

УНИВЕРЗИТЕТ СИНГИДУНУМ

ФАКУЛТЕТ ЗА ИНФОРМАТИКУ И РАЧУНАРСТВО

Конструисање псеудослучајног генератора *PRNG* на основу случајних почетних стања, добијених преко физичког извора информација *TRNG*

- Дипломски рад -

Ментор:

Доц. др Александар Јевремовић

Студент:

Никола Савановић

Индекс: 2010/201445



ФАКУЛТЕТ ЗА ИНФОРМАТИКУ И РАЧУНАРСТВО

УНИВЕРЗИТЕТ СИНГИДУНУМ

ФАКУЛТЕТ ЗА ИНФОРМАТИКУ И РАЧУНАРСТВО

Београд, Данијелова 32

Кандидат: Никола Савановић

Број индекса: 2010/201445

Смер: Информатика и рачунарство

Тема: Конструисање песудослучајног генератора *PRNG* на основу случајних почетних стања, добијених преко физичког извора информација *TRNG*.

Задатак: Задатак овог дипломског рада је конструсање хардверског уређаја, за генерисање случајних бројева. Затим, врше се статистички тестови како би се испитало да ли је могуће такав псеудослучајни генератор (PRNG) користити у криптолошке сврхе.

Датум одобрења рада:
Београд, ___.___._____.

Ментор

_____

ДЕКАН

_____

Конструисање псеудослучајног генератора *PRNG* на основу случајних почетних стања, добијених преко физичког извора информација *TRNG*

Сажетак: У овом раду бавимо се конструисањем и испитивањем псеудослучајног генератора бројева *PRNG*. На основу добијених случајних почетних стања – генеришемо истинито случајне бројеве *TRNG*, које добијамо преко физичког извора информација – на основу шума, односно, буке коју праве транзистори. У раду се бавимо приказивањем статистичких тестова и анализом за шта је све могуће користити конструисани псеудослучајни генератор (PRNG).

Кључне речи: *PRNG*, *TRNG*, псеудослучајни генератор бројева, истинито случајни бројеви, криптографија

Constructing pseudorandom generator PRNG based on random initial conditions, obtained through physical source of information TRNG

Abstract: In this paper we are constructing and testing pseudorandom generator PRNG. On the basis of the random initial conditions – we generate true random numbers TRNG, obtained over the physical source of information - on the basis junction noise source.

Keywords: PRNG, TRNG pseudorandom generator, true random number, cryptography

„Информација: обрнуто пропорционална негативна вредност вероватноће“

Клод Елвуд Шенон

САДРЖАЈ

Списак слика ..... - 3 -
Списак табела ..... - 4 -
1 Увод ..... - 5 -
1.1 Предмет истраживања ..... - 5 -
1.2 Доприноси рада ..... - 5 -
1.3 Структура рада ..... - 6 -
2 Преглед у области истраживања ..... - 7 -
2.1 Предности и недостаци псеудослучајног генератора бројева ..... - 9 -
3 Теоријске основе истраживања ..... - 10 -
3.1 Комуникациони систем ..... - 10 -
3.2 Ентропија ..... - 13 -
3.3 1 Дискретни извори с меморијом ..... - 14 -
3.3 2 Дискретни извори без меморије ..... - 15 -
3.4 Савршена тајност ..... - 16 -
3.5 Псеудослучајни генератори ..... - 16 -
3.6 ANSI X9.17 ..... - 17 -
3.7 Комуникације ..... - 18 -
3.8 Електроника ..... - 19 -
3.8.1 Напон ..... - 19 -
3.8.2 Електрично оптерећење ..... - 19 -
3.8.3 Енергија ..... - 20 -
3.8.4 Електрично поље ..... - 20 -
3.8.5 Идеални електрични елементи ..... - 20 -
3.8.6 Проводници, изолатори и полупроводници ..... - 20 -
3.8.7 Електрична струја ..... - 21 -
3.9 Електрично коло ..... - 22 -
3.9.1 Први (струјни) Кирхофов закон ..... - 22 -
3.9.2 Други (напонски) Кирхофов закон ..... - 23 -
3.9.3 Паралелна и серијска веза отпорника ..... - 23 -

3.9.6 Наизменична струја ..... - 24 -
3.9.7 Елементи електричног кола ..... - 25 -
3.9.7 1 Диода ..... - 25 -
3.9.7 2 Кондензатори ..... - 26 -
3.9.7 3 Светлећа (LED) диода ..... - 27 -
3.9.7 4 Транзистори, типа НПН ..... - 27 -
3.9.7 5 Отпорници ..... - 28 -
4 Преглед предложеног решења ..... - 30 -
4.1 Генеричка шема предложеног решења ..... - 30 -
4.2 Поставка и објашњење експерименталног окружења ..... - 31 -
4.3 Спроведене анализе и експерименти ..... - 39 -
4.4 Приказ експерименталних резултата ..... - 44 -
4.5 Област примене предложеног решења ..... - 51 -
5 Закључак ..... - 53 -
5.1 Сумарни циљеви рада ..... - 53 -
5.2 Предлог за будући рад ..... - 53 -
Литература ..... - 55 -

Списак слика

3.1.1 Блок шема комуникационог модела ..... - 11 -
3.1.2 Шенонов математички модел ..... - 12 -
3.2 Ентропија случајне варијабле са два исхода ..... - 14 -
3.9.1 Паралелна веза отпорника ..... - 24 -
3.9.2 Симбол наизменичне струје ..... - 25 -
3.9.3 Диода и њен симбол ..... - 26 -
3.9.4 Поларизовани кондензатор ..... - 26 -
3.9.5 Светлећа диода ..... - 27 -
3.9.6 Симбол светлеће диода ..... - 27 -
3.9.7 НПН транзистор ..... - 27 -
3.9.8 Симбол НПН транзистора ..... - 27 -
3.9.9 Отпорници ..... - 28 -
3.9.10 Симбол отпорника ..... - 28 -
4.1 Генеричка шема предложеног решења ..... - 30 -
4.2 Генератор у пракси ..... - 30 -
4.3 Генеричка шема предложеног решења ..... - 32 -
4.4 Конструисани „PRNG“ генератор ..... - 32 -
4.5.1 Једна грана електричног кола ..... - 34 -
4.5.2 Друга грана електричног кола ..... - 34 -
4.6 Прва целина електричног кола ..... - 35 -
4.7 Трансформатор и „PRNG“ ..... - 35 -
4.8 „PRNG“ ..... - 36 -
4.9 „Stereo“ кабл ..... - 37 -
4.10 Компоненте генератора (1) ..... - 37 -
4.10.1 Компоненте генератора (2) ..... - 37 -
4.11.1 Укључен „PRNG” (1) ..... - 38 -
4.11.2 Укључен „PRNG” (2) ..... - 38 -
4.11.3 Укључен „PRNG” (3) ..... - 38 -
4.12.1 Снимљен шум из генератора (1) ..... - 40 -
4.12.2 Снимљен шум из генератора (2) ..... - 40 -

4.12.3 Снимљен шум из генератора (3) ..... - 40 -
4.13 Низ бројева ..... - 42 -
4.14 Бинарни низ ..... - 42 -
4.15 Уклоњена редуданса ..... - 43 -
4.16 Ентропија бинарног низа ..... - 43 -
4.17 Генерисан шум ..... - 44 -
4.18 Генерисан шум ..... - 48 -
4.19 Шум у функцији топлоте ..... - 49 -
4.20 Насумични бројеви ..... - 49 -
4.21 Насумични генерисани битови ..... - 50 -
4.22 Хистограм генерисаних битова ..... - 50 -
4.23 Хистограм (polimatrix) генерисаних битова ..... - 51 -

Списак табела

4.1 Ентропија са преклапањем (random.org) ..... - 45 -
4.2 Ентропија са преклапањем (PRNG) ..... - 45 -
4.3 Ентропија без преклапања (random.org) ..... - 46 -
4.4 Ентропија без преклапања (PRNG) ..... - 46 -
4.5 Серијски тест (random.org) ..... - 47 -
4.6 Серијски тест (PRNG) ..... - 47 -
4.7 Мауреров тест (PRNG) ..... - 48 -

1 Увод

1.1 Предмет истраживања

У данашње време, када рачунарска комуникација није безбедна, када комуникација између крајњих корисника може да буде угрожена у сваком тренутку, наш циљ је да обезбедимо што јачу и сигурнију комуникацију између две стране. Јавља се потреба за коришћењем јаких софтверских алгоритама или хардверских уређаја за генерисање насумичних бројева, који могу да нам обезбеде сигурнију комуникацију. Поставља се питање да ли је хардверски генератор решење, да ли је нешто што генеришемо из било ког генератора стварно насумично и да ли ће генератор моћи да емитује стално случајни шум.

У овом раду бавимо се конструисањем генератора лажно случајних бројева, у даљем тексту - псеудослучајног генератора *PRNG,* на основу кога се генеришу случајни бројеви. Псеудослучајни генератор *PRNG* представља физички извор информација. У генерисању истинито случајних бројева *TRNG*, веома је важно да постоји извор који стално емитује случајан низ, односно, случајне информације. Како бисмо добили брз и ефикасан истинито случајан низ *TRNG*, конструисан је генератор, који емитује шум из биполаризованог транзистора, типа НПН „BC547A“. Затим, врше се статистички тестови, како бисмо утврдили да ли је могуће користити такав псеудослучајни генератор у криптографске сврхе и да ли су добијени случајни бројеви стварно истинити случајни бројеви.

Добијени аналогни шум се снима путем рачунара, преко програмског пакета *Sound Forge*. На тај начин се генерисани аналогни шум претвара у дигитални сигнал. Након што је генерисан и снимљен шум, на рачунару се, путем програмског алата *MATLAB*, врше даље анализе и статистички тестови. Такође, испитује се ентропија извора информација.

У наставку текста биће приказане већине метода које су примењене у самој анализи генерисаног шума. Алати који су коришћени у овом раду су *MATLAB*, програмски пакет *Sound Forge* и програмски језик *Java*, за статистичке тестове. За поређење и тестирање шумова, коришћен је шум, који је доступан преко интернет странице *random.org*.

1.2 Доприноси рада

Након одређених тестова генератора, као допринос рада могуће је навести следеће:

- доказан насумичан псеудослучајан низ,
- овакав псеудослучајан генератор је могуће користити за генерисање *One-Time-Pad* кључева.

1.3 Структура рада

У наставку текста, описана је у кратким цртама комплетна структура рада.

У другом поглављу, дат је преглед области истраживања. Анализирано је неколико научно-истраживачких радова, који су упоређени са конструисаним псеудослучајним генератором (PRNG). Представљен је развој решења и концепт процене, у какве сврхе је могуће користити овакав генератор случајних бројева (PRNG).

У трећем поглављу, дат је теоријски приступ ентропији и Шеноновим теоремама. С обзиром да је предмет истраживања овог рада конструисање електричног кола и физичка израда псеудослучајног генератора, описане су све компоненте електричног кола и представљене теоријске основе из области електронике.

У четвртом поглављу детаљно је описан рад псеудослучајног генератора *PRNG*, начин на који се емитује шум, како се добијени шум преводи у бинарни низ и како се из генерисаног шума добијају истинито случајни бројеви. Добијени резултати су упоређени са другим добијеним званичним резултатима.

У петом поглављу извршена је анализа добијених резултата, на основу које је дат закључак о добијеним резултатима постигнутим у овом раду.

2 Преглед у области истраживања

Током истраживања ове материје, издвојено је и описано неколико научно-истраживачких радова који се могу довести у везу са овим радом. Из наведених радова одабрани су цитати који детаљније објашњавају појмове и појаве који се описују у овом раду.

У већ поменутом сажетку, споменут је проблем софтверских генератора. Софтверски псеудослучајни генератори имају проблем детерминистичког својства, што за криптолошке сврхе није добра карактеристика. Следећи цитат [3] из научно-истраживачког рада даје веома јасну дефиницију о начину функционисања хардверског псеудослучајног генератора и говори о манама софтверског генератора:

> *„Звучне картице рачунара се у пракси најчешће користе за генераторе псеудослучајних бројева (PRNG). За добијање излазног низа бројева неопходна је примена почетне вредности, а добијени излазни низ је периодични. У захтевним ситуацијама, као што је на пример генерисање криптографских кључева, коришћење оваквих софтверских генератора може постати непоуздано, пре свега због њихових детерминистичких својстава.“[3]*

Такође, битно је да се дефинишу два типа псеудослучајних генератора и какве су њихове особине. Случајни бројеви су подељени у две основне класе, које се зову детерминистиче и недетерминистичке. Детерминистички генератори насумичних бројева производе низ битова из иницијалне вредности – сид, са специфичним алгоритмом.

Недетерминистички генератори производе и генеришу излази који су непредвидиви, а зависе од неког физичког извора, који је ван људске контроле.

Случајни бројеви су од фундаменталне важности у области криптографије, који могу да се користимо нпр. за шифровање у мрежном саобраћају, за генерисање кључева итд. Временом су се софтверски програми за генерисање случајних бројева показали као лошији, с обзиром да када се један алгоритам имплементира, он мора да има свој почетак и крај; прецизније, једног тренутка ће алгоритам почети да се понавља. Због тога се све више пажње придаје конструисању хардверских решења, која имају сталан и константан извор информација.

Праву случајност је немогуће добити на детерминистичком рачунару, па се из тог разлога користе генератори псеудослучајних бројева, такви, да добијени низ бројева пролази већину статистичких тестова случајности.

Псеудослучајни низови се могу генерисати и помоћу једносмерних функција уколико на располагању имамо неку од једносмерних хеш функција, као што су „MD5“ или „SHA1“.[6]

Као што се научници слажу да у природи живота све има свој почетак и крај, да се циклуси понављају како у организму, тако и у природи, остаје отворено питање да ли постоји такав псеудослучајни генератор бројева *PRNG*, који ће увек моћи да емитује случајне бројеве, а да се, притом, случајни бројеви никада не понове. Један део научника, професора, студената и свих других који се баве истраживањем на овом пољу, воде се тезом да такви генератори не постоје, већ да све има свој почетак и крај и да ће сваки генератор једном морати да се ресетује и врати на почетно стање.

У криптографији, овакви псеудослучајни генератори бројева (PRNG) се углавном користе управо за, већ поменуто, генерисање кључева, за одређене и јединствене параметре у дигиталном потпису, за шифровање порука у мрежи, иницијализационе векторе, итд. Случајни, односно, насумични бројеви су углавном засновани на физичком недетерминистичком феномену. Један од популарнијих приступа заснива се на генерисању термичких шумова (шум из диоде, транзистора и сл.)

Постоје два основна приступа за генерисање случајних бројева коришћењем рачунара: псеудо случајни генератори бројева (PRNG) и истинито случајни генератори бројева (TRNG). Сваки од наведених приступа има своје предности и мане.

Карактеристике „TRNG“ су поприлично другачије од „PRNG“, „TRNG“ су неефикасни у односу на „PRNG“. Потребно им је знатно више времена да произведу одређен број случајности.[6]

Оно што је најбитније код псеудослучајних генератора *PRNG* је да сви генерисани бројеви, који су добијени из термичког шума, морају да буду непредвидиви. Низови тих бројева не смеју никако да буду познати унапред, нити сме да постоји један познати скуп бројева, из кога ће се бирати низ бројева.

Управо на основу поменутог, можемо довести у везу научно-истраживачки рад, где је дата дефиниција непредвидивости низа бројева, где пише да:

Случајни и псеудослучајни бројеви генерисани за криптографске системе морају бити непредвидиви. У случају псеудогенератора, ако је сид или иницијално стање генератора непознато, следећи бинарни низови ће бити непредвидиви и поред било ког знања о претходним бинарним низовима.

Такође, не би требало да буде могуће да се утврде сидови на основу претходно генерисаних низова. Између сидова и бинарних низова нема корелације, сваки бит низа требало би да буде потпуно независан, чија је вероватноћа ½.

Издвојени цитат [6] можемо да доведемо директно у везу са конструисаним псеудослучајним генератором *PRNG*, јер је управо на тој идеји и заснован и псеудослучајни генератор, који је предмет истраживања. Добијени низови бројева из псеудослучајног генератора (PRNG) су потпуно независни и сви битови су потпуно независни.

2.1 Предности и недостаци псеудослучајног генератора бројева

Недостаци псеудослучајног генератора бројева су лоше дизајнирани генератори, где је могуће открити улазни низ бројева.

Неки од напада на псеудослучајне генераторе бројева су:

- директни криптоаналитички напади – нападач је у стању да примети разлику између *PRNG* излаза и случајности у низу,
- напади засновани на улазним вредностима генератора – овакви напади догађају се када је криптоаналитичар у стању да користи знање или контролу над улазним параметрима генератора псеудослучајних бројева.

3 Теоријске основе истраживања

Овај дипломски рад је уско везан за ентропију, самим тим, псеудослучајни генератор се управо ослања на Шенонову теорему. У овом поглављу представљене су теоријске основе истраживања; дате су Шенонове теореме, дата је блок-шема класичног Шеноновог комуникационог система, затим, представљен је укратко и Шенонов модел савршене тајности везан за блок-шему комуникационог модела.

Веома је важно испитивање и анализирање добијених резултата псеудослучајног генератора. Као основа за испитивања самог генератора, примењена је ентропија извора информација. На основу анализираних узорака, односно, понављањем експеримената више пута и на основу ентропије која је као крајњи резултат, могуће је донети неколико закључака:

- генератор је могуће користити за генерисање кључева за *One-Time-Pad* шифарски систем,
- генератор је могуће користити за шифровану комуникацију у рачунарској мрежи,
- генератор је могуће користити за јединствене параметре у дигиталном потпису и друго.

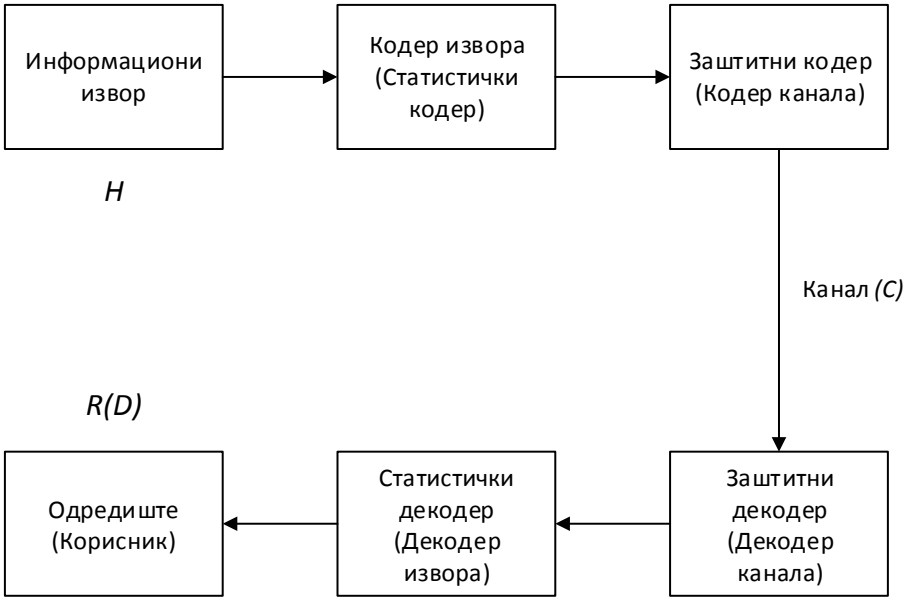
Данашњи и главни проблем у Статистичкој теорији је да се пренесени сигнали мењају услед сметњи, тачније, услед појаве шума. Такође, сигнали и сметње су моделовани као случајни процеси.

Основа генератора псеудослучајних вредности се може гледати из угла Прве Шенонове теореме где је Шенон је показао везу ентропије и минималног броја сигнала по поруци, потребног за представљање информација које емитује извор.

У наставку текста описан је класичан модел комуникациониог система кроз блок шему и пренос информација од извора до одредишта. Затим, описана је ентропија, дат је математички приступ Првој и Другој Шеноновој теореми, у циљу довођења у везу Шенонове теорије са конструисаним псеудослучајним генератором.

3.1 Комуникациони систем

Рад псеудослучајног генератора може да се прикаже на основу блок дијаграма класичног комуникационог система. Блок шема се посматра само из једног смера, од информационог извора ка крајњем одредишту – кориснику. Овај процес је могуће описати и од одредишта (корисника) до информационог извора.



Слика 3.1.1: Блок шема комуникационог модела[9]

У шеми је приказан извор информација (*H*), кодер извора (у литератури може да се нађе и термин - статистички кодер), заштитни кодер (често се зове и кодер канала). Затим, заштитни декодер или декодер канала и статистчки декодер (декодер извора).

Информациони извор по дефиницији Теорије информација узима поруке које се налазе у већ дефинисаном скупу и почиње да их емитује. Емитоване поруке долазе до статистичког кодера, који има задатак да кодује емитоване поруке од стране информационог извора. Следећи део је заштитни кодер који има задатак да убаци редудансу – сигнал који не садржи информацију; служи као превентива изобиличавању сигнала који се преноси кроз комуникациони канал.

Редуданса омогућава откривање грешака које су се појавиле током преноса, а управо захваљујући убаченој редудансу је могуће исправити изобличени сигнал. Могући фактори сметњи сигналу могу да буду разни шумови, сам квалитет комуникационог канала и слично.

Следећа два блока су заштитни кодер и статистички декодер који врше комплементарне операције на пријему, да би се на одредишту (кориснику) предале информације које му је упутио извор.

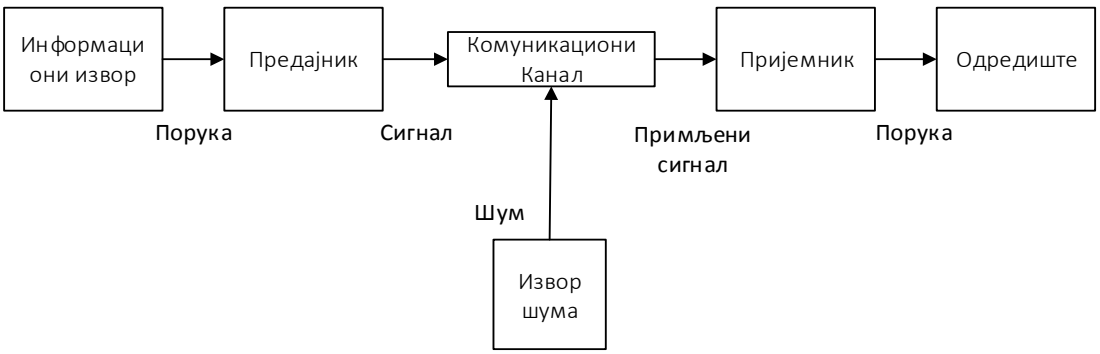
Пренос информација подразумева или њихово преношење из једне тачке у другу или њихово преношење кроз време. Пример преношења од једне тачке до друге је комуницирање између два мобилна телефона у једној мрежи.

Код комуникационих канала, јавља се проблем, појаве шума који омета пренос информација. У таквим условима, где је висок шум, тешко је да се обави поуздан пренос информација. У неким случајевима, могуће је пренети поруку са малом грешком, која ће се након пријема исправити кодовањем. Та ситуација је позната као пренос поруке са вероватноћом грешке.

На слици 3.1.1, нису приказани блокови за шифровање и дешифровање. Блок за шифровање може да се нађе на било ком месту у предајном делу, али пре кодера извора, пре кодера канала или пре самог канала. Блок за дешифровање може да се нађе на комплементарној позицији, у пријемном делу.

Основна идеја заштитног кодовања је додавање редундансе у кодоване поруке, тако да и поред грешака у преносу преостаје довољно непромењених информација у кодованим порукама на основу којих се може реконструисати послата порука са задатим нивоом грешке реконструкције.

Модел комуникационог канала може да се престави Шеноновим математичким моделом из 1949. године:



Слика 3.1.2: Шенонов математичи модел из 1949. године

На слици 3.1.2 може да се види да порука, која се шаље са информационог извора, пролази кроз предајник, на ком се врши кодовање поруке у сигнал. Затим, извор шума преноси сигнал до пријемника, где се врши декодовање сигнала у поруке, а потом, пријемник прослеђује поруку одредишту.

3.2 Ентропија

Прва Шенонова теорема

Ентропија представља меру неизвесности о поруци коју ће извор емитовати. Код извора са већом ентропијом, ова неизвесност је већа. Имајући у виду статистичко кодовање, Шенон је показао везу ентропије и минималног броја сигнала по поруци, потребног за представљање информација које емитује извор[9].

Из Прве Шенонове теореме може да се закључи да је за информације које је емитовао извор, постоји дефинисана доња граница до које може да се иде.

Када се говори о ентропији, мора да се дефинише какву количину информација носи порука. Шенон је сваку поруку, у дискретном извору (извор са коначним или пребројивим скупом порука), дефинисао као логаритам реципрочне вредности вероватноће поруке:

$$\boldsymbol{H(S) = \overline{Q(Si)} = \sum_{i=1}^{q} P(Si) ldP(Si)\ [\frac{Sh}{simb}]}$$

Количина информација коју носи нека порука обрнуто је сразмерна њеној (априорној) вероватноћи понављања:

$$\boldsymbol{Q(Si) = ld\left(\frac{1}{P(Si)}\right) = -ld\big(P(Si)\big)\ [Sh]} \text{ или } \boldsymbol{[bit]},$$

где је 1 Шенон $[\boldsymbol{Sh}]$или $[\boldsymbol{bit}]$ је количина информације коју садржи порука о догађају који има само два једнако вероватна исхода.

Друга Шенонова теорема

У вези са заштитним кодовањем, Шенон је показао да се увек може наћи такав код, да се вероватноћа грешке учини произвољно малом, све док је проток информација из извора мањи од величине коју је назвао капацитет канала (C). Ова величина са своје стране зависи од фреквенцијског опсега и односа сигнал-шум. Узимајући у обзир захтеве корисника, Шенон је дефинисао функцију оштећења информација – *R(D),* која представља минималну количину информација (по поруци) коју треба пренети кориснику, а да при томе да оштећење информација не буде веће од оног оштећења које дозвољава корисник, квантитативно описаног са *D.*

Друга Шенонова теорема гарантује постојање добрих зашитних кодова и оцењује основу за заштитне кодове – кодове за контролу грешака.

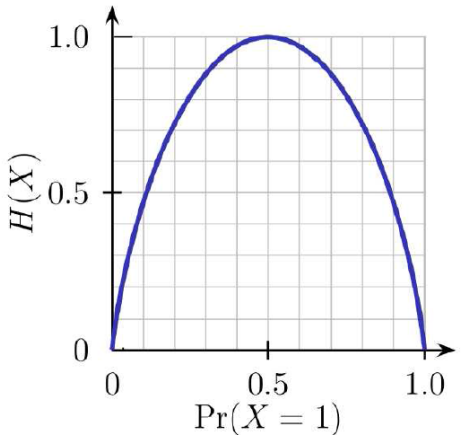
Из Друге Шенонове теореме може да се закључи да је дефинисана најмања горња граница информационе мере чистог податка, који може бити послат датом просечном сигналном јачином S, кроз аналогни комуникациони канал.

Важно је дефинисати и ентропију бинарног извора информација, где се каже да један извор, да би уопште могао да емитује информације, мора на располагању да има бар два симбола. Такав извор се назива бинарни извор информација.

Симболи се могу обележити са s_1 и s_2, али је уобичајено да се они обележавају са 0 и 1 – тј. симболи се називају бити. Нека је P(0) = P, тада је P(1) = 1-P и ентропија је:

$$P(0) = Pld\frac{1}{P} + (1-P)ld\frac{1}{1-P}[\frac{Sh}{b}]$$

Ова функција се често назива ентропијска функција и означава се са *H(X*) и на слици 3.2 је приказана.



Слика 3.2: Ентропија случајне варијабле са два исхода
(Проф. др М.Милосављевић, Лекција 2 - Ентропија)

Опште познати закључак је да је ентропија максимална када су вероватноће оба симбола подједнаке, *P = 1-P = 0.5* и тада износи *1[Sh/b]*. Дакле, у зависности од вероватноћа појављивања „нула“ и „јединица“, један бит може у просеку да носи количину информација која се креће између 0 и 1 шенона.

3.3 1 Дискретни извори с меморијом

Код извора са меморијом, појављивање, односно, емитовање једног симбола зависи од низа претходно емитованих симбола, тј. „стања“ извора. Ако је дужна овог низа коначна и износи *m*, таа се ради о извору с меморијом *m*-тог реда. Ови извори су познати као Марковљеви извори *m*-тог реда. На излазу из Марковљевог извора, појављује се Марковљев низ (енгл. *Markov chain*). Дискретни извори с

коначним скупом стања, често се називају „коначни Марковљеви извори (низови)“ (енгл. *finite Markov chains*). Извор без меморије је Марковљев извор нултог реда.

На излазу из дискреног извора са меморијом, појављује се дискретан случајни процес с меморијом. Ако је овај процес (извор) *m*-тог реда, тада се он математички описује листом симбола:

$$S \{s_1, s_2, \dots, s_q\},$$

и скупом условних вероватноћа емитовања једног симбола, када се зна претходно емитован низ дужине *m*, тј.:

$$P(S_j / Si_1, Si_2, \dots, Si_k, Si_m)\ (j = 1,2,\dots,q)\ (i_k = 1,2,\dots,q)\ (k = 1,2,\dots,m),$$

где је Si_1 најстарија а Si_m њмлађи симбол, после чега следи симбол S_j.[9]

Овакав дискретан извор није добар за псеудослучајни генератор *PRNG*. Марковљеви извори могу да се доведу са софтверским генераторима бројева, где је, након одређеног броја понављања алгоритма, могуће знати емитовани низ унапред.

3.3 2 Дискретни извори без меморије

У дискретном извору без меморије постоји дефинисан скуп са листом порука:

$$S \{s_1, s_2, \dots, s_q\},$$

и скупом њима одговарајућих вероватноћа:

$$P(S_i)\ (i = 1,2,\dots,q),$$

где се емитовање симбола, брзином *v [simb/s]* представља као потпун скуп међусобно искључивих догађаја. На основу тога, може да се одреди колику симболи носе количину информација:

$$Q(Si) = ld\left(\frac{1}{P(s_i)}\right)[Sh], (i = 1,2, \dots q)$$

Након познатих вредности, може да се одреди средња количина информација, по једном симболу, коју емитује извор:

$$H(S) = -\sum_{i=1}^{q} P\,(s_i) ld P(s_i) \quad [\frac{Sh}{s}]$$

Када је одређена средња количина информација, по једном симболу, коју емитује извор, могуће је одредити просечну брзину информација.

$$\Phi(S) = \upsilon H(S)[\frac{Sh}{s}]$$

Овде се уводи термин - информациони флукс извора или само флукс. Из дате форумле, може да се каже да је просечна брзина којом извор емитује информације средња количина информација у секунди, односно, шенона по секунди.

3.4 Савршена тајност

Користећи уведени појам ентропије, Шенон је дефинисао савршену тајност која се састоји у томе да се ентропија (неизвесност) употребљеног кључа не смањује, без обзира колико дугачак криптограм стајао на располагању. Дао је и одговарајући услов везујући ентропију кључа са ентропијом поруке која је шифрована. Интересантно је да је и одредио везу дужине криптограма потребног за дешифровање (тј. одређивање употребљеног кључа) и сувишности садржане у шифрованој поруци за случај једноставне (моноалфабетске) шифре.

3.5 Псеудослучајни генератори

Потреба за случајним и псеудослучајним бројевима јавила се због велике примене у криптографским системима. Заједничко за све криптографске системе је потреба за криптолошким кључем који је генерисан на случајан начин. Многи криптографски протоколи, протоколи за аутентификацију, *RSA* алгоритми за генерисање дигиталног потписа користе на улазу случајне или псеудослучајне вредности. Најчешће коришћени генератори случајних бројева су генератори псеудослучајних бројева (PRNG). *PRNG* генератори користе детерминистички систем и иницијални сид (енгл. seed - семе) за генерисање излазног низа.

Шенонова ентропија излаза зависи од ентропије сид-а и никада је не може надмашити.

Случајни бинарни низ може да се тумачи као резултат бацања новчића који је означен са „писмо“ или „глава“, где је вероватноћа исхода (0 и 1) приближно 0,5.

Један од добрих примера генаротара случајних бројева је бацање новчића, јер главу и писмо можемо да дефинишемо као 1 и 0. Као што је дефинисано у Теорији информација, мера неизвесности неког догађаја да ће се десити је управо овај пример; не може се знати шта ће пасти, глава или писмо, односно 1 или 0. Управо је то суштина *PRNG*-а, да се низ генерише независно. Дакле, из примера са новчићем не можемо да знамо који је следећи исход, с обзиром да је вероватноћа исхода сваки пут 0,5.

Репродуктивност *PRNG*-а, тј. могућност генерисања истог излазног низа, има велике предности код симулација. Поред тога, зависност ентропије и избор сид-а јесу велики изазов за његову експлоатацију, паралелизам и скалабилност. Познато је да *PRNG* генератори одговарају потребама многих апликација. Међутим, у неким случајевима генерисаним вредностима недостају јаке статистичке карактеристике. То су захтевне ситуације у којима се *PRNG* генератори замењују са *TRNG*, као што су генерисање криптографских кључева, генерисање листа код игара на срећу или статистичке симулације**.**

Код оваквих генератора, најбитније је да су они са униформном расподелом и да су њихови бројеви случајни.

Постоје два начина за генерисање случајних бројева коришћењем рачунара. Псеудослучајни генератори бројева *PRNG* и истинито случајни генератори бројева *TRNG*.

Псеудослучајни генератори су алгоритми који на основу почетних (иницијалних) стања дају излазни низ псеудослучајних бројева. Почетни услов је задовољен уколико је улаз у генератор истински случајан. Управо се на овој тези заснива овај дипломски рад. Суштина је да се докаже да на основу буке (шума), коју генерише транзистор из генератора, да су то истински случајни бројеви.

3.6 ANSI X9.17

ANSI X9.17 је један од најчешће коришћених генератора при конструисању криптографских апликација. Користи се за генерисање тајних кључева код *DES* алгоритма, као и приликом добијања почетних вредности иницијализационог вектора. Основу овог генератора псеудослучајних бројева чини насумична, односно, непредвидива вредност почетног стања (сид-а) и временски параметар. Вредност генератора је низ који задовољава ANSI X9 стандард по препоруци *NIST*-а.

ANSI X9.17 генератор шифровање обавља помоћу троструког *DES* алгоритма са два кључа. Улазни подаци генератора су шездесетчетворо-битна вредност *s* (енгл. seed) која се генерише на сонову тренутног времена и датума, затим, цели број *m* и кључеви за шифровање K_1 и K_2 . Генератор обавља шифровање помоћу следеће функције:

$$I = E_k^3(s)$$

Алгоритам се даље одвија према следећим корацима:

Рачуна се вредност *I = E(D),* где је *D* 64-битни запис тренутног времена, а следећи корак је:

$x_i = E_k(I \oplus s)$ и $s = E_k(x_i \oplus I)$, излаз из генератора је 64-битни низ случајних бројева $x_1, x_2 ... x_m$.

Овај генератор се показао довољно сигурним, односно, употребљивим у већини примена, али је потребно напоменути да није формално доказано да је овај алгоритма криптографски сигуран. Предности примене ANSI X9.17 генератора су једноставније извођење и знатно већа брзина у односу на остале криптографске генераторе псеудослучајних бројева.

3.7 Комуникације

Комуникације или телекомуникације су део области електротехнике која се бави начином како се преносе информације са једног места на друго. Информације се преносе помоћу електричних проводника, електромагнетских таласа, класичним кабловима, оптичким кабловима, итд. Један од важних проблема који се решава комуникацијама је начин на који се информације утискују у електрични сигнал. Тај процес се назива модулација или кодовање и обавља се на предајној страни, док се на пријемној страни обавља обрнути процес који се назива демодулација или декодовање. У процесу преноса настаје и деградација или такозвано изобличење сигнала због дејства сметњи или шума, па се у комуникацијама велика пажња придаје методима за извлачење корисних информација из шума и методима за заштиту информација.

Рачунарско инжењерство је једна од области електротехнике које се бави развојем и пројектовањем рачунарског хардвера и софтвера који контролише његов рад. Савремени рачунарски системи могу бити веома различити, почев од једноставних микроконтролера који обављају једноставне надзорне функције, преко персоналних рачунара и радних станица који се користе за обављање разноврсних апликација, слушања музике, гледање филмова и игру, па до моћних суперрачунара за извршавање комплексних прорачуна у физици, метеорологији и истраживању свемира.

3.8 Електроника

Област електронике се бави проучавањем и конструкцијом електронских елемената којима се контролише ток струје повезивањем таквих елемената у сложена кола која обављају жељену функцију. Основни елементи савремене електронике су диоде и транзистори који се повезују у дискретна или интегрисана кола. Поред тога, електроника се бави и пројектовањем електронских кола за одређене намене, развојем алгоритама за пројектовање, развојем и применом рачунарске подршке процесу пројектовања, имплементацијом електронских кола која реализују разне методе потребне у осталим областима електротехнике, итд.

Најпре ће бити дефинисане основе из области електронике, биће дат основни теоријски приступ о напону, струји, као и о елементима електричног кола.

3.8.1 Напон

Напон представља потенцијалну енергију. Разлика потенцијала представља способност преноса наелектрисања у току струје.

Јединица за напон је *V* (Волт) и представља енергију од 1 *J* (џул), која је потребна за померај позитивног наелектрисања од 1 *C* (кулон). Уобичајена ознака за напон електроници је *V* или *v*.

Посматрајући инкременталне промене енергије и наелектрисања, тренутни напон се може дефинисати као:

$$v = \frac{dw}{dq}$$

3.8.2 Електрично оптерећење

Електрично оптерећење је фундаментално својство материје које се не може се створити нити уништити. То значи да ако се наелектрисање одстрани са неког места, оно се мора појавити на неком другом месту. Постоје два типа наелектрисања: позитивно и негативно наелектрисање. Два нелектрисања се међусобно привлаче ако су супротног поларитета или међусобно одбијају ако су истог поларитета.

Упрошћена структура атома се састоји од позитивно наелектрисаног језгра и електрона који круже око језгра по различитим орбитама. Електрично оптерећење електрона је најмање наелектрисање које постоји. Електрично оптерећење једног електрона назива се елементарно наелектрисање или квант наелектрисања. Позитивно наелектрисање језгра је компензовано истом количином негативног наелектрисања електрона, па је атом електрички неутралан. Међутим, пошто се електрони из најудаљенијих орбита могу на разне начине одвојити од атома, атом

може постати наелектрисан (тада се назива јон), а електрони се могу кретати и формирати електричну струју.

Уобичајени симбол за оптерећење је q (Q), а јединица кулон (C). Електрично оптерећење једног електрона је $-1{,}602\times10^{-19}$ C.

3.8.3 Енергија

Енергија је важан појам у анализи електричних кола. У електротехници и електроници се срећемо са елементима који примају енергију од кола или предају енергију колу. Смер преноса енергије зависи од знакова напона и струје.

3.8.4 Електрично поље

Око сваког наелектрисаног тела постоји поље које се назива електрично поље. Јачина електричног поља се дефинише као вектор чији је интензитет:

$$E = \frac{F}{q}$$

где се правац и смер поклапају са смером силе која делује на позитивно електрично опетрећење. Електрично поље око тачкастог налектрисања је:

$$E = k\,\frac{q}{d^2}$$

3.8.5 Идеални електрични елементи

Идеални електрични елементи су комплетно описани математичком релацијом између напона на елементу и струје кроз елемент. Идеални електрични елементи се могу поделити на активне или пасивне зависно од тога да ли предају енергију остатку кола или примају енергију из кола.

3.8.6 Проводници, изолатори и полупроводници

Материјал код којег су електрони лако покретљиви назива се проводник. Типични проводници су метали: сребро, злато, бакар, алуминијум, итд. Код метала електрони из спољашњих орбита атома могу лако напустити атоме. Такви електрони се називају слободни електрони и они омгућавају лако успостављање електричне струје.

Материјал код којег су електрони слабо покретљиви назива се изолатор или диелектрик. Типични изолатори су неметали: стакло, пластичне масе, керамика, гума итд. Наелектрисање које се доведе на изолатор остаје непокретно и назива се статички електрицитет. Изолациони материјали се често користе за изоловање проводника да би се спречио нежељени додир два проводника и успостављање струје између њих.

Полупроводници су по својим особинама негде између проводника и изолатора и умерено се супростављају кретању носилаца електрицитета. Најважнији полупроводници су силицијум, германијум, галијум арсенид, итд. Полупроводнички материјали су основ савремене електронике.

Отпорност је мера супростављања кретању носилаца електрицитета. Проводници имају малу отпорност, док изолатори имају велику отпорност. На пример, отпорност бакра је око 10^{25} пута мања од отпорности кварца истих димензија.

3.8.7 Електрична струја

Електрична струја је један од основних појмова у електротехници и представља меру количине електрицитета која се померила у јединици времена. Померај наелектрисања може се вршити на различите начине. Код металних проводника, механизам померања је кретање слободних електрона. У растворима механизам померања је кретање позитивно или негативно наелектрисаних јона, као што је то случај у електрохемијским батеријама или у поступку галванизације. У полупроводницима наелектрисање се креће кретањем слободних електрона или шупљина које су носиоци позитивног наелектрисања. Уобичајена ознака за струју је *I* или *i.* Јединица за струју је ампер (*A*) и представља померај наелектрисања од једног кулона за једну секунду (1 C/s). По конвенцији се узима да смер струје одговара смеру кретања позитивног наелектрисања.

Просечна (средња) струја *I* се дефинише као количник укупног помереног наелектрисања Δq и временског интервала у коме се врши тај померај Δt:

$$I = \frac{\Delta q}{\Delta t}$$

С друге стране, тренутна струја и се дефинише као брзина промене наелектрисања, односно први извод количине електрицитета по времену:

$$i = \frac{\mathrm{d}q}{\mathrm{d}t}$$

У случајевима када се струја састоји од кретања два типа носилаца, тренутна струја се може изразити и на следећи начин:

$$i = \frac{\mathrm{d}q}{\mathrm{d}t} = \frac{dq^{+} + dq^{-}}{dt}$$

где је $\mathrm{d}q+$ померено инкрементално позитивно наелектрисање док је $\mathrm{d}q-$ померено инкрементално негативно наелектрисање (инкрементално: фиксно или променљиво повећање/смањење вредности наелектрисања, тј.промена количине наелектрисања у јединици времена).

У електротехници се срећу врло различите вредности струје. Струја код муња и громова је реда величине од неколико десетина хиљада ампера. У индустријским погонима и електричним возилима струје су реда стотину ампера. Уређаји у домаћинству обично раде са струјама у опсегу од 0,5 A до 16 *A*. У електронским колима струје су реда *mA, μA* или *nA*. У разним мерним уређајима у физици струје могу бити врло мале, реда *pA* (10-12 *A*), колике су и струје између нервних ћелија код живих бића.

3.9 Електрично коло

Електрично коло представља интерконекцију два или више елемената. Повезивање елемената се врши проводницима чија се отпорност може занемарити.

3.9.1 Први (струјни) Кирхофов закон

Први Кирхофов закон се односи на струје у колу и гласи:

„Алгебарска сума струја које утичу у ма који чвор кола једнака је нули.“

$$\sum_{j-1}^{N} I_j = 0$$

где је I_j струја *j*-те гране која улази у чвор, док је *N* број грана које улазе у чвор. По конвенцији се струје чија је референтна оријентација ка чвору узимају се са позитивним предзнаком, док се струје чија је референтна оријентација од чвора узимају са негативним предзнаком.

Алтернативна дефиниција првог Кирхофовог закона гласи:

„Сума струја које утичу у ма који чвор кола једнака је суми струја које истичу из истог чвора.“

3.9.2 Други (напонски) Кирхофов закон

Други Кирхофов закон се односи на напоне у струјном колу и гласи:

„Алгебарска сума напона у било којој петљи кола једнака је нули.“

$$\sum_{j-1}^{N} V_j = 0$$

где је V_j напон на *j*-тој грани петље која укупно има *N* грана. По конвенцији се напони на гранама чија је референтна оријентација супротна оријентацији петље узимају се са позитивним предзнаком, док се напони на гранама чија је референтна оријентација иста са оријентацијом петље узимају са негативним предзнаком.

3.9.3 Паралелна и серијска веза отпорника

Први и други Кирхофов закон описују стање сваког електричног кола. Међутим, када се примене на кола са само једним паром чворова, или на кола са само једном петљом, они дају неке врло корисне резултате, који се могу применити за упрошћавање електричних кола.

3.9.4 Серијска (редна) веза отпорника

Ако се *N* отпорника тако повеже тако да се у сваком чвору стичу само по два отпорника (осим код првог и последњег чвора), таква веза се назива серијска или редна веза отпорника. За једину петљу у колу се може написати једначина по другом Кирхофовом закону:

$$V = R_1 I_s + R_2 I_s + \cdots + R_N I_s (R_1 R_2 + \cdots + R_N) I_s$$

Ако су напон извора и струја кроз извор у оба кола исти, онда се за еквивалентну отпорност добија:

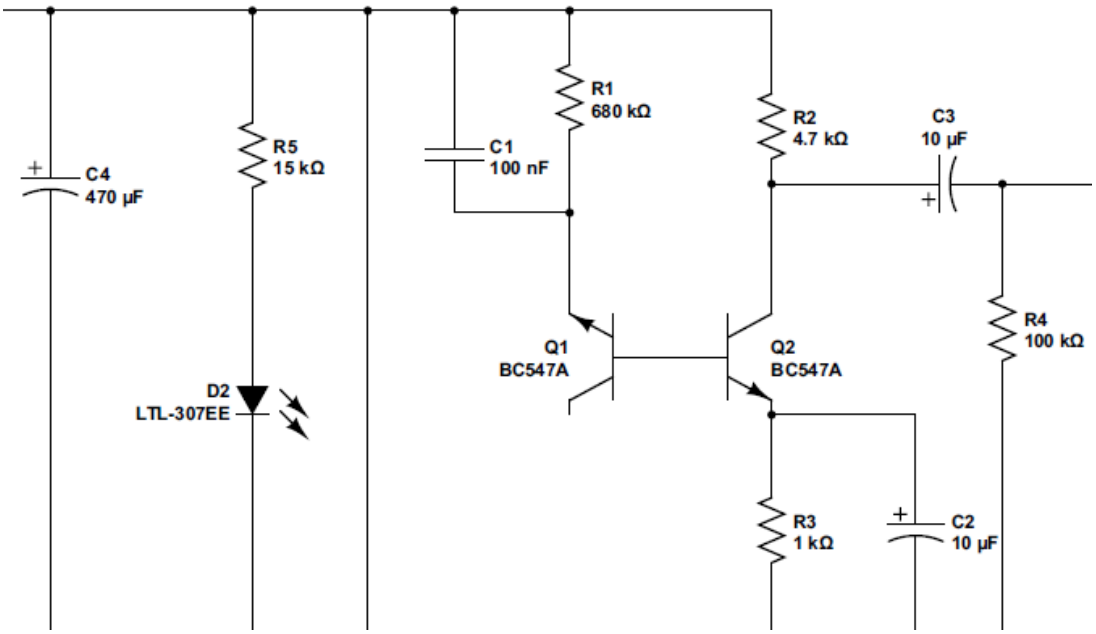
$$R_s = R_1 R_2 + \cdots + R_N$$

односно, еквивалентна отпорност серијски везаних отпорника једнака је збиру појединачних отпорности.

3.9.5 Паралелна веза отпорника

Ако се *N* отпорника тако повежу да сви имају заједничке прикључке, таква веза се назива паралелна веза отпорника и приказана је на слици. За чвор у коме су повезани напонски извор и сви отпорници се може написати једначина по првом Кирхофовом закону:

$$I_p = G_1V + G_2V + \cdots + G_NV = (G_1 + G_2 + \cdots + G_N)V$$



Слика 3.9.1: Паралелна веза отпорника

3.9.6 Наизменична струја

Посебна класа електричних кола су кола код којих су напони и струје побудних извора синусоидалне функције времена. У режиму који настаје после смиривања прелазних појава, напони и струје елемената кола ће такође имати исти временски облик, тј. представљаће синусоидалне функције времена. У електротехници је интерес за проучавање оваквих кола велики с обзиром на чињеницу да је наизменични напон доминантан у снабдевању електричном енергијом у домаћинствима и индустрији. Такође, пошто се применом Фуријеове анализе може показати да се било каква периодична функција може представити збиром синусоидалних функција, за анализу кола са сложеним периодичним побудама може се применити принцип суперпозиције.

Анализа кола помоћу фазора (вектора чији смер одређује фазу, а износ амплитуду) неке периодичке појаве представља анализу кола у фреквенцијском домену. У фазорској анализи се систем диференцијалних једначина са синусоидалним побудним функцијама у временском домену трансформише у

систем алгебарских једначина са комплексним коефицијентима у фреквенцијском домену. Такав систем је неупоредиво лакши за решавање. Када се одреде непознати фазори, они се поново трансформишу у временски домен да би се добило решење оригиналног система диференцијалних једначина.

Ова функција је периодична са периодом од 2π радијана. Период ове функције T и учестаност синусоиде f су повезани релацијом:

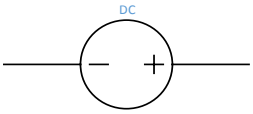
$$f = \frac{1}{T}$$

где из услова периодичности следи:

$$x(t) = X_M \sin(\omega + \theta),$$

где је θ фазни угао или почетна фаза.

Анализа кола помоћу фазора представља анализу кола у фреквенцијском домену. У фазорској анализи се систем диференцијалних једначина са синусоидалним побудним функцијама у временском домену трансформише у систем алгебарских једначина са комплексним коефицијентима у фреквенцијском домену. Такав систем је неупоредиво лакши за решавање. Када се одреде непознати фазори, они се поново трансформишу у временски домен да би се добило решење оригиналног система диференцијалних једначина.



Слика 3.9.2: Симбол наизменичне струје

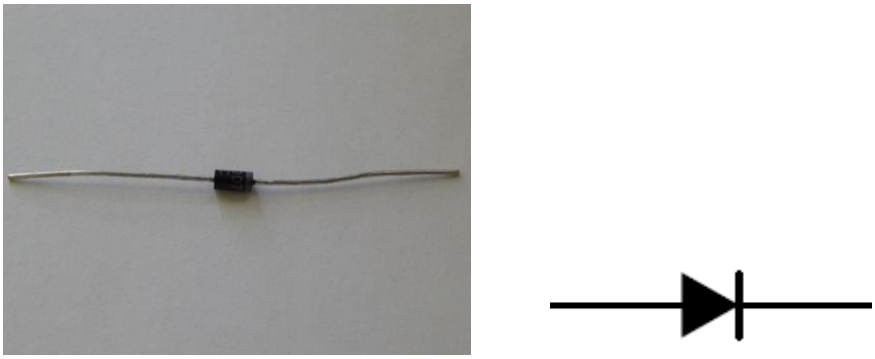
3.9.7 Елементи електричног кола

У наставку текста биће описане компоненте електричног кола.

3.9.7 1 Диода

Диода је електронска компонента која дозвољава проток електричне струје у једном смеру без отпора (или уз веома мали отпор) док у супротном смеру представља бесконачан (или бар веома велики) отпор. Зато се за диоду каже да постоји проводни и непроводни смер. Може се сматрати да за протицање струје у проводном смеру диода има отпорност колико и жица проводника (нула), а за непроводни смер се може

посматрати као прекид проводника (бесконачно). Диоде се производе, углавном, од полупроводничких материјала као што су силицијум или германијум. Међутим, још увек постоје и диоде са термојонском емисијом, некада популарне електронске цеви.

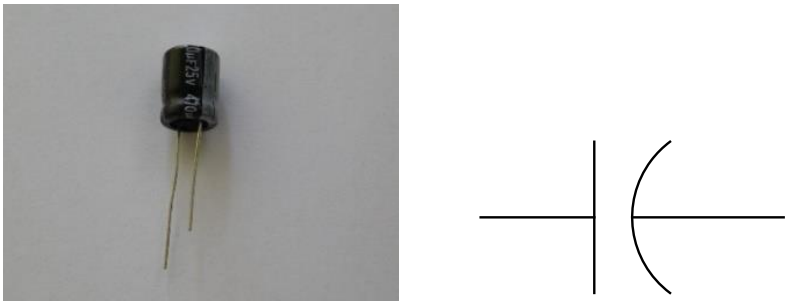


Слика 3.9.3: Диода и њен симбол

Другим речима, диода омогућава да струја тече у само у једном смеру, у оном смеру, где је постављена стрелица симбола.

3.9.7 2 Кондензатори

Кондензатор је електротехнички елемент, који може да сачува енергију у облику електричног поља између двеју електрода раздвојених са изолатором (диелектриком).



Слика 3.9.4: Поларизовани кондензатор (лево) и његов симбол (десно)

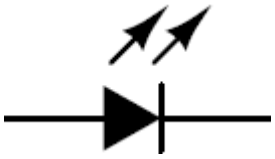
Његова битна величина је капацитивност. СИ јединица за електричну капацитивност је *F* (фарад) по Мајклу Фарадеју. Пошто је фарад веома велика вредност, најчешће се користи са префиксима микро (*μ*), нано (*n*) и пико (*p*) за кондензаторе. Кондензатори се разликују по материјалу, од ког је сачињен диелектрик: ваздух, папир, металопапир, алуминијум силикат, и сл.

3.9.7 3 Светлећа (LED) диода

LED, односно светлећа диода (енгл. LED; Light-emiting diode) је посебна врста полупроводничке диоде која емитује светлост када је пропусно поларисана, тј. када кроз њу тече струја. Фотони светлости се емитују приликом рекомбинације пара електрон-шупљина. Такво својство имају полупроводници: галијум-фосфид (GaP), галијум-арсенид (GaAs), галијум-нитрид (GaN), галијум-арсенид-фосфид (GaAsP), цинк-селенид (ZnSe), дијамант (C), алуминијум-нитрид (AlN), сафир (Al2O3), силицијум-карбид (SiC), итд. Боја емитованог светла зависи од врсте полупроводоника, као и од примеса у њему, и варира од инфрацрвеног до ултраљубичастог дела спектра.



Слика 3.9.5: Светлећа диода



Слика 3.9.6: Симбол светлеће диода

У конструисаном псеудослучајном генератору, боја светлеће диоде нема никакве везе са функционисањем генератора.

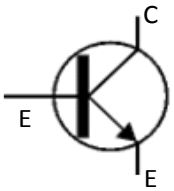
3.9.7 4 Транзистори, типа НПН

Постоје два типа биполаризована транзистора: НПН и ПНП. ПНП се данас ретко користе, док су НПН транзистори у чешћој употреби због лакше израде. У овом раду, за конструисање генератора, је коришћен НПН транзистор.

Транзистор је активни полупроводнички елемент са три извода (два приступа) који се користи најчешће као појачивач, за прекидање струје, за стабилизацију напона у струјним колима, за модулацију сигнала и многе друге операције.



Слика 3.9.7: НПН транзистор



Слика 3.9.8: Симбол НПН транзистора

Ознаке на транзистору су следеће:

- B – База
- C – Колектор
- E - Емитор

Једна од основних намена кондензатора је да појача напон, такође, могуће га је користити, као прекидач, као појачало и др. На конструисаном псеудослучајном генератору бројева, кондезатор има намену – да „глуми“ појачало, односно, да прави и појачава буку (шум).

3.9.7 5 Отпорници

Отпорник (енгл. resistor) је пасивна електронска компонента са два извода (једним приступом) која пружа отпор струји, стварајући притом пад напона између прикључака. Пружање отпора струји као основна особина отпорника описује се електричним отпором. Према Омовом закону електрични отпор једнак је паду напона на отпорнику подељеном са јачином струје која протиче кроз отпорник.

Другим речима, отпор је константа сразмере између напона и струје отпорника.



Слика 3.9.9: Отпорници



Слика 3.9.10: Симбол отпорника

Отпорник се користи као елемент у електричним мрежама и електронским уређајима. Још један од примера како отпорник контролише проток струје је када је отпорник смештен у низ са светелћим диодама, он контролише, односно, ограничава проток струје кроз њих.

Отпорници имају више намена:

- Ако је струја у колу позната, тада се отпорник користи за стварање познате разлике потенцијала пропорционалне тој струји. Обрнуто, уколико је позната разлика потенцијала између две тачке у колу, тада се отпорник може користити за стварање познате струје пропорционалне тој разлици потенцијала.

- Отпорник се може користити за ограничавање јачине струје. Постављањем отпорника у серију с неком другом компонентом, као што је *LED* диода, струја кроз ту компоненту се ограничава на познату и дозвољену вредност.

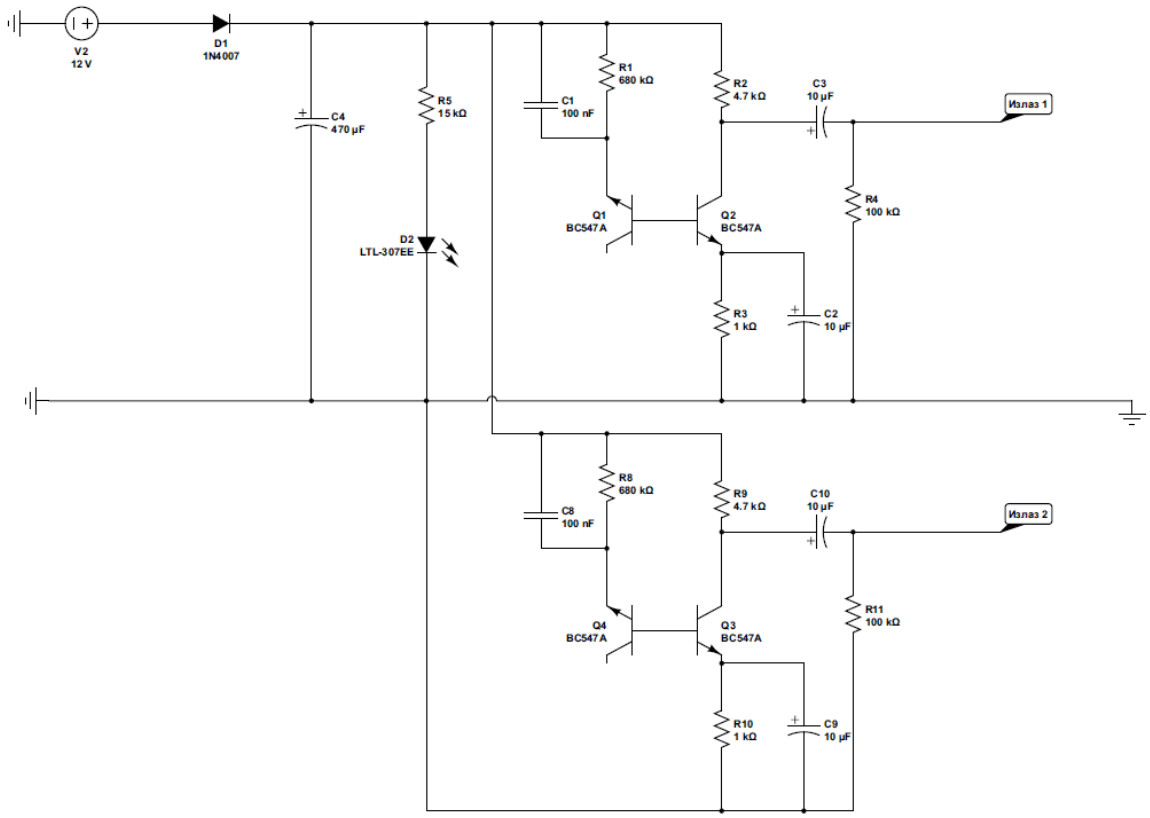
- Пригушивач (атенуатор) је мрежа два или више отпорника (делитељ напона) који служе за смањење напона сигнала.

- Линијски терминатор је отпорник на крају преносне линије, конструисан као завршна импеданса (отпор чија вредност отпора одговара отпору остатка кола на који је спојен) и тиме минимизира рефлексију сигнала.

Јединица мере за отпорник је 1*Ω* (Ohm). За ознаку јединице мере се користи грчко слово омега *Ω*. Поменута величина је толико мала, да се за отпорнике величине крећу од *кΩ* или *МΩ*.

4 Преглед предложеног решења

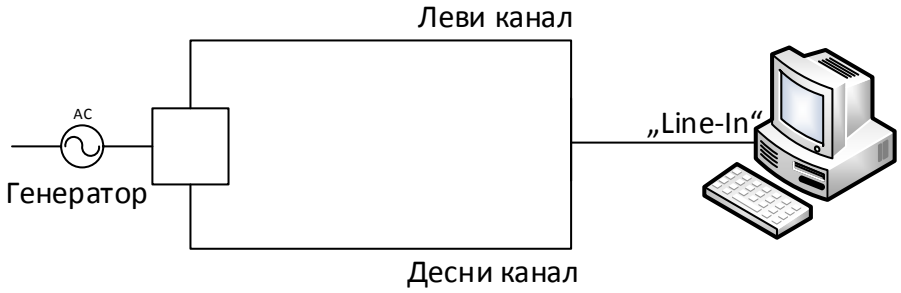
4.1 Генеричка шема предложеног решења



Слика 4.1: Генеричка шема предложеног решења

На генеричкој шеми предложеног решења приказано је електрично коло псеудослучајног генератора бројева *PRNG* који ствара шум, односно буку.

На слици 4.2 је приказана шема генератора, како функционише у пракси.



Слика 4.2: Генератор у пракси

Псеудослучајни генератор функционише на следећи начин: генератор добија наизменичну струју од 12 волти од извора, која напаја диоду, типа *1N4007*. Поменута диода служи да спречи нежељени ефекат, као нпр. обрнути поларитет. Светлећа (LED) диода има функцију да прикаже да ли има струје у генератору. Уколико светлећа диода светли - има струје у електричном колу; уколико не светли – нема струје у колу. Отпорницима се регулише јачина струје у појединим деловима кола на познату и дозвољену вредност. Затим, на генератору се налазе транзистори, типа НПН, који служе за за прављење буке, односно, шума.

На самом генератору постоје две паралелне гране електричног кола које емитују шум из истог типа транзистора. Излаз са електричног кола је аудио излаз, који се директно повезује у звучну картицу рачунара, у *line-in* улаз.

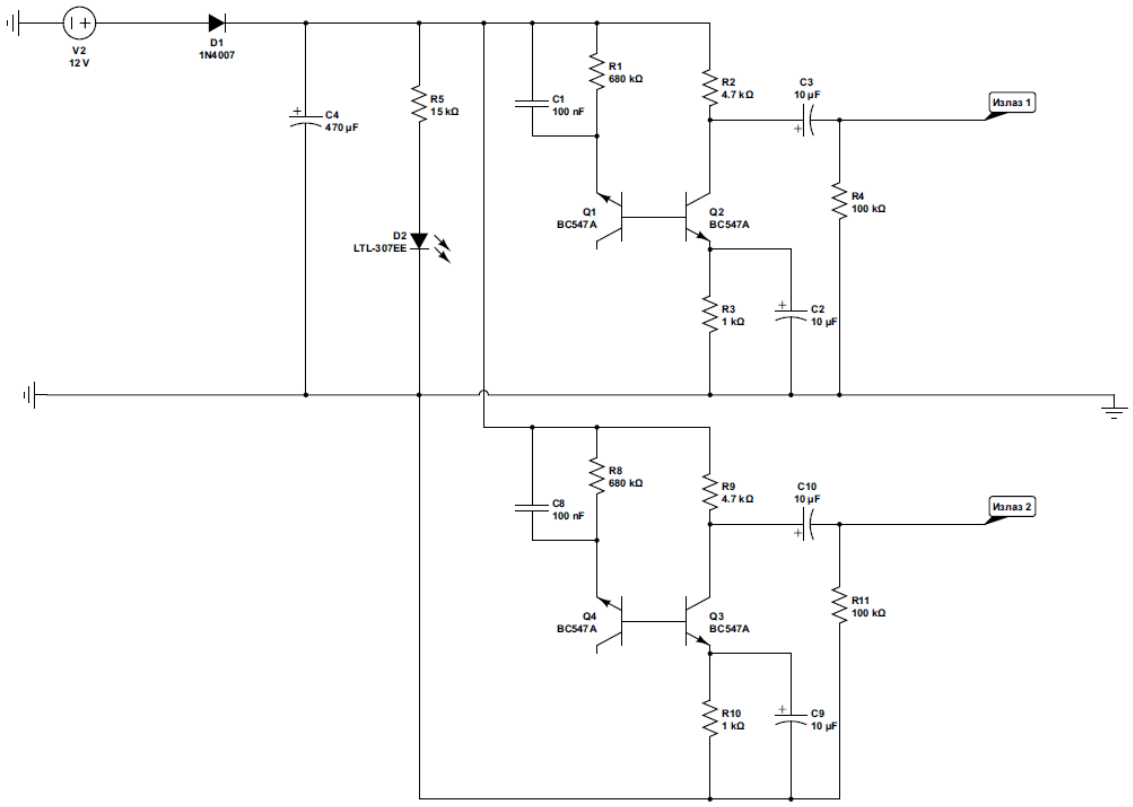
4.2 Поставка и објашњење експерименталног окружења

Експериментална софтверска окружења која су коришћена су алат *MATLAB* и програмски пакет *Sound Forge*. Алат *MATLAB* је врло погодан алат за рад статистичких тестова и ефикасан је за генерисање, испитивање и анализирање велике количине бројева. *MATLAB* је алат који је ефикасан за испитивање ентропије, приказивање графова и хистограма, погодан за обрађивање комплексних бројева, за обраду звука, вршења математичких функција и многих других операција. Програмски језик *Java* коришћен је у сврхе статистичких тестова, као што су *NIST*-ови тестови.

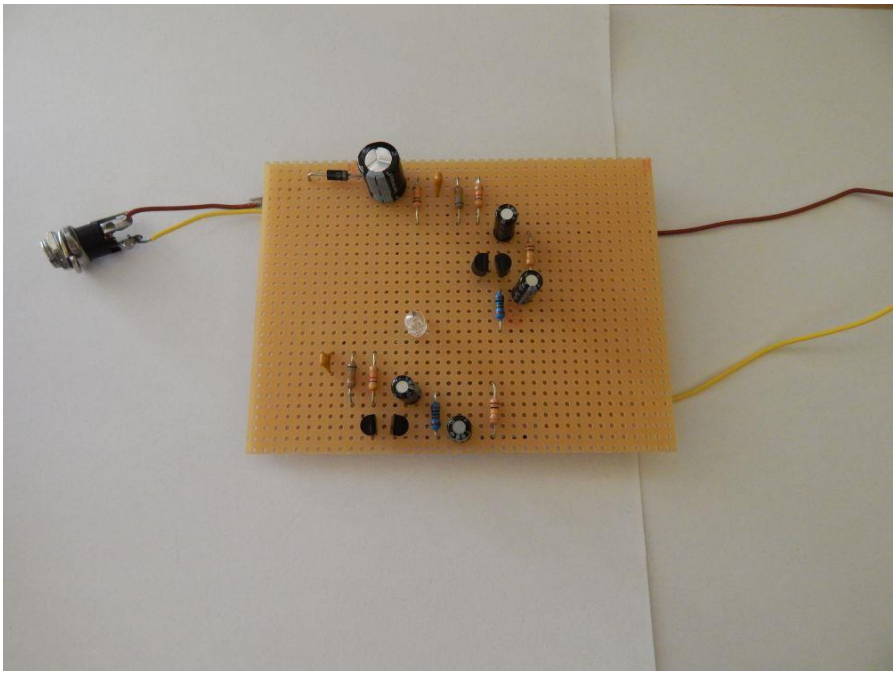
Експериментално хардверско окружење чине следећи елементи:

- Штампана плоча
- Диода (1N4007)
- Кондензатори
- *LED* диода,
- Транзистори типа НПН,
- Отпорници

На слици 4.3 приказано је електрично коло псеудослучајног генератора. На основу шеме електричног кола, могу се видети две симетричне стране, тачније, две паралелне гране стране електричног кола. Ради се о електричном колу са паралелном везом. Приказана шема електричног кола представља једноставно решење у коме транзистори, као активни полупроводнички елемнти, производе шум, односно, стварају буку. Овакав генератор је јефтин, лак за израду и ефикасан за генерисање великог броја насумичних бројева. Електрично коло је састављено из три целине, где у ствари две од три целине чине управо поменуте паралелне гране електричног кола.



Слика 4.3: Генеричка шема предложеног решења



Слика 4.4: Конструисани „PRNG“ генератор

Компоненте електричног кола са њиховим спецификацијама:

C1, C8; 0.1µf, 25 волти (најмање) керамички (µf =микро-фарад или 10^{-6} фарада);

C2, C9; 10 µf, 25 волти (најмање) електролит;

C3, C10; 10 µf, 25 волти (најмање) електролит;

C4; 10 - 470 µf, 25 волти (најмање) електролит. На шеми електричног кола је кондезатор означен величине 470 µf, али може да се стави било која друга величина;

D1 1N4001; може и било која друга диода из опсега 1N400X;

D2; било која светлећа (LED) диода – величина и боја су небитне;

Q1, Q3; било који транзистор типа НПН са јачином од 6 волти или мање;

Q2, Q4; било који НПН транзистор са струјним појачањем (познат као hFE или β) дефинисан преко 100 и идеално мање од 500;

транзистори који долазе у обзир су: BC549, BC547, BC548, PN100, 2N3904, 2N2222A.

Отпорници су реда величине:

R1, R8 680k, ¼ W
R2, R9 4.7k, ¼ W
R3, R10 1k, ¼ W
R4, R11 100k, ¼ W
R5 15k ¼ W

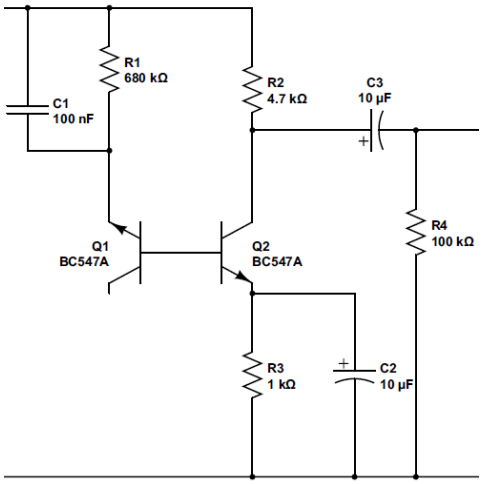
Остало:

2,5 милметра конектор за наизменичну струју. Могуће је користити било који други конектор за струју, који може да одговара утикачу. На излазу електричног кола користи се 3,5 милиметарски стерео конектор. У овом случају, на конструисаном генератору је излаз са електричног кола повезан проводницима на већ постојећи *stereo* кабл.

Коришћена је обична штампана плоча (енгл. Veroboard или Stripboard), за прављење прототипова, са већ избушеним рупама од 2,54 милиметра. За боље резултате генератора, могуће је конструисати штампану плочу познату као *PCB*.

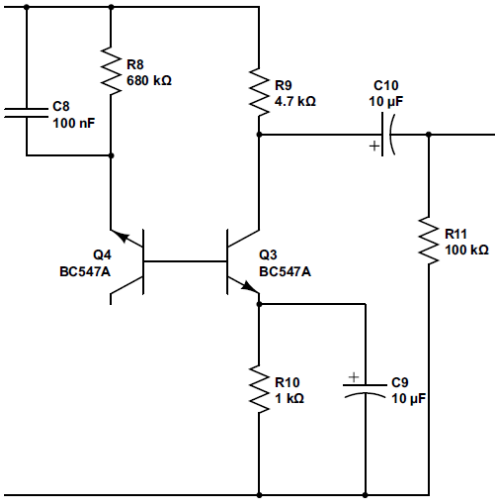
Што се тиче опреме за прављење генератора, неопходно је имати лемилицу, пасте за лемљење и уређаје за мерење и испитивање струје и напона у колу.

На слици може да се види једна целина, односно једна грана електричног кола. Свака грана електричног кола је генератор шума за себе, коју чине елементи, редом: C1, C2, C3, R1, R2, R3, Q1, Q2 – за горњу грану електричног кола.



Слика 4.5.1: Једна грана електричног кола

Што се тиче доње гране електричног кола, која уједно чини другу целину електричног кола, ту спадају елементи, редом: C8, C9, C10, R8, R9, R10, Q3, Q4

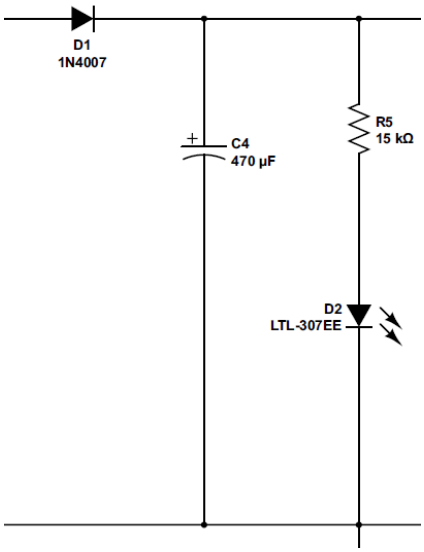


Слика 4.5.2: Друга грана електричног кола

„Обрнута волтажа“ повезана на емитор није стандардна, али ипак функционише. За тразнисторе Q1 и Q4, база је извор шума, док колектори остају неповезани.

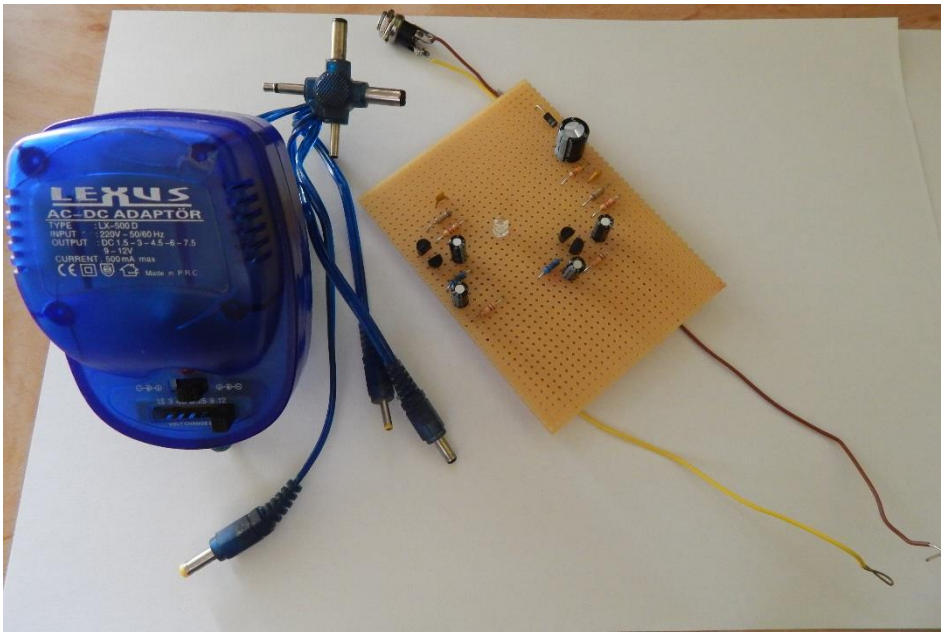
На слици (испод) налазе се прва четири елемента електричног кола, која чине:
- D1 диода, типа 1N4007,
- C4 кондензатор од 470 µf,
- R5 отпорник 15кΩ,
- D2 светлећа (LED) диода.

Диода D1 (слика 4.6) служи за спречавање било какве штете, у случају да је напајање обрнутог поларитета, јер управо обрнути поларитет може да направи штету на уређају. Један од примера каква штета може да се изазове је да се „спржи“ комплетно електрично коло.



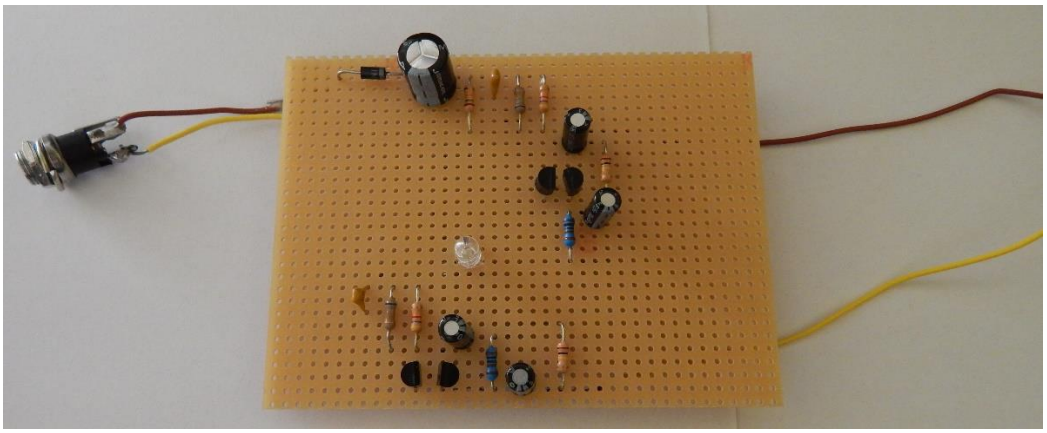
Слика 4.6: Прва целина електричног кола

У наредних неколико слика биће представљен и описан конструисани генератор. На слици 4.7 се налазе трансформатор (лево) и генератор (десно). На овом трансформатору могуће је подешавање волтаже, али за генератор је потребно струја од 12V.



Слика 4.7: Трансформатор и „PRNG“

На слици 4.8 је приказан генератор. Генератор је лемљен тако да приближно подсећа на електрично коло. Није вођено рачуна о утрошеном месту на штампаној плочи, јер се овај генератор користи у лабораторијске сврхе. Лемљење може да се уради на много начина и могућа је огромна уштеда простора на штампаној плочи, с обзиром да нема много елемената електричног кола.



Слика 4.8: PRNG

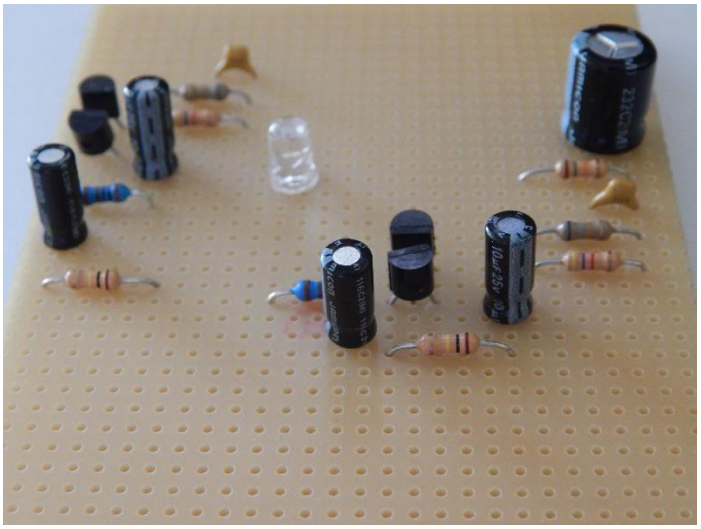
На слици 4.9 види се кабл, који се повезује (проводницима) на једном крају са излазом из генератора, а други крај се повезује у звучну картицу, у *line-in* улаз.



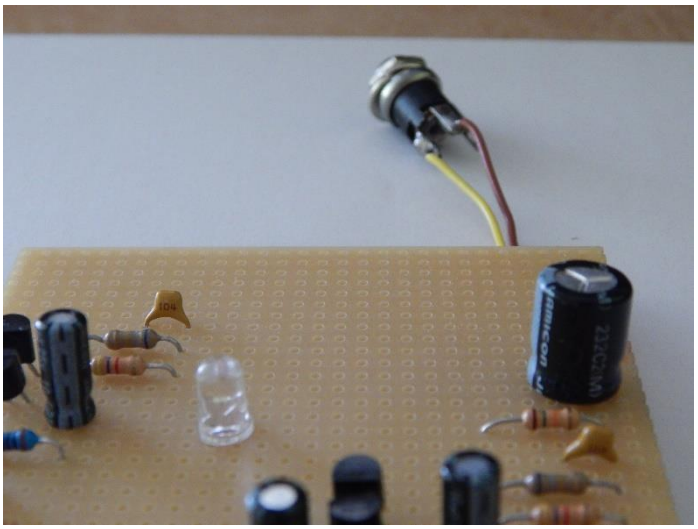
Слика 4.9: „Stereo“ кабл

Мора да се води рачуна о томе да, проводници који служе за уземљење, никако не додирну проводнике које се повезују са генератором. На слици 4.9 могу да се виде издвојни проводници које служе као уземљење.

У наредне две слике, ближе су приказани делови генератора:



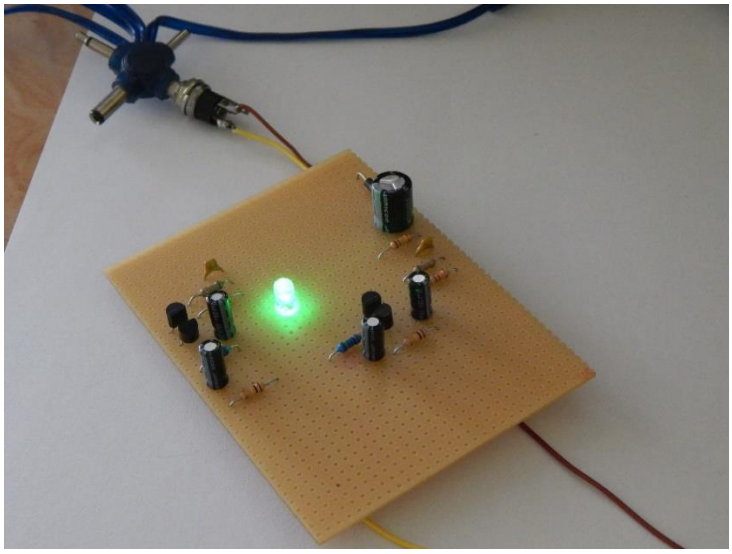
Слика 4.10: Компоненте генератора (1)



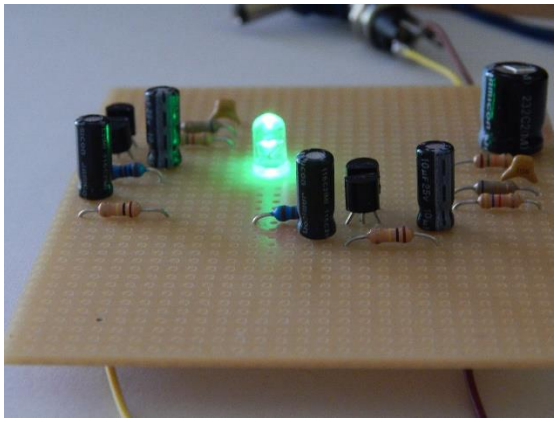
Слика 4.10.1: Компоненте генератора (2)

Као што је већ објашњено у претходном делу, када генератор почне да се напаја струјом од 12V, светлећа диода почиње да светли. Њена функција је управо да покаже да ли постоји струја у колу. Уколико светлећа диода не светли, постоји више разлога зашто не светли. Могући разлози за такав догађај су да неки елемент није добро залемљен, да елемент није правилно залемљен, да је елемент електричног кола прегорео и многи други разлози. Уколико се тако нешто деси, неопходно је узети уређај за испитивање, односно, мерење струје и напона у електричном колу и почети са детаљним испитавањем целог кола.

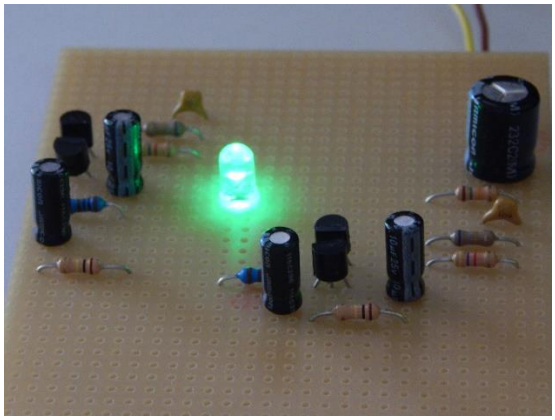
На сликама испод може да се види генератор који добија довољну количину струје, што показује да је светлећа диода активна.



Слика 4.11.1: Укључен „PRNG” (1)



Слика 4.11.2: Укључен „PRNG” (2)



Слика 4.11.3: Укључен „PRNG” (3)

4.3 Спроведене анализе и експерименти

Током тестирања генератора, вршени су разни експерименти. Мерена је ентропија извора информација, снимање шума је вршено у различитим фреквенцијама, са различтим бројем битова и различитим бројем семплова. Такође, у једном од тестова, упоређен је шум који је добијен из конструисаног псеудослучајног генератора са шумом који је доступан преко интернет странице *random.org*.

У наставку биће представљен детаљан опис активирања генератора, биће приказани сви урађени тестови, као и добијени резултати.

Псеудослучајни генератор повезујемо на трансформатор од 12V, како би добио довољно струје, затим, излази са генератора се повезују у звучну картицу, у *line-in* улаз. У зависности од звучне картице, уколико је звучна картица добро подешена у делу за снимање звука, требало би да истог тренутка чујемо шум. Уколико се не чује шум, неопходно је подесити звучну картицу. Затим, следи активирање програма за аудио снимање, попут програма *Audacity*, *Sound Forge* или било ког другог програма. За тестирање генератора, у овом раду је коришћен програмски пакет *Sound Forge*, који има веома квалитетне перфорансе и све што је неопходно за тестирање генератора.

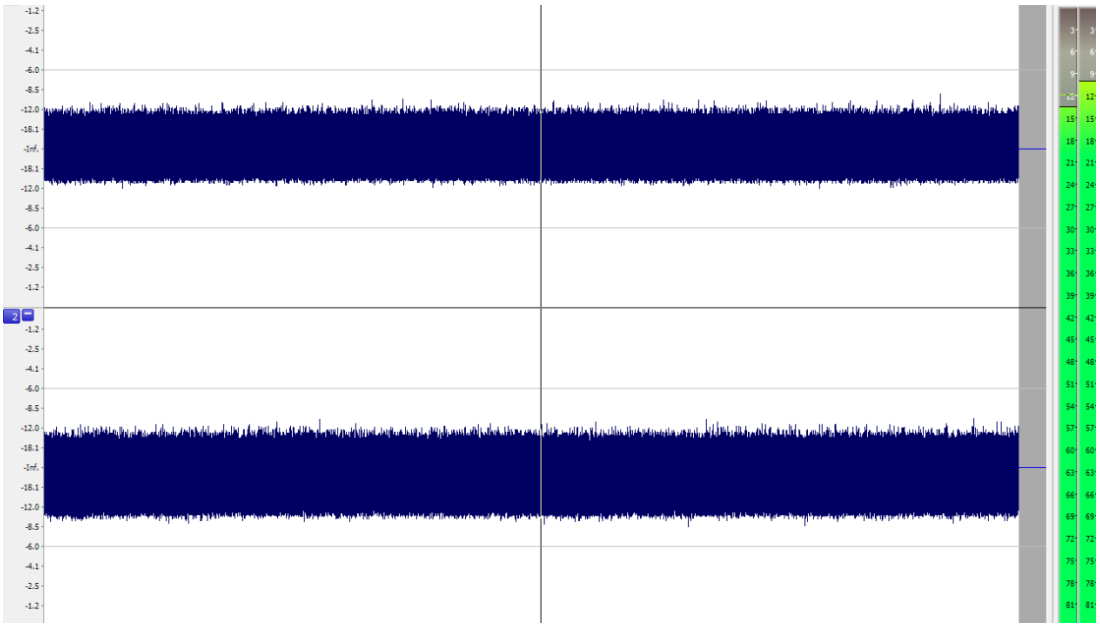
4.3.1 Процес снимања шума из псеудослучајног генератора

Приликом активирања алата за снимње, следе основна подешавања за снимање шума. Тест је вршен на шеснаест бита, на фреквенцији 44.100Hz, у *stereo* режиму.

Као алат за снимање и обраду термичког шума коришћен је програм *Sound Forge*. За снимање термичког шума може да се користи било који други програм такве намене, али због одличних перформанси и карактеристика, за тестирање овог генератора коришћен је управо поменути програм.

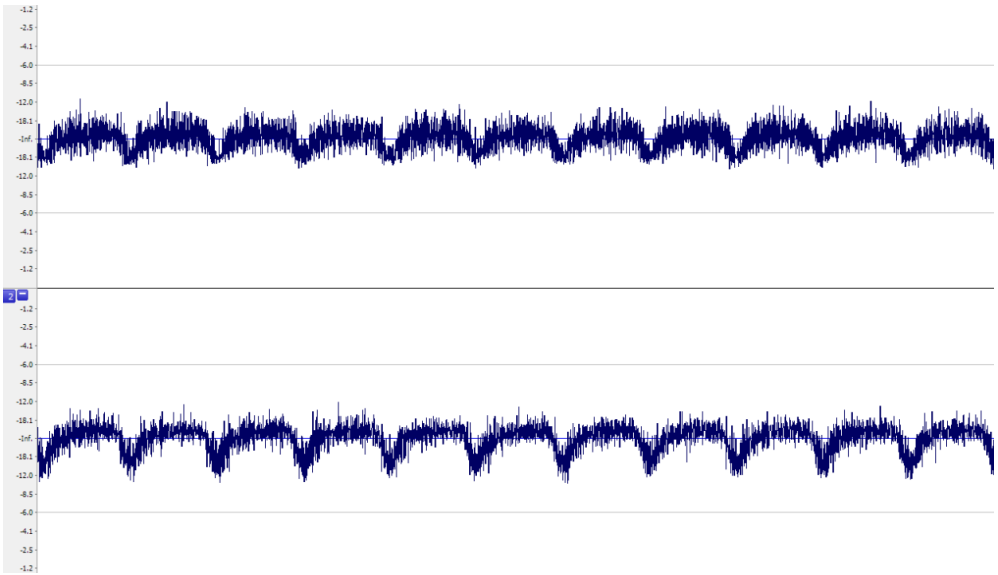
У наставку текста биће приказан начин на који се снима шум, затим, како се добијени аналогни сигнал претвара у дигитални сигнал. Потом, како се добијени шум претвара у хексадецимални низ, односно, у бинарни низ. На крају ће бити описани и приказани сви статистички тестови који су вршени.

На слици 4.12.1 приказан је снимљен шум који је генерисан из псеудослучајног генератора. Снимљен је на поменутој фреквенцији и у *stereo* режиму, на шеснаест бита и у трајању од једног минута.



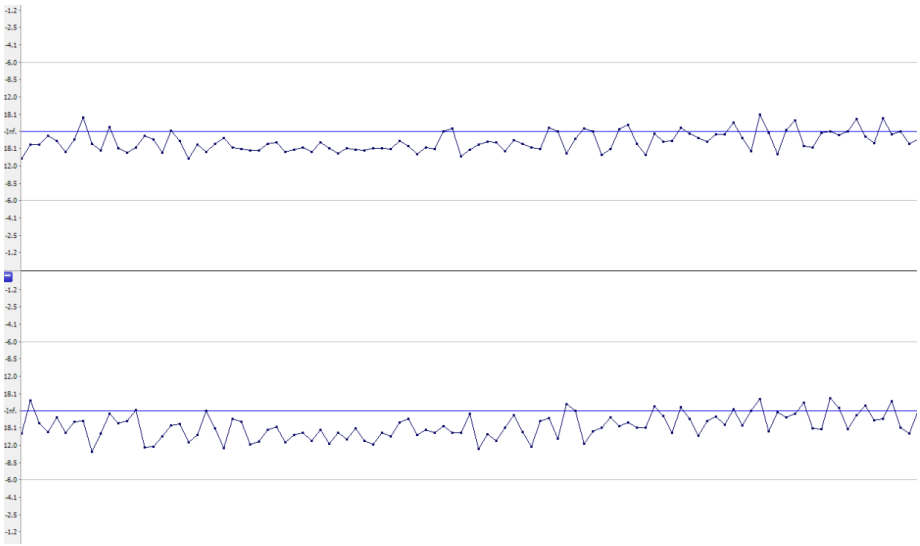
Слика 4.12.1: Снимљен шум из генератора (1)

На слици 4.12.2 може да се види исти снимљени шум, као на слици 4.12.1, али у пропорцији 1:4, на основу које може да се закључи да се добија различити шум, на оба канала. Као што је већ речено, свака грана електричног кола је генератор шума за себе.



Слика 4.12.2: Снимљен шум из генератора (2)

Како би се приказало да два канала нису само на очиглед различита, на слици 4.12.3 у пропорцији 12:1, може да се види колико се добијени два шума у ствари разликују.



Слика 4.12.3: Снимљен шум из генератора (3)

Генерисани шум много зависи и од саме звучне картице. Уколико се шум снима на било ком типу интегрисане звучне картице, јасно је да ће бити више шумова које треба уклонити. За такве ствари је могуће користити и филтере за уклањање вишка шума и програмске операције за уклањање редундансе. Уколико се користи боља звучна картица, јасно је да ће бити мање редундансе, а више чистијег шума који је могуће користити у криптографске сврхе.

Конструисани генератор је тестиран на следећој конфигурацији:

- Процесор: Intel® Core™ i5-2310 CPU @ 2.90GHz - 3.10GHz

- Матична плоча: GIGABYTE Z68XP-UD3P

- Меморија: RAM 4.00 GB DDR3

- Оперативни систем: Windows 7 Ultimate x64

- Звучна картица: Creative X-Fi XtremeMusic

Када је генерисан и снимљен шум, фајл се чува у *.wav* формату. Затим, тај фајл се учитава у радно окружење, у алату *MATLAB*. Пре свега је неопходно да се тај фајл претвори у низ бројева. У овом случају, прво се генерисани *.wav* фајл претвара у хексадецимални низ.

На слици 4.13 може да се види добијени хексадецимални низ. Види се да је добијена вредност матрице 2712150x2, што је веома велика количина података, али у овом добијеном низу постоји редуданса, односно, шум који смета и који мора да се одстрани.

wavdata ×

wavdata <2712150x2 double>

	1	2
1	-0.1961	-0.1655
2	-0.0959	0.0757
3	-0.0989	-0.0930
4	-0.0367	-0.1564
5	-0.0721	-0.0511
6	-0.1486	-0.1611
7	-0.0604	-0.0796
8	0.1018	-0.0755
9	-0.0948	-0.2986
10	-0.1376	-0.1685
11	0.0358	-0.0262
12	-0.1239	-0.0935
13	-0.1535	-0.0744
14	-0.1189	0.0103
15	-0.0355	-0.2687
16	-0.0603	-0.2590
17	-0.1579	-0.1856
18	0.0069	-0.1058
19	-0.0688	-0.0974
20	-0.1956	-0.2298
21	-0.0984	-0.1794

Слика 4.13: Низ бројева

Следеће што је неопходно, то је да се добијени хексадецимални низ претвори у бинарни низ, како би могла да се израчуна ентропију извора информација. Коришћењем операције *bin2dec*, у *MATLAB*-у, претворен је добијени хексадецимални низ у бинарни низ, где је добијена матрица 10848600x16 (Слика 4.14).

wavbinary <10848600x16 double>

	1	2	3	4	5	6	7	8	9
1	1	1	0	0	1	0	0	0	0
2	1	0	1	1	1	1	1	0	0
3	0	1	1	1	0	0	0	0	0
4	1	0	1	1	1	1	0	1	1
5	1	0	1	0	0	0	0	0	0
6	1	0	1	1	1	1	0	1	1
7	0	0	1	0	0	0	0	0	0
8	1	0	1	1	1	1	0	1	0
9	1	0	1	0	0	0	0	0	0
10	1	0	1	1	1	1	0	1	1
11	0	0	1	1	0	0	0	0	0
12	1	0	1	1	1	1	1	0	0

Слика 4.14: Бинарни низ

С обзиром да се вредности интеџера за *.wav* фајл, снимљен на шеснаест бита, на фреквенцији од 44.100Hz крећу од -32768 до 32768, потребно је уклањање редудансе, тј. уклањање вишка информација. Коришћена је примитивна операција *bitand*.

Из слике 4.15 може да се закључи да је добијена бинарна матрица далеко мања у односу на претходну. Претходна матрица била је реда 10848600x16, а нова добијена матрица, у којој је избачена редуданса, износи 2712150x2. Већ може да се каже да је ово велика количина информација, за један минут снимљеног шума.

wavbinary <2712150x2 double>

	1	2
1	1	1
2	1	0
3	0	0
4	1	1
5	0	1
6	0	1
7	0	0
8	1	1
9	0	1
10	0	1
11	0	0
12	1	1
13	0	0
14	0	0
15	0	0
16	1	0
17	0	1
18	0	0

Слика 4.15: Уклоњена редуданса

Следеће што је неопходно, то је да се установи колико износи ентропија извора информација. Ентропијом се утврђује да ли псеудослучајни генератор бројева генерише стварно насумичан низ информација, што је основа за све *PRNG* генераторе.

За добијање статистичке мере ентропије користили смо команду *E = entropy(I)*, што је еквивалентно *-sum(p.*log2(p))*.

Добијена ентропија износи равно један, што даје добру основу за наставак тестирања. На слици 4.16 може да се види добијена ентропија:

```
>> E = entropy(wavbinary)

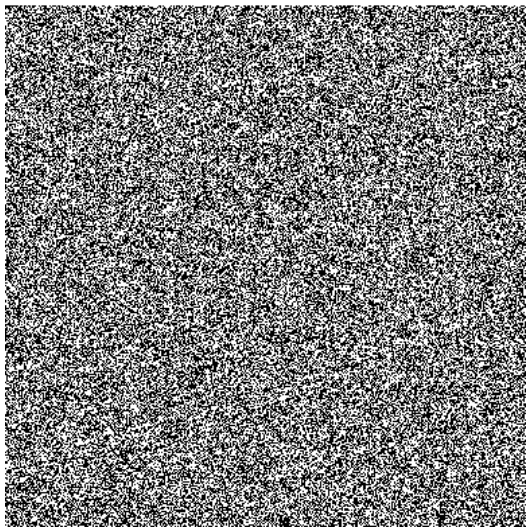
E =

    1.0000

fx >>
```

Слика 4.16: Ентропија бинарног низа

Када је хексадецимални низ претворен у бинарни низ и када је израчуната ентропија извора информација, добијена је стварна дужина низа генерисаног шума и избачена је редуданса из шума. Сада је могуће приказати добијени шум без вишка информација (Слика 4.17).



Слика 4.17: Генерисан шум

У даљем тексту ће бити приказани упоредни тестови који су вршени и добијени резултати.

4.4 Приказ експерименталних резултата

У овом делу ће бити приказани упоредни тестови бинарног низа генерисаног шума са интернет странице *random.org*, са бинарним низом добијеног на основу генерисаног шума са конструисаног псеудослучајног генератора (PRNG).

Испитивање се односи на упоредни тест ентропија извора информација са преклапањем и без преклапања.

Табела 4.1 представља статистички тест ентропије са преклапањем генерисаног бинарног низа.

Ентропија са преклапањем	**Интернет страница: *random.org***
Тип теста	**Резултат**
Ентропија – Монобит:	0.9999999970453606
Ентропија – Биграм:	0.9999938028778617
Ентропија – Триграм:	0.9999776564462013
Ентропија – 4x4 Матрице:	0.9999632491279191

Табела 4.1: Ентропија са преклапањем (random.org)

Табела 4.2 представља тест ентропије са преклапањем бинарног низа, добијеног на основу снимљеног шума из конструисаног *PRNG* генератора.

Ентропија са преклапањем	***PRNG* генератор**
Тип теста	**Резултат**
Ентропија – Монобит:	0.9999999851224279
Ентропија – Биграм:	0.999998712659246
Ентропија – Триграм:	0.9999971314264103
Ентропија – 4x4 Матрице:	0.9999918362253594

Табела 4.2: Ентропија са преклапањем (*PRNG*)

На следећој табели (4.3), приказан је тест ентропије без преклапања, за генерисани шум са интернет адресе *random.org*.

Ентропија без преклапања	**Интернет страница: *random.org***
Тип теста	**Резултат**
Ентропија – Монобит:	0.9999999970453606
Ентропија – Биграм:	0.9999850632203415
Ентропија – Триграм:	0.9999443542760401
Ентропија – 4x4 Матрице:	0.9999632491279191

Табела 4.3: Ентропија без преклапања (*random.org*)

У табели 4.4 је приказ статистичког теста ентропије без преклапања, за генерисани шум са псеудослучајног генератора *PRNG*.

Ентропија без преклапања	***PRNG* генератор**
Тип теста	**Резултат**
Ентропија – Монобит:	0.9999999851224279
Ентропија – Биграм:	0.9999935149038766
Ентропија – Триграм:	0.9999798584606167
Ентропија – 4x4 Матрице:	0.9999918362253594

Табела 4.4: Ентропија без преклапања (PRNG)

Следећи статистички тест је „NIST“-ов серијски тест, где се такође упоређују вредности са интернет адресе „random.org“ псеудослучајног генератора „PRNG“.

Подаци о тесту:

- *NIST* серијски тест,
- Генерисан низ са странице *random.org*, узорак: 62500 битова;

000	7685	**001**	7877
010	7823	**011**	7867
100	7877	**101**	7813
110	7867	**111**	7691

P-Value 1	0.3163829931140636
P-Value 2	0.16154427908405955
P-Value 1 (Децимално)	0.316382993114063593
P-Value 2 (Децимално)	0.161544279084059549

Табела 4.5: Серијски тест (*random.org*)

Подаци о тесту:

- *NIST* серијски тест,

- Низ генерисан из псеудослучајног генератора, узорак: 264600 битова;

000	33289	**001**	32967
010	32936	**011**	33089
100	32968	**101**	33058
110	33090	**111**	33203

P-Value 1	0.6923043172125305
P-Value 2	0.5234603306475408
P-Value 1 (Децимално)	0.692304317212530495
P-Value 2 (Децимално)	0.523460330647540827

Табела 4.6: Серијски тест (*PRNG*)

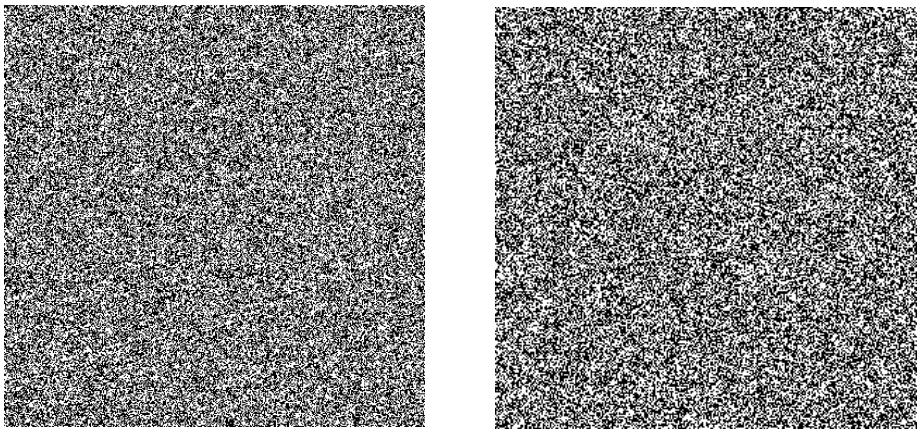
Мауреров универзални статистички тест – испитивање могућности компресије низа без губитка информације. За низ који се може значајно компресовати сматра се да није низ случајних битова због чињенице да је компресија низа ефикаснија уколико низ показује периодична својаства. У следећој табели следе резултати Маурерового статистичког теста, који је препоручен од стране *NIST*-а. Генерисан је шум од шест секунди, на шеснаест бита и на фреввенцији од 44100Hz, како би се добила довољна количину информација за поменути статистички тест. За шест секунди генерисаног шума, добијена је матрица 264600x2 бинарног низа. Следи табеларни приказ урађеног теста:

Мауреров тест	препоручен од стране „NIST“-а
Observed sum	456584.6075373749
Observed fn	5.21453411988779
Expected fn	5.2177052
Varriance	2.954
P-Value	0.9985278848454993
P-Value (Decimal)	0.99852788484549925840383

Табела 4.7: Мауреров тест (PRNG)

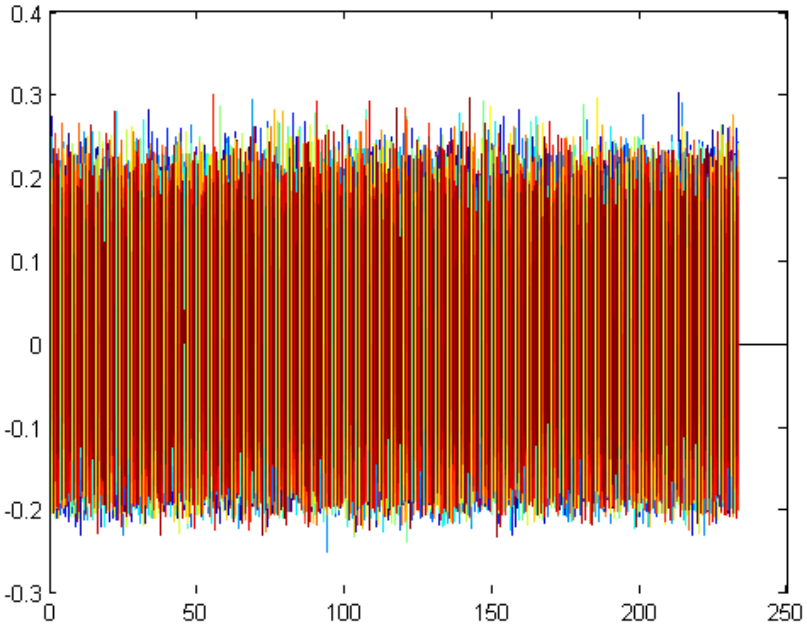
Важно је напоменути да је за овај тест потребно најмање 264600 битова; за генерисан шум од шест секунди „прочитано“ је 529200 битова.

На основу добијене слике 4.17 генерисаног шума, може да се упореди шум, који нам је доступан преко интернет странице *random.org*, са шумом који је генерисан преко псеудослучајног генератора (Слика 4.18).



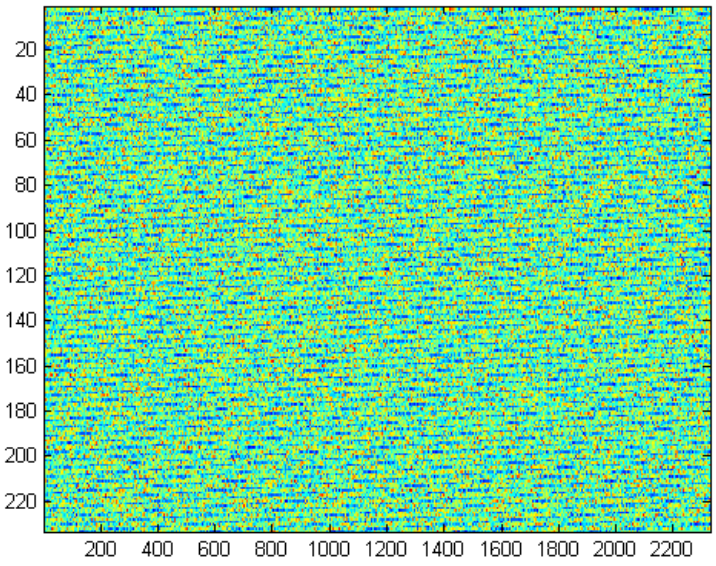
Слика 4.18: Генерисан шум (*PRNG* – лево, *random.org* - десно)

На слици 4.19 може да се види генерисани шум у функцији топлоте:



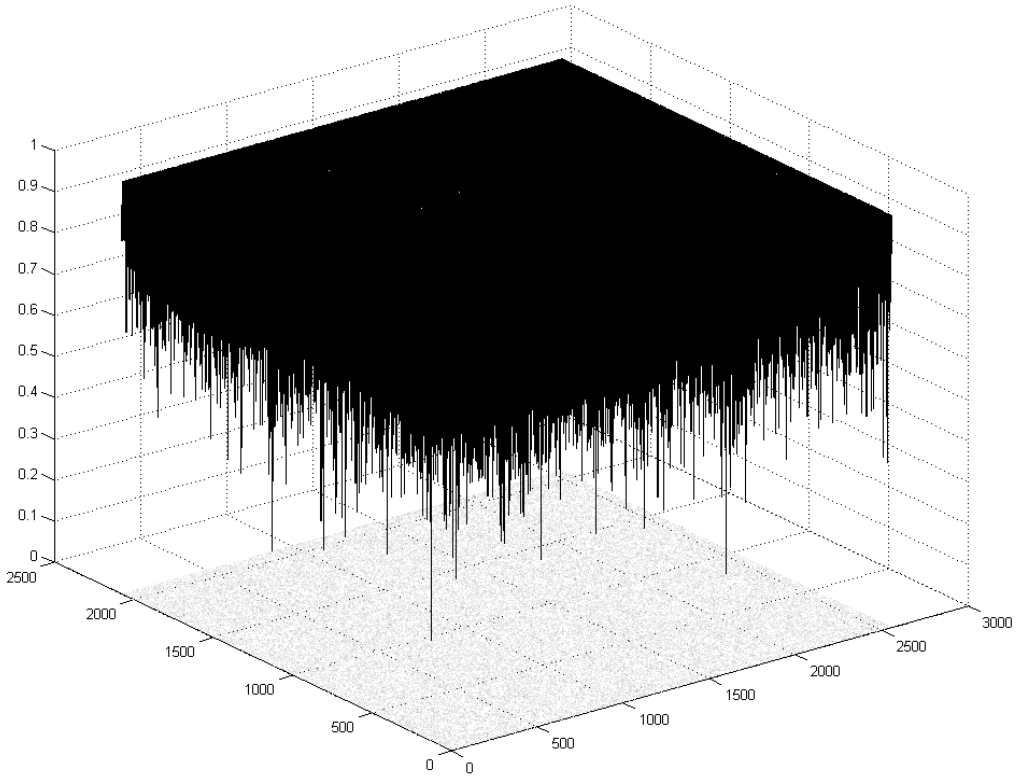
Слика 4.19: Шум у функцији топлоте

На слици 4.20 такође може да се примети насумично генерисани бројеви. То показује велика количина зелене и жуте боје, у односу на плаву боју.



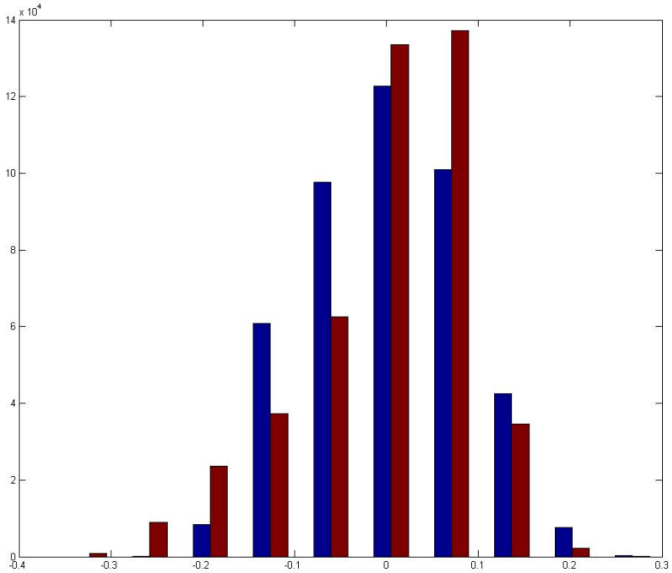
Слика 4.20: Насумични бројеви

На слици 4.21 су приказани насумично генерисани битови:



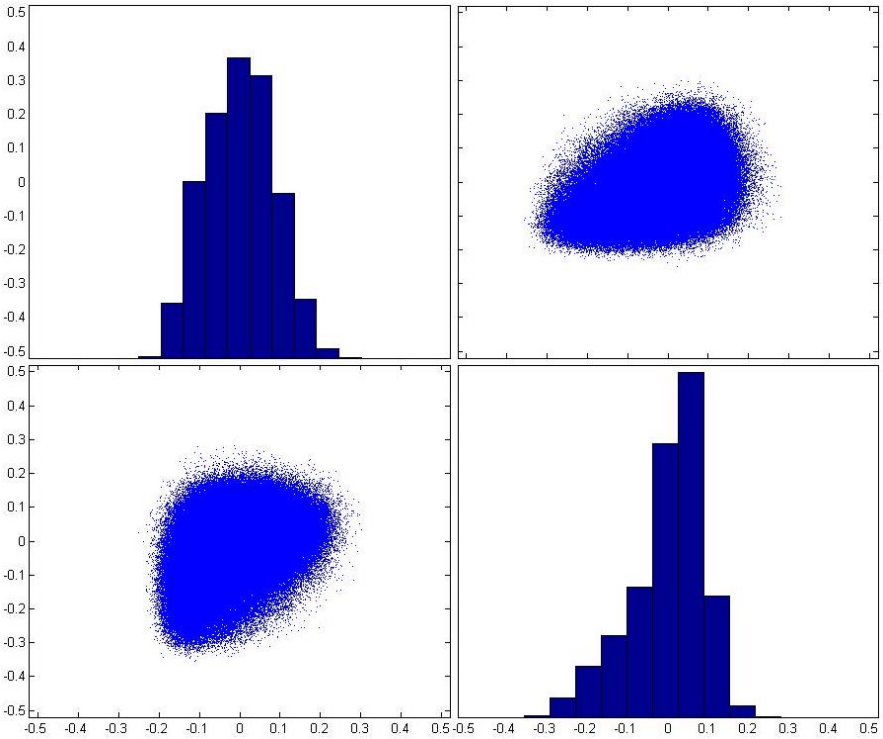
Слика 4.21: Насумични генерисани битови

На слици 4.22 може да се види хистограм случајних бројева, за десети део снимљеног шума:



Слика 4.22: Хистограм генерисаних битова

На слици 4.23 могу да се виде насумично генерисани бројеви, представљени графом *polimatrix*:



Слика 4.23: Хистограм (polimatrix) генерисаних битова

4.5 Област примене предложеног решења

Предлог примене псеудослучајног генератора *PRNG* је маскирање протокола.

Пренос података кроз мрежу обавља се по протоколима – утврђеним правилима која су позната свим учесницима у комуницирању. Протокол представља стандард (конвенцију) за остваривање и контролу везе и пренос података између две крајње тачке. Комуникациони протокол је скуп стандардизованих правила за представљање података, сигнализацију, проверу аутентичности и контролу грешака, неопходних за пренос информација комуникационим каналом. Веома је битна заштита у рачунарским мрежама, где две стране комуницирају. Оно што је најбитније у рачунарској мрежи јесте да две стране имају сигурну комуникацију и да нападач, чак и да пресретне комуникацију између две стране, не може да добије никакву информацију из тих података. Такође, када информација стигне до примаоца, примаоц мора да зна како да из маскиране информације добије поруку.

Овакав псеудослучајни генератор *PRNG* може да се користи у спречавању *replay* напада, који се јављају код протокла аутентикације, затим, могуће је генерисати јавне кључеве, кључеве сесије и др. Такође, један од предлога за коришћење псеудослучајног генератора је за генерисање кључева за *One-Time-Pad* алгоритам.

5 Закључак

5.1 Сумарни циљеви рада

Постигнути циљеви рада су засновани на практичном решењу, на генерисању велике количине термичког шума, односно, буке из псеудослучајног генератора. Идеја овог рада је била да се генерисани шум сними, обради у рачунару, а затим, извршити анализе у какве је сврхе могуће користити овакав генератор.

5.2 Предлог за будући рад

Идеја будућег рада је наставак истраживања и конструисања псеудослучајних генератора. Као предлог за будуће решење је конструисање квантног генератора. То је један од тренутно популарних метода за генерисање велике количине насумичних бројева, поред обраде термичког шума. Начин на који се конструише тај генератор је снимање камером слободног пада течне материје из лава лампе. Тај снимак се, затим, обрађује на рачунару; из добијеног снимка могуће је „извући“ истинито случајне бројеве. Претпоставља се да је то један од бољих јефтиних псеудослучајних генератора бројева јер је до сада прошао многе јаке тестове. Такав генератор је могуће користити у сврху генерисња кључева, прављења јединствених параметара дигиталног потписа, као и у многе друге криптолошке сврхе. Једна од метода која није била овде примењена за тестирање генератора је *Monte Carlo*. За тестирање квантног генератора ће бити коришћена управо та метода, јер се она до сада показала као једна од најпоузданијих и виталних метода за тестирање, не само генератора, већ и многих других ствари. Неки од примера за шта је могуће користити ту методу су процена гужве на метро станици, економија, физика, компјутерска графика, вештачка ингелигенција и многи други.

Команде „MATLAB“ (прилог, део)

>> wav = wavread('naziv_fajla.wav'); %учитавање аудио записа у радно окружење у МАТЛАБ; претварање шума у хексадецимални низ

>> wavbinary = dec2bin(typecast(single(wav(:)), 'uint16'), 16) -'0'; %претварање хексадецималног низа у бинарни низ.

>> wavbinary = bitand(wav*32768+32768,1); %уклањање редудансе из снимљеног шума

>> E = entropy(wavbinary) %израчунавање ентропије извора информација, након уклоњене редудансе

>> wavbinary=reshape(wavbinary, 1, 'величина матрице');

>> wavbinary = wavbinary(1:'величина матрице');

>> wavbinary = vec2mat(wavbinary,'квадратни корен од величине матрице');

>> imshow(wavbinary) %приказ генерисаног шума

>> wav = vec2mat(wav(1:'величина матрице'),'квадратни корен од величине матрице');

>> imagesc(wav);figure(gcf);

...

Литература

[1] Kriptologija I, Mladen Veinović, Saša Adamović, Univerzitet Singidunum

[2] Random Number Generation with a Simple Transistor Junction Noise Source, Version 1 Revision 2. 22 June 2004, David Eather

[3] Jedna realizacija generatora istinskih slučajnih impulsa na bazi zvučne kartice računara, Mladen Veinović, Slaviša Nikolić, Univerzitet Singidunum

[4] Osnovi elektronike za studente Odseka za softversko inženjerstvo, Dr. Miodrag Popović, Elektrotehnički fakultet, Beograd

[5] Generatori pseudoslučajnih brojeva, Milan Milosavljević, Miloš Milenković, Saša Adamović, Univerzitet Singidunum

[6] Generatori slučajnih sekvenci i njihov uticaj na sigurnost, Saša Adamović, Miloš Milenković, Marko Šarac, Dalibor Radovanović, Univerzitet Singidunum

[7] KRIPTOLOGIJA I, Osnove za analizu i sintezu šifafrskih sistema, Mladen Veinović, Saša Adamović

[8] Generation of Pseudorandom Numbers From Microphone Input in Computing Devices, Giles Cotter, The Faculty of the School of Engineering and Applied Science University of Virginia

[9] Uvod u teoriju informacija i kodovanje, D. Drajić, P. Ivaniš, III prošireno izdanje

[10] Pseudorandom Number Generators for Cryptographic Applications, Andrea Röck, Naturwissenschaftliche Fakultät - Universität Salzburg

[11] Рачунарске мреже, Младен Веиновић, Александар Јевремовић

[12] Kanali za prenos informacija, prof. Dr. Milan M. Milosavljević

[13] ClaudeE.Shannon, "CommunicationTheoryofSecrecySystems", BellSystemTechnical Journal,vol.28-4,page656-715, Oct. 1949

[14] Интернет страница: http://www.mathworks.com/help/

[15] Интернет страница: http://www.wikipedia.org/