DOI 10.31891/2307-5732-2023-329-6-307-311
УДК 621.396.662

ПЕТРУШАК ВОЛОДИМИР
Хмельницький національний університет
ORCID ID: 0000-0002-7232-1044,
e-mail: petrushak@ukr.net
КАЗІОНОВ НІКІТА
Хмельницький національний університет
0009-0004-0177-3336
e-mail: nkazionov@gmail.com

ОГЛЯД АПАРАТНИХ ЗАСОБІВ ФОРМУВАННЯ ПСЕВДОВИПАДКОВОЇ ПОСЛІДОВНОСТІ

У роботі зазначено важливість прямих цифрових синтезаторів частот для сучасних радіоелектронних пристроїв. Їх переваги включають швидкість переналаштування, високу роздільну здатність та широку смугу частот. Багаторівневі DDS, завдяки своїм технологічним особливостям та унікальним характеристикам, знайшли широке застосування в системах зв'язку, особливо в тих, що вимагають високої надійності та захищеності. Однак, для досягнення максимальної продуктивності й якості спектрального складу таких синтезаторів, швидкість окремих арифметичних операцій у цифровому ядрі є критичним фактором.

Разом з тим у статті розглянуті різні види генераторів на базі яких можна реалізувати виникнення псевдовипадкової послідовності, використовуючи різні методи, сформована оптимізована схема для найкращої реалізації формування псевдовипадкової послідовності на базі методу Фібоначчі, представлено їх характеристики та види формування сигналів, вказано на їх основні переваги і недоліки порівнянно з іншими методами.

Ключові слова: метод Фібоначчі, прямі цифрові синтезатори частоти, методи формування псевдовипадкової послідовності, технічні інформаційні системи.

PETRUSHAK VOLODYMYR KAZIONOV NIKITA
Khmelnytskyi National University

OVERVIEW OF HARDWARE-BASED PSEUDORANDOMNESS GENERATION

At work, the importance of direct digital frequency synthesizers for modern radio-electronic devices is emphasized. Their advantages include rapid reconfiguration, high resolution, and broad frequency bandwidth. Multilevel DDS, due to their technological features and unique characteristics, have found wide application in communication systems, especially those requiring high reliability and security. However, to achieve maximum productivity and quality of the spectral composition of such synthesizers, the speed of individual arithmetic operations in the digital core is a critical factor.

The article discusses various types of generators that can be used to create a pseudo-random sequence, employing different methods. An optimized scheme for the best implementation of generating pseudo-random sequences based on the Fibonacci method is presented. It includes characteristics, types of signal formation, as well as their main advantages and disadvantages compared to other methods.

Random numbers are widely used in cryptography and security applications. If their generation process is weak, it can undermine the entire security framework: such vulnerabilities can be exploited by attackers to gain information and even compromise the most robust encryption implementations. Random number generators are usually tailored to specific silicon technology and are challenging to scale on programmable hardware without losing entropy. On the other hand, programmable devices and systems on a chip have gained extensive use, including critical security applications where high-quality random number generation is essential.

The presented article describes an overview of random number generators applicable in cryptographic algorithms such as the Vernam method and implemented on programmable logic integrated circuits (PLICs).

Keywords: Fibonacci method, direct digital frequency synthesizers, methods of generating pseudo-random sequences, technical information systems.

Вступ та постановка проблеми

Випадкові числа широко використовуються в криптографії та застосунках безпеки. Якщо процес їх генерації є слабким, це може підірвати все коло безпеки: такі вразливості можуть бути використані зловмисником для отримання інформації та навіть зламати найбільш надійну реалізацію шифру. Генератори випадкових чисел зазвичай налаштовані на конкретну кремнієву технологію і складно масштабуються на програмованому обладнанні без втрати ентропії. З іншого боку, програмовані пристрої та програмовані системи на кристалі здобувають широке використання, включаючи й застосування у критичних заходах безпеки, де необхідно високоякісне генерування випадкових чисел. Представлена стаття описує огляд генераторів випадкових чисел, які можуть бути використанні в таких криптографічних алгоритмах, як метод Вернама[1] і реалізовані на програмованих логічних інтегральних схемах(ПЛІС).

Аналіз останніх джерел

Апаратні засоби формування псевдовипадкової послідовності представляють собою ключовий елемент у сучасних технологіях кібербезпеки та цифрових систем. Вони забезпечують надійність та непередбачуваність випадкових даних, що має важливе значення для безпеки інформації та захисту систем від небажаних втручань. У цій статті ми розглянемо роль та переваги апаратних засобів формування псевдовипадкової послідовності, їхнє застосування в сучасних технологіях, а також виклики та можливості, пов'язані з їхнім вдосконаленням. Розглянемо детальніше, як ці засоби впливають на безпеку та функціональність цифрових систем у сьогоденній інформаційній ері. Псевдовипадкова послідовність

виявляється критичною у сфері кібербезпеки та в сучасних технологіях, оскільки вона утворює основу безпеки багатьох систем. У цьому контексті, апаратні засоби формування псевдовипадкової послідовність є невід'ємною складовою, забезпечуючи випадковість у числових послідовностях, які використовуються для шифрування, аутентифікації та інших аспектів кібербезпеки. Важливість апаратних рішень у цьому контексті полягає у їхній здатності генерувати високоякісні випадкові дані на основі фізичних процесів, що дозволяє створювати непередбачувані послідовності чисел, надійно захищаючи цифрові системи від зловмисників та несанкціонованого доступу. Такі апаратні засоби забезпечують величезний потенціал у розвитку безпечних систем, але одночасно існують виклики у плані ефективності, надійності та енергоефективності, які потребують постійного вдосконалення та досліджень у цій області.

Мета даної роботи полягає в проведенні комплексного огляду апаратних засобів формування псевдовипадкової послідовності. Основні завдання включають аналіз сучасних технологій та методів, використовуваних для створення випадкових числових послідовностей у цифрових системах. Робота спрямована на вивчення ролі та важливості апаратних засобів псевдовипадкової послідовності в контексті кібербезпеки та функціонування різноманітних цифрових систем. Додатково, метою є оцінка переваг, викликів та можливостей, пов'язаних із застосуванням таких засобів у сучасних технологіях, зокрема в областях криптографії, систем зв’язку та безпеки даних. Ця робота спрямована на систематизацію інформації про апаратні рішення формування псевдовипадкової послідовності, їхні технологічні особливості та потенційні обмеження. Головна мета полягає в створенні повного та обґрунтованого огляду цих засобів для вивчення їхнього впливу на безпеку та ефективність сучасних цифрових систем.

Теоретичний матеріал

Для того дослідження було розглянуто 3 види генераторів псевдовипадкової послідовності(ГПВП) на базі яких можна побудувати найбільш оптимізований варіант використання.

1. Генератор формування М-послідовностей[2]

М-генератор псевдовипадкової послідовності (М-генератор) - це цифровий генератор псевдовипадкової послідовності, який використовує лінійну рекурентну формулу для генерування послідовності бітів. М-генератори(рис.1) були розроблені в 1950-х роках і є одними з найпоширеніших типів генераторів псевдовипадкових послідовностей.

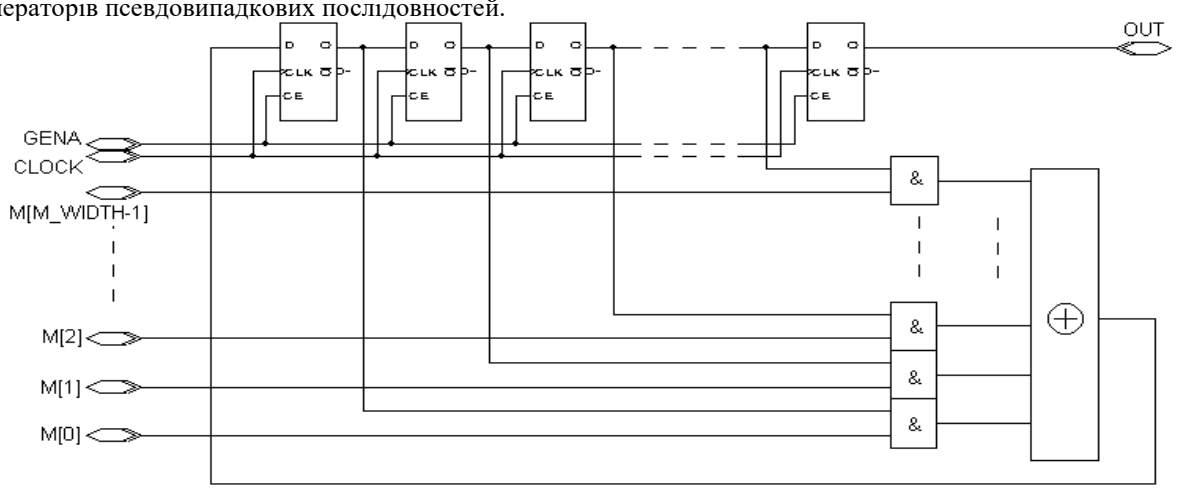

Рис.1 Функціональна схема генератора М-послідовності.

М-генератори мають ряд переваг, включаючи:

Простота реалізації: М-генератори відносно прості у реалізації, що робить їх популярними для застосування в цифрових системах.

Висока швидкість генерування: М-генератори можуть генерувати псевдовипадкові послідовності з високою швидкістю.

Добре вивчені: М-генератори добре вивчені, і їх властивості добре розуміються.

Недоліки М-генераторів

М-генератори також мають деякі недоліки, включаючи:

Недостатня ентропія: М-генератори можуть мати недостатню ентропію для деяких застосувань.

Відкритість: М-генератори можуть бути відкритими для атак, таких як атака методом грубої сили.

Лінійне рекурентне рівняння для М-генератора має наступний вигляд[2]:

$$x_n = \left(a * x\left(n-1\right)+c\right)\%n \tag{1}$$

де:

x_n - наступний біт послідовності

x_(n-1) - попередній біт послідовності

a - коефіцієнт лінійного рекурентної рівняння

c - константа лінійного рекурентної рівняння

m - модуль лінійного рекурентної рівняння

Вихідний фільтр для М-генератора може мати наступний вигляд[2]:

$$y_n = f\left(x_n\right) \tag{2}$$

де:

y_n - вихідний біт послідовності

f - функція вихідного фільтра

2. Генератор формування псевдовипадкової послідовності з використанням методу Фібоначчі[2] представлено на рис.2.

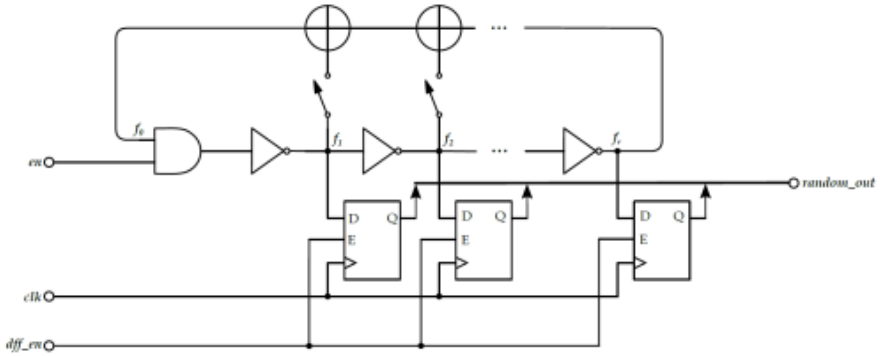

Рис.2 Функціональна схема генератора псевдовипадкової послідовності на основі методу Фібоначчі.

Генератор формування псевдовипадкової послідовності з використанням методу Фібоначчі - це тип генератора псевдовипадкової послідовності, який використовує послідовність чисел Фібоначчі для генерування послідовності бітів. Генератори Фібоначчі були розроблені в 1960-х роках і є одними з найпоширеніших типів генераторів псевдовипадкових послідовностей.

Послідовність Фібоначчі:

Це послідовність чисел, яка визначається наступним рівнянням[2]:

$$f_n = f\left(n-1\right) + f\left(n-2\right) \tag{3}$$

де:

f_n - n-й член послідовності Фібоначчі

f_{n-1} - (n-1)-й член послідовності Фібоначчі

f_{n-2} - (n-2)-й член послідовності Фібоначчі

Вихідний фільтр: Цей фільтр обробляє вихід послідовності Фібоначчі для видалення будь-яких нелінійних залежностей, які можуть бути присутніми.

Переваги генераторів Фібоначчі:

Генератори Фібоначчі мають ряд переваг, включаючи:

1.Висока ентропія: Генератори Фібоначчі мають високу ентропію, що робить їх придатними для використання в таких застосуваннях, як криптографія.

2.Добре вивчені: Генератори Фібоначчі добре вивчені, і їх властивості добре розуміються.

Недоліки генераторів Фібоначчі

Генератори Фібоначчі також мають деякі недоліки, включаючи:

1.Висока складність реалізації: Генератори Фібоначчі можуть бути складними у реалізації, особливо в апаратному виконанні.

2.Відкритість: Генератори Фібоначчі можуть бути відкритими для атак, таких як атака методом грубої сили.

3.Генератор формування псевдовипадкової послідовності з використанням методу Галлуа[3], представлено на рис.3.

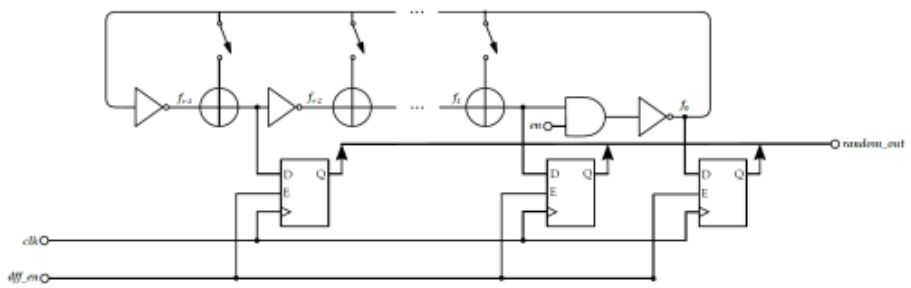

Рис.3 Функціональна схема генератора псевдовипадкової послідовності на основі методу Галлуа.

Генератор формування псевдовипадкової послідовності з використанням методу Галлуа - це алгоритм, який використовує алгебру Галлуа для генерування псевдовипадкової послідовності. Алгоритм працює, використовуючи поле Галлуа, яке є алгебраїчною структурою, що складається з елементів, які не обов'язково є цілими числами.

Переваги

Генератор формування псевдовипадкової послідовності з використанням методу Галлуа має ряд переваг, включаючи:

-Висока ентропія: Послідовності, генеровані методом Галлуа, є високоентропійними, що означає, що вони мають мало кореляцій між сусідніми елементами. Це робить їх придатними для використання в таких додатках, як шифрування, де важливо мати послідовність з високою ентропією.

-Стабільність: Алгоритм є стабільним, що означає, що він генерує послідовності з низьким рівнем кореляцій. Це робить його придатним для використання в таких додатках, як шифрування, де важливо мати послідовність з низьким рівнем кореляцій.

Безпека: Алгоритм є безпечним, що означає, що він важко піддається атакам. Це робить його придатним для використання в таких додатках, як шифрування, де важливо мати безпеку.

Недоліки

- Генератор формування псевдовипадкової послідовності з використанням методу Галлуа також має деякі недоліки, включаючи:

-Складність реалізації: Алгоритм може бути складним у реалізації, що може ускладнити його використання в деяких системах.

-Висока вартість: Алгоритм може бути дорогим у реалізації, що може ускладнити його використання в деяких системах.

Формула для генератора формування псевдовипадкової послідовності з використанням методу Галлуа має наступний вигляд[3]:

$$x_n = f(x(n-1), x(n-2), \ldots, x(n-k)) \quad (4)$$

де:

x_n - наступний елемент в послідовності

x_(n-1) - попередній елемент в послідовності

x_(n-2) - передпопередній елемент в послідовності

x_(n-k) - елемент, який знаходиться k кроків назад в послідовності

f - функція, яка визначає, як генерується наступний елемент в послідовності.

Як варіант для формування псевдовипадкової послідовності може бути удосконалено схему генератора на основі DDS[4], шляхом застосування в колі зворотного зв’язку регістра Фібоначчі[4], що представлена на рис.4.

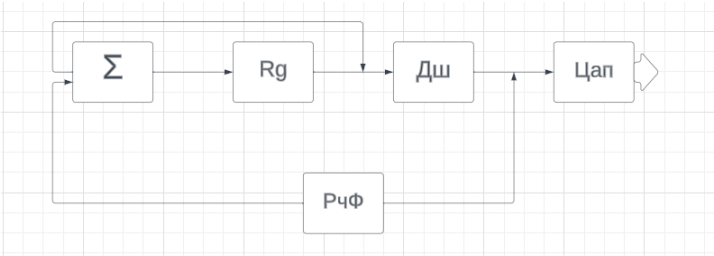

Рис.4 Оптимізована Функціональна схема генератора псевдовипадкової послідовності на основі методу Фібоначчі.

Переваги генератора формування псевдовипадкової послідовності з використанням методу Фібоначчі:

Висока ентропія: Послідовність чисел Фібоначчі має мало кореляцій між сусідніми числами.

Простота реалізації: Алгоритм простий у реалізації.

Недоліки генератора формування псевдовипадкової послідовності з використанням методу Фібоначчі:

Нестійкість: Алгоритм може генерувати послідовності з кореляціями.

Відкритість: Алгоритм може бути відкритим для атак.

Загалом, генератор формування псевдовипадкової послідовності з використанням методу Фібоначчі є простим і ефективним алгоритмом, який може бути використаний для генерування псевдовипадкових послідовностей з високою ентропією. Однак алгоритм може бути нестійким і відкритим для атак.

Висновки

У цій статті було проаналізовано відомі методи формування псевдовипадкової послідовності сигналів, сформовано їх характеристики, вказані їх переваги і недоліки порівнянно до інших. На базі представлених методів і їх детального аналізу була представлена універсальна оптимізована схема генератора формування псевдовипадкової послідовності з використанням методу Фібоначі. Порівнянно до інших методів формування псевдовипадкової послідовності представлена схема надає ряд переваг та простоту реалізації, що в майбутньому для реалізації певних проєктів для яких буде потрібен саме такий метод формування псевдовипадкової послідовності, розроблена схема буде більш легкою для розробки і

буде мати ряд переваг порівнняно з іншими методами.

Література

1. Pelzl J. C.P. Understanding Cryptography / Jan Pelzl. – Berlin: Heidelberg, 2011. – 245 с. – (2011Daniel Guijo.). – (Springer; вип. 3).

2. Sensor-based random number generator seeding – Hon-kong: IEEE Access, 2015. – 144 с. – (Liu). – (3; 3).

3. Rostami, M. A Primer on Hardware Security: Models, Methods, and Metrics / Rostami, M, Koushanfar F, Karri R.A. – berlin: Heidelberg, 2015. – 301 с

4. Baldanzi, L.; Crocetti, L.; Falaschi, F.; Bertolucci, M.; Belli, J.; Fanucci, L.; Saponara, S. Cryptographically secure pseudo-random number generator IP-core based on SHA2 algorithm / Baldanzi, L.; Crocetti, L.; Falaschi, F.; Bertolucci, M.; Belli, J.; Fanucci, L.; Saponara, S., 2020. – 1049 с. – (20).

References

1. Pelzl J.C.P. Understanding Cryptography / Jan Pelzl. - Berlin: Heidelberg, 2011. - 245 p. – (2011Daniel Guijo.). – (Springer; 3rd ed.).

2. Sensor-based random number generator seeding - Hong Kong: IEEE Access, 2015. - 144 p. - (Liu). – (3; 3).

3. Rostami, M. A Primer on Hardware Security: Models, Methods, and Metrics / Rostami, M, Koushanfar F, Karri R.A. - berlin: Heidelberg, 2015. - 301 p

4. Baldanzi, L.; Crocetti, L.; Falaschi, F.; Bertolucci, M.; Belli, J.; Fanucci, L.; Saponara, S. Cryptographically secure pseudo-random number generator IP-core based on SHA2 algorithm / Baldanzi, L.; Crocetti, L.; Falaschi, F.; Bertolucci, M.; Belli, J.; Fanucci, L.; Saponara, S., 2020. - 1049 p. – (20).