ДОДАТОК А

Графічний матеріал кваліфікаційної роботи

Харківський національний університет радіоелектроніки
Кафедра ЕОМ

ДОСЛІДЖЕННЯ ГЕНЕРАТОРІВ ВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА МІКРОКОНТРОЛЕРАХ

Кваліфікаційна робота
Другий (магістерський) рівень

Автор:
Пушкар О.О.
студ. гр. СПзм-20-1

Керівник:
Торба А.А.
проф. каф. ЕОМ

Мета, і завдання роботі

- Мета:

  визначення ефективних механізмів поліпшення статистичних параметрів випадкових послідовностей, що генеруються, та підвищення надійності апаратних засобів генерації випадкових послідовностей.

- Завдання:

  аналіз існуючих систем генерації випадкових і псевдо-випадкових послідовностей для криптографічних систем.

Мета, і завдання роботі

- Завдання:

  вибір та обґрунтування джерел ентропії (датчиків шуму, джерел невизначеності),

  розробка апаратної та програмної складової недетермінованих генераторів випадкових послідовностей на елементній базі сучасних мікроконтролерів,

  дослідження генераторів випадкових послідовностей з метою досягнення максимальної швидкості формування випадкових бітових послідовностей.

3

Аналіз існуючих систем генерації випадкових послідовностей для криптографічних систем

- Граничні характеристики стійкості криптографічних систем захисту інформації досягаються у разі, якщо для формування ключів, параметрів і синхромаркерів використовується генератор випадкових послідовностей на основі фізичних датчиків шуму із статистично обґрунтованими параметрами рівноймовірності, незалежності і некорельованості.
- При реалізації державних і комерційних криптографічних систем необхідною умовою являється застосування вітчизняних розробок, що виключають наявність програмних і апаратних "закладок" і, як наслідок, не допускають маніпуляцію або злом систем захисту інформації.

4

Аналіз існуючих систем генерації випадкових послідовностей для криптографічних систем

- Опублікований в 2005-му році Міжнародний стандарт ISO/IEC 18031 : 2005 – Information technology – Security techniques – Random bit generation узагальнює величезний міжнародний досвід практичних і теоретичних досліджень та встановлює спеціальні вимоги, яких необхідно дотримуватися при розробці генераторів випадкових біт, які використовуватимуться для криптографічних застосувань.
- Сучасна елементна база обчислювальних систем на основі мікроконтролерів дозволяє реалізовувати генерацію та тестування випадкових послідовностей на одному кристалі з криптопроцесорами, разом з алгоритмами обмеження доступу до апаратних та програмних засобів.

5

Вибір та обґрунтування джерел ентропії (датчиків шуму, джерел невизначеності)

- Генератор випадкових послідовностей **обов'язково включає** джерело випадковості (чи джерело невизначеності) – фізичний датчик шуму.
- Проектування апаратного пристрою або програми для використання такої випадковості і отримання бітової послідовності, що не має помилок і кореляцій, є важким завданням. Крім того, для більшості криптографічних застосувань, генератор не повинен піддаватися спостереженню або маніпуляції супротивником

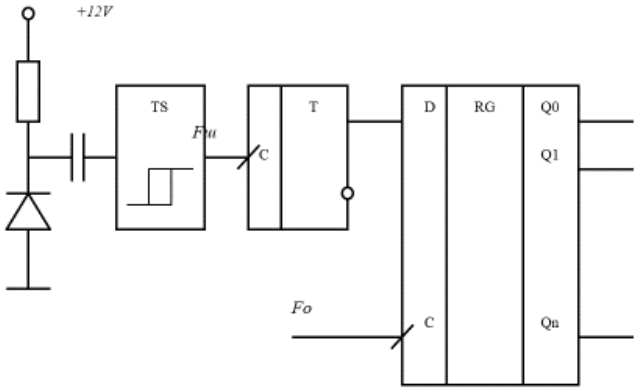
6

Вибір та обґрунтування джерел ентропії (датчиків шуму, джерел невизначеності)

- Серед відомих датчиків шуму: резистори, p-n- перехо-ди, кремнієві діоди із Зенерівським пробоєм (стабілітрони), електронні лампи, газорозрядні лампи, фотоелектронні помножувачі (ФЕП), лічильник Гейгера та інші -
- доцільно застосувати в сучасних обчислювальних системах фізичні датчики шуму на основі кремнієвих діодів із Зенерівським пробоєм.

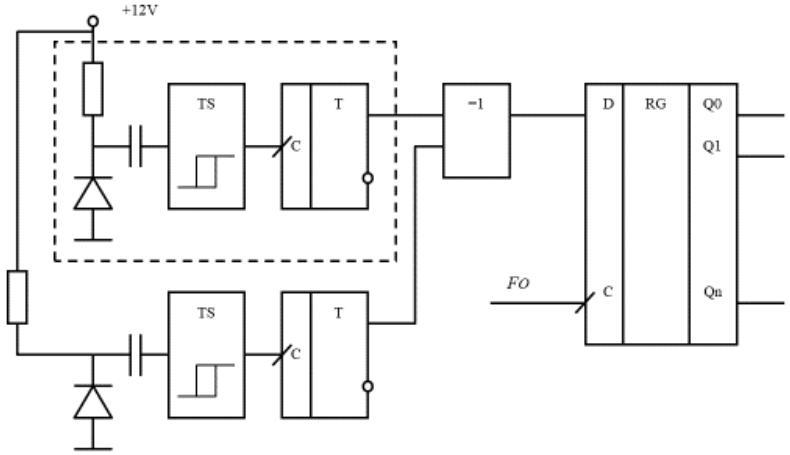
7

Базова модель генератора випадкових послідовностей



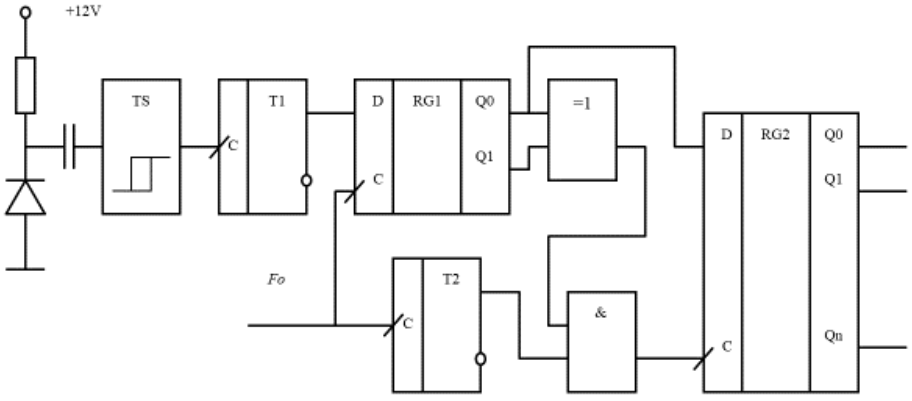
7

Генератор випадкових послідовностей з гарячим резервуванням каналів формування випадкових бітів



8

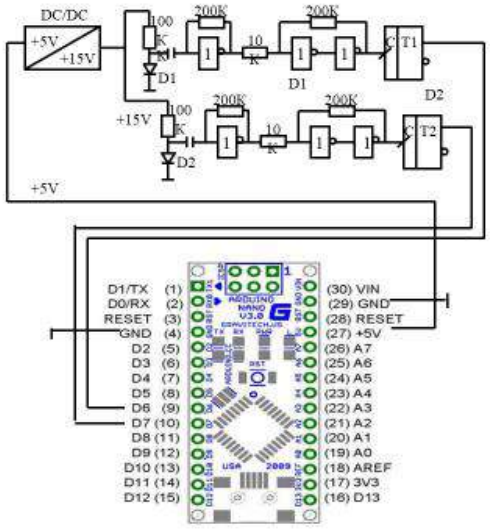
Генератор випадкових послідовностей з повним вирівнюванням імовірностей (за алгоритмом Неймана)



9

Процесорна плата ARDUINO NANO з мікроконтролером ATMega 328P

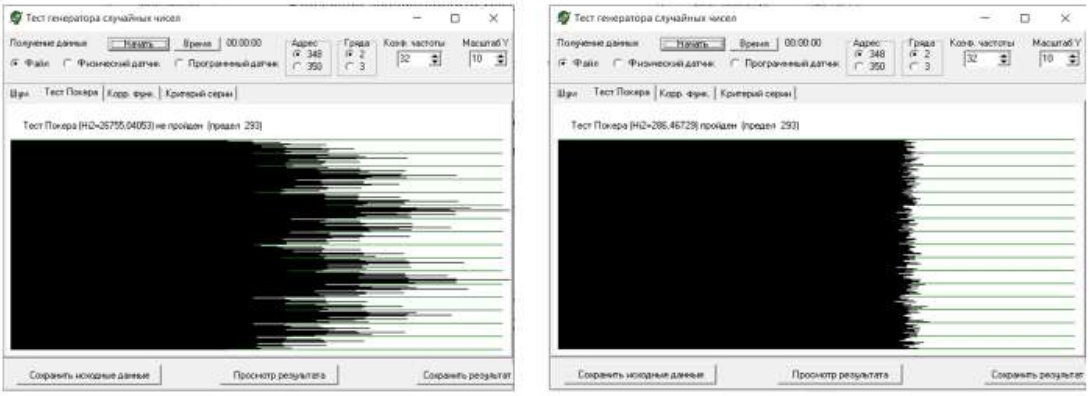
10



Лабораторний макет для дослідження генераторів випадкових послідовностей на основі ARDUINO–NANO

11

Тестування генератора випадкових послідовностей

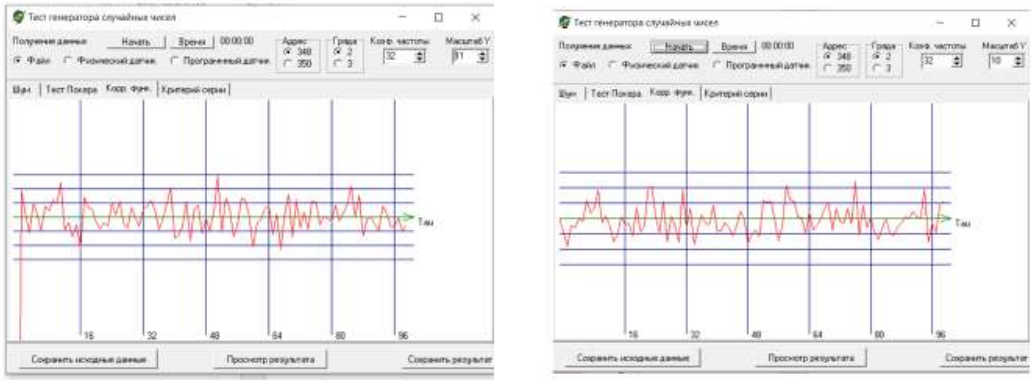


Тест Покера

Не пройдено Пройдено

12

Тестування генератора випадкових послідовностей



Автокореляційний тест

Не пройдено Пройдено

13

Тестування генератора випадкових послідовностей

```
Самая длинная серия  20 бит
Число 0 в последовательности - 4196779   вероятность 0,500295042591638
Число 1 в последовательности - 4191829   вероятность 0,499704957008362
Вероятности 0 или 1 должны быть в пределах от  0,499661684036255
                                            до  0,500338315963745
Монобитный тест по критерию  Hi2=2,920925617210O2  пройден (предел 3.84)
Тест Покера (Hi2=26755,04053) не пройден (предел 293)
Тест серий по критерию  Hi2=34909,5144117611  не пройден (предел 76.55)
```

Тест серій

Не пройдено

```
Самая длинная серия  24 бит
Число 0 в последовательности - 4196226   вероятность 0,500229120254517
Число 1 в последовательности - 4192382   вероятность 0,499770879745483
Вероятности 0 или 1 должны быть в пределах от  0,499661684036255
                                            до  0,500338315963745
Монобитный тест по критерию  Hi2=1,76147651672363  пройден (предел 3.84)
Тест Покера (Hi2=286,46729) пройден (предел 293)
Тест серий по критерию  Hi2=49,4294728671949  пройден (предел 76.55)
```

Пройдено

15

Головні результати теоретичних досліджень

- Проведено аналіз існуючих систем генерації випадкових і псевдовипадкових послідовностей для криптографічних систем, вітчизняних та світових стандартів для побудови недермінованих генераторів випадкових послідовностей.
- Вибрані та обґрунтовані джерела ентропії (датчики шуму, джерела невизначеності) на основі кремнієвих діодів з Зенеровським пробоєм (стабілітронів).
- Проаналізовані методи тестуваннявипадкових послідовностей, що генеруються, на основі вітчизняних та міжнародних алгоритмів і стандартів.

15

Головні результати експериментальних досліджень

- Розроблена апаратна частина генератора випадкових послідовностей на основі мікроконтролера ATMega 328P. Розроблені та досліджені методи поліпшення статистичних параметрів випадкових послідовностей, що генеруються.
- Запропоновано реалізувати генератор випадкових послідовностей у вигляді лабораторного макета на основі апаратного процесорного модуля ARDUINO_NANO.
- Проведені дослідження лабораторного макета генератора випадкових послідовностей з метою визначення фізичних обмежень на максимальну швидкість формування випадкових бітових послідовностей
- Протестовані вихідні випадкові послідовності генератора, запропоновані параметри та коефіцієнти програмної обробки сигналів з метою досягнення максимальної швидкості формування та підвищення надійності генератора.

16