSR-у и када се оне изједначе врши се одабирање. На овај начин је обезбеђено да ће се у једној осмини такта бројача извршити само једно одабирање S&H1 кола, као и S&H2 кола. Након што S&H1 коло одабере сигнал у неком случајном тренутку генерисаном описаном процедуром, S&H2 коло врши прослеђивање тог напона на излаз, тако што прослеђује напон на излаз на свако ново задавање у LFSR-у тј. на осмину такта бинарног бројача.

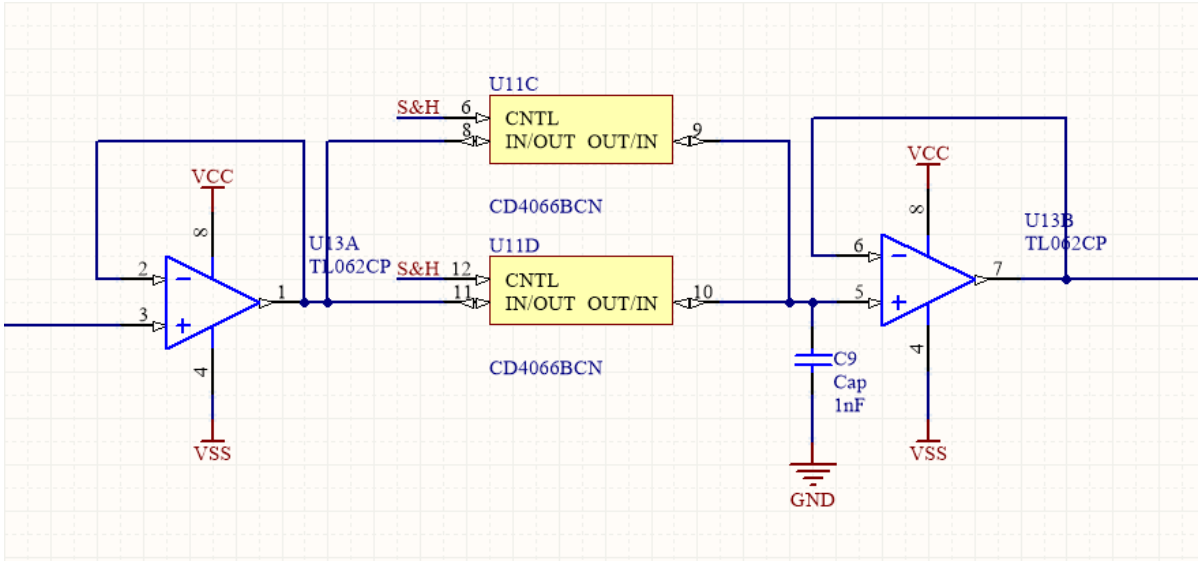
Шема повезивања бројача и компаратора дата је на слици 6.




**Слика 6. Шема повезивања бројача CD4040 и компаратора 74HCT688**

**S&H кола**

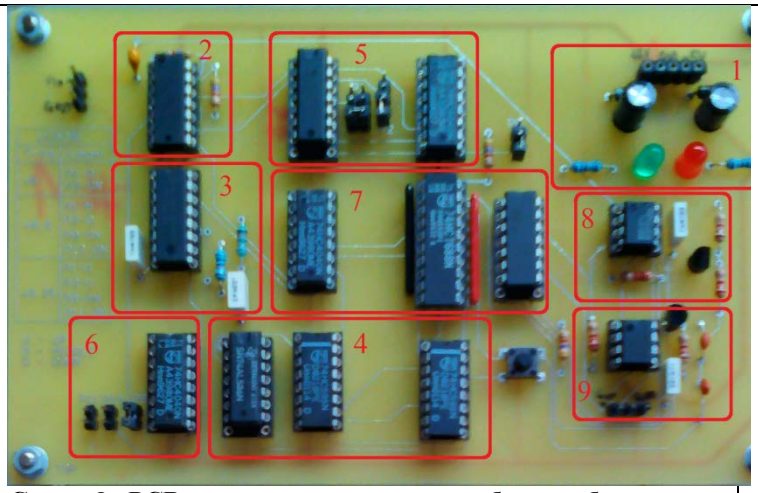
S&H1 и S&H2 кола представљају два потпуно идентична кола и приказана су на слици 7.




**Слика 7. S&H коло**

S&H коло се састоји из два операциона појачавача и два аналогна прекидача.

Описани хардвер је направљен како би се извршила провера концепта. На слици 8 је приказан прототип хардвера.



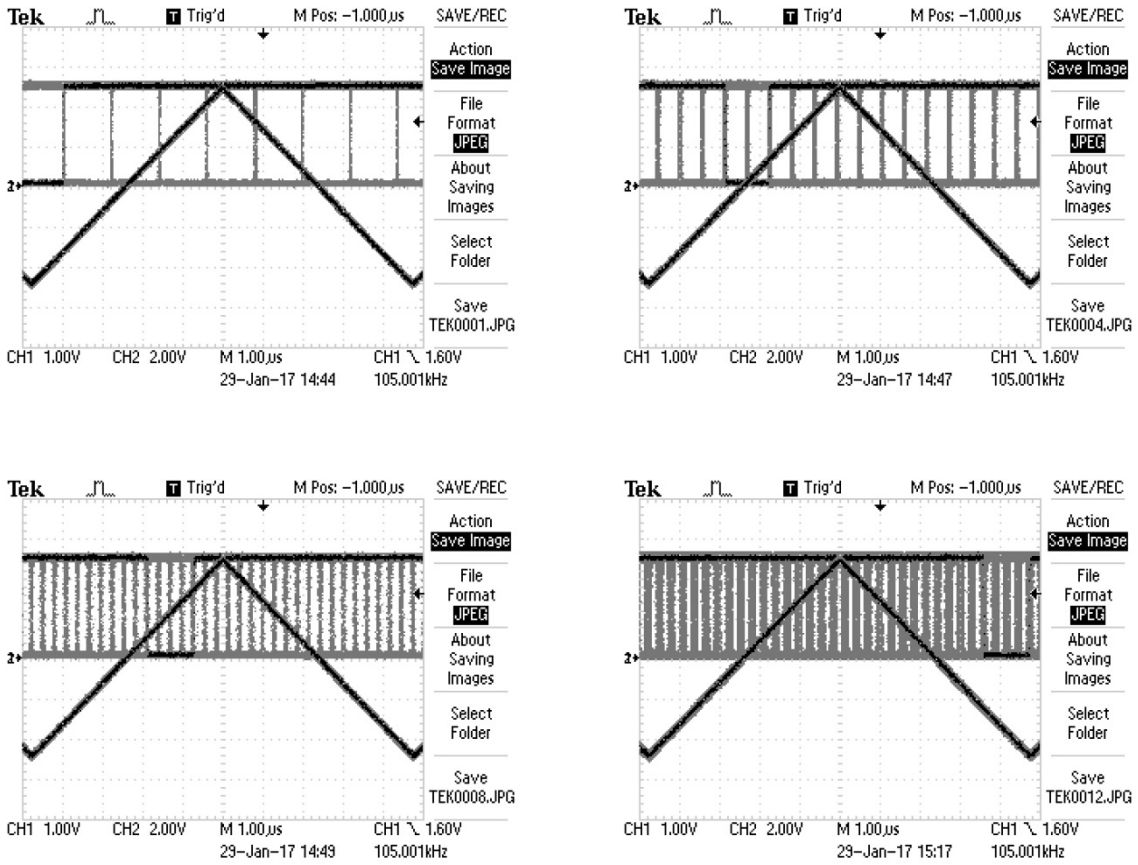

1. Power Supply
2. Clock extractor
3. PLL
4. LFSR
5. Divider K
6. Divider L
7. Digital comparator
8. S&H1
9. S&H2

**Слика 8. PCB прототипа са означеним битним блоковима**

Карактеристични напонски облици су снимљени дигиталним осцилоскопом. Циљ је био да се једноставном и брзом провером установи провера концепта, без озбиљнијег проверавања постигнутих перформанси.

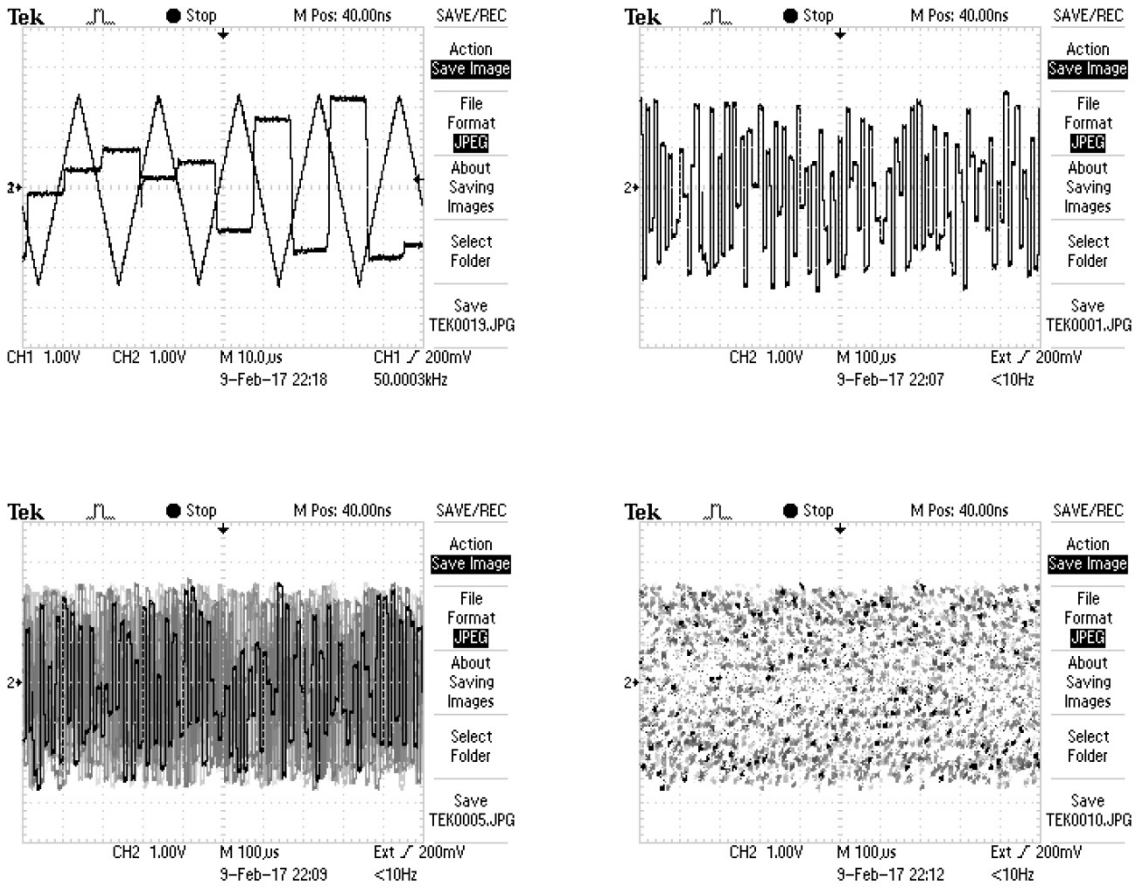
На плочу је довођен напон троугаоног облика амплитуде 2.5 V, из генератора. Омогућено је генерисање учестаности семпловања која је 8, 8.5, 8.25 пута већа од учестаности тестерастог сигнала.

На слици 9 су приказана четири графика, на којима је дат приказ улазног троугаоног сигнала и поворке импулса на излазу из PLL-а. Четврти график представља случај са ослабљеним НФ филтером, па се види присуство jitter-а. При даљем повећавању присуства jitter-а, добија се у потпуности замрљана слика, која није од интереса за приказивање.




**Слика 9. Четири графика троугаоног сигнала и поворке импулса на излазу PLL-а**

На слици 10 су дати прикази троугаоног напона и напона шума, а затим само шум при различитим временским базама и са укљученом перзистенцијом екрана. Равномерна истачканост екрана илуструје очекивање да генерисани шум има униформну функцију густине расподеле вероватноће (PDF) .




**Слика 10.** Прикази троугаоног напона и напона шума (горња два графика) и само сигнала шума са различитим временским базама (доња два графика)