



УКРАЇНА

(19) **UA** (11) **108586** (13) **C2**
(51) МПК
G06F 7/58 (2006.01)
H04L 9/20 (2006.01)

ДЕРЖАВНА СЛУЖБА
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА ВИНАХІД

(21) Номер заявки: а 2014 06408	(72) Винахідник(и): Максимович Володимир Миколайович (UA), Мандрона Марія Миколаївна (UA), Гарасимчук Олег Ігорович (UA), Костів Юрій Михайлович (UA)
(22) Дата подання заявки: 10.06.2014	(73) Власник(и): НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ "ЛЬВІВСЬКА ПОЛІТЕХНІКА", вул. Ст. Бандери, 12, м. Львів, 79013 (UA)
(24) Дата, з якої є чинними права на винахід: 12.05.2015	(56) Перелік документів, взятих до уваги експертизою: Іванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях: Учебное пособие / Иванов М.А.(под ред.), Чугунков И.В. – М.: НИЯУ МИФИ, 2012. – С. 258-261. Дослідження генераторів псевдовипадкових послідовностей побудованих з використанням R-блоків/ Мандора М.М., Максимович В.М., Рибак Ю.Ю., Костів Ю.М., Гарасимчук О.І. Інформаційна безпека : наук. журн. / Східноукр. нац. ун-т ім.Володимира Даля. – Луганськ: 4 (12). – 2013. – С. 84-92. UA 86401 C2, 27.04.2009 SU 1493995 A1, 15.07.1989 SU 1406585 A1, 30.06.1988 US 2013230172 A1, 05.09.2013 EP 0545183 A1, 09.06.1993
(41) Публікація відомостей про заявку: 10.11.2014, Бюл.№ 21	
(46) Публікація відомостей про видачу патенту: 12.05.2015, Бюл.№ 9	

(54) АДТИВНИЙ ГЕНЕРАТОР ФІБОНАЧЧІ ІЗ ЗАПІЗНЕННЯМ**(57) Реферат:**

Аддитивний генератор Фібоначчі із запізненням належить до систем захисту інформації, а також в інших системах для імітації і моделювання випадкових процесів з високими статистичними характеристиками. Аддитивний генератор Фібоначчі із запізненням містить комбінаційний суматор та $q+1$ регістрів пам'яті, тактові входи яких підключені до тактового входу пристрою, інформаційні входи кожного наступного регістра пам'яті з'єднані з виходами попереднього регістра пам'яті, виходи r -го регістра пам'яті підключені до першої групи входів комбінаційного суматора, друга група входів якого з'єднана з виходами q -го регістра пам'яті, а виходи комбінаційного суматора підключені до інформаційних входів 0 -го регістра пам'яті. Додатково містить логічну схему, інформаційні входи якої з'єднані з виходами 0 -го регістра пам'яті і виходами пристрою, керуючі входи підключені до керуючих входів пристрою, а її вихід з'єднаний з входом переносу комбінаційного суматора. В аддитивному генераторі Фібоначчі із запізненням за рахунок введення нових конструктивних елементів та зв'язків забезпечується збільшення періоду повторення вихідних псевдовипадкових послідовностей чисел і бітів та

UA 108586 C2

покращуються їх статистичні характеристики, що значно покращує характеристики систем захисту інформації і інших систем, в яких використовується запропонований пристрій.

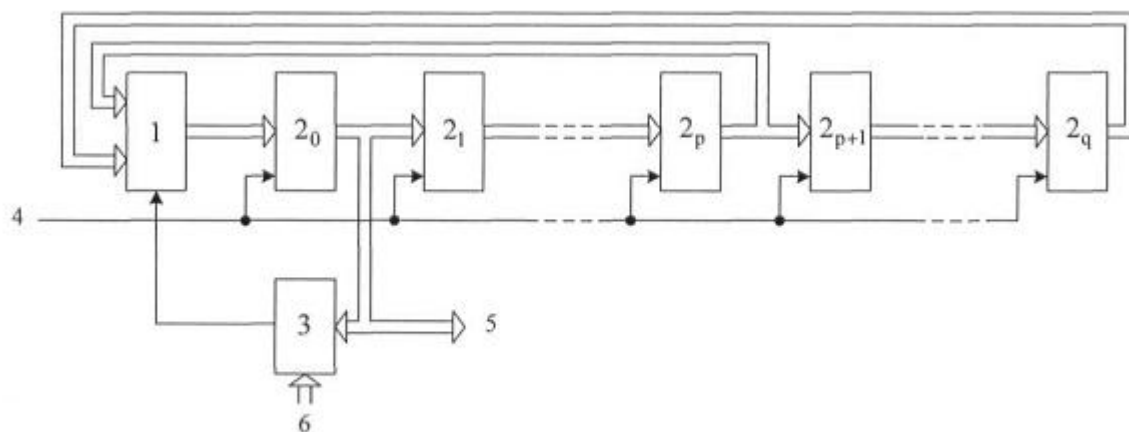


Fig. 1

Винахід належить до галузі приладобудування, генерування послідовностей псевдовипадкових чисел і псевдовипадкових бітових послідовностей. Генератор може бути використаний в системах захисту інформації, а також в інших системах для імітації і моделювання випадкових процесів з високими статистичними характеристиками.

Відомий адитивний генератор Фібоначчі із запізненням [Іванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях: Учебное пособие / Под ред. М.А. Иванова. М.: НИЯУ МИФИ, 2012. - 400 с: ил., ст. 261], який містить комбінаційний суматор і регістри пам'яті $q+1$, тактові входи яких підключені до тактового входу пристрою, інформаційні входи кожного наступного регістра пам'яті з'єднані з виходами попереднього регістра пам'яті, виходи p -го регістра пам'яті підключені до першої групи входів комбінаційного суматора, друга група входів якого з'єднана з виходами q -го регістра пам'яті, а виходи комбінаційного суматора підключені до інформаційних входів 0-го регістра пам'яті.

Але виходи комбінаційного суматора є виходами пристрою, а вхід переносу комбінаційного суматора є незадіяним, що істотно зменшує період повторення вихідних псевдовипадкових послідовностей чисел і бітів і погіршує їх статистичні характеристики. Це пояснюється тим, що процес додавання молодших розрядів чисел в комбінаційному суматорі і послідовний зсув чисел в регістрах пам'яті спричиняє явище "зациклювання", яке розповсюджується і на усі старші розряди чисел, оскільки на цей процес не впливають ніякі інші сигнали.

В основу винаходу поставлено задачу створення адитивного генератора Фібоначчі із запізненням, в якому введення нових конструктивних елементів та зв'язків забезпечувало б збільшення періоду повторення вихідних псевдовипадкових послідовностей чисел і бітів і покращення їх статистичних характеристик.

Поставлена задача вирішується тим, що адитивний генератор Фібоначчі із запізненням, який містить комбінаційний суматор і регістри пам'яті $q+1$, тактові входи яких підключені до тактового входу пристрою, інформаційні входи кожного наступного регістра пам'яті з'єднані з виходами попереднього регістра пам'яті, виходи p -го регістра пам'яті підключені до першої групи входів комбінаційного суматора, друга група входів якого з'єднана з виходами q -го регістра пам'яті, а виходи комбінаційного суматора підключені до інформаційних входів 0-го регістра пам'яті, згідно з винаходом, він додатково містить логічну схему, інформаційні входи якої з'єднані з виходами 0-го регістра пам'яті і виходами пристрою, керуючі входи підключені до керуючих входів пристрою, а її вихід з'єднаний з входом переносу комбінаційного суматора.

Це дає змогу ввести додаткову складову в процес додавання чисел, що зберігаються в регістрах пам'яті, змінити за рахунок цього алгоритм обчислення і, з використанням незначного додаткового обладнання, істотно збільшити період повторення псевдовипадкових послідовностей вихідних чисел і бітів генератора і покращити їх статистичні характеристики, що значно покращує характеристики систем захисту інформації і інших систем, в яких використовується запропонований пристрій.

На Фіг. 1 представлена блок-схема адитивного генератора Фібоначчі із запізненням, де 1 - комбінаційний суматор, $2_0, 2_1, \dots, 2_p, 2_{p+1}, \dots, 2_q$ - регістри пам'яті, 3 - логічна схема, 4 - тактовий вхід пристрою, 5 - виходи пристрою, 6 - керуючі входи пристрою.

На Фіг. 2 наведений приклад реалізації логічної схеми 3, де $7_0, 7_1, \dots, 7_{m-3}, 7_{m-2}$ - суматори за модулем два; $8_0, 8_1, \dots, 8_{m-2}, 8_{m-1}$ - елементи логічного множення.

На Фіг. 3 наведені результати імітаційного моделювання запропонованого пристрою і пристрою прототипу: на Фіг. 3а - результати тестування пристрою-прототипу, а на Фіг. 3б - запропонованого пристрою.

Адитивний генератор Фібоначчі із запізненням складається з комбінаційного суматора 1, логічної схеми 3 і регістрів пам'яті $2_0, 2_1, \dots, 2_p, 2_{p+1}, \dots, 2_q$, тактові входи яких підключені до тактового входу 4 пристрою, інформаційні входи кожного наступного регістра пам'яті 2 з'єднані з виходами попереднього регістра пам'яті, виходи регістра пам'яті 2_p підключені до першої групи входів комбінаційного суматора 1, друга група входів якого з'єднана з виходами регістра пам'яті 2_q , а виходи комбінаційного суматора 1 підключені до інформаційних входів регістра пам'яті 2_0 . Інформаційні входи логічної схеми 3 з'єднані з виходами регістра пам'яті 2_0 і виходами пристрою 5, керуючі входи підключені до керуючих входів 6 пристрою, а її вихід з'єднаний з входом переносу комбінаційного суматора 1.

Логічна схема 3 складається з суматорів за модулем два $7_0, 7_1, \dots, 7_{m-3}, 7_{m-2}$ і елементів логічного множення $8_0, 8_1, \dots, 8_{m-2}, 8_{m-1}$, перші входи яких підключені до інформаційних входів 5 логічної схеми 3, другі входи з'єднані з керуючими входами 6 логічної схеми 3, виходи елементів логічного множення $8_0, 8_1, \dots, 8_{m-2}$ підключені до перших входів суматорів за модулем два $7_0, 7_1, \dots, 7_{m-3}, 7_{m-2}$, другі входи кожного наступного суматора за модулем два $7_0, 7_1, \dots, 7_{m-3}$ з'єднані з виходами попереднього суматора за модулем два $7_1, \dots, 7_{m-3}, 7_{m-2}$ відповідно, другий вхід суматора

за модулем два 7_{m-2} підключений до виходу елемента логічного множення 8_{m-1} , а вихід суматора за модулем два 7_0 з'єднаний з входом логічної схеми 3.

Адитивний генератор Фібоначчі із запізненням працює таким чином. З кожним тактовим імпульсом в регістрах $2_0, 2_1, \dots, 2_p, 2_{p+1}, \dots, 2_q$ формуються нові значення чисел. В регістрі 2_0 число, що визначається вихідним сигналом комбінаційного суматора 1, а в регістрах 2_i ($i=1, 2, \dots, q$) числа, що визначаються вихідними сигналами в регістрах 2_{i-1} .

На виході логічної схеми 3 формується сигнал у відповідності до логічного рівняння:

$$a = b_0 \oplus b_1 \oplus \dots \oplus b_s, \quad (1)$$

де b_k ($k=0, 1, \dots, s$) значення двійкових розрядів числа в регістрі 2_0 , а s може приймати значення від 0 до $m-1$, де m кількість двійкових розрядів кожного з регістрів $2_0, 2_1, \dots, 2_p, 2_{p+1}, \dots, 2_q$. Таким чином, в роботі логічної схеми 3, може бути задіяна будь-яка задана кількість двійкових розрядів регістра 2_0 , що визначається значенням коду c_0, \dots, c_{m-1} на керуючих входах 6 пристрою. Наприклад, якщо на керуючі входи 6 подані значення керуючого коду $c_0=1, c_1=c_2=\dots=c_{m-1}=0$ - на виході логічної схеми 3 буде сформований логічний сигнал у відповідності до рівняння $a=b_0$. При наявності на керуючих входах логічної схеми 3 значень $c_0=1, c_1=1, c_2=\dots=c_{m-1}=0$ - на виході буде сигнал у відповідності до рівняння $a=b_0 \oplus b_1$ і т.д.

З надходженням чергового тактового імпульсу в регістр 2_0 записується число, що формується на виходах комбінаційного суматора 1, у відповідності з виразом

$$Q_i = (Q_{i-p} + Q_{i-q} + a) \bmod 2^m, \quad (2)$$

де Q_i, Q_{i-p} і Q_{i-q} - числа в регістрах пам'яті $2_0, 2_p$ і 2_q відповідно.

На відміну від пристрою-прототипу, в якому алгоритм додавання не містить додаткової складової - а, в запропонованому генераторі завдяки цій складовій не виникає явище "зациклювання" при додаванні молодших розрядів чисел, яке розповсюджується і на усі старші розряди. В результаті істотно збільшується період повторення псевдовипадкових послідовностей вихідних чисел і бітів і покращуються їх статистичні характеристики.

Покращення характеристик запропонованого генератора у порівнянні з пристроєм-прототипом підтверджується результатами імітаційного моделювання при будь-якій кількості регістрів пристрою і будь-якій кількості їх двійкових розрядів.

Наприклад, при $p=3, q=8$ і $m=10$, тобто при умові, що на виході комбінаційного суматора 1 формується число у відповідності до виразу

$$Q_i = (Q_{i-3} + Q_{i-8} + a) \bmod 2^{10}, \quad (3)$$

були отримані наступні результати для порівнювальних пристроїв.

Період повторення послідовності вихідних чисел пристрою-прототипу становить 261631. В запропонованому пристрої: якщо $s=0$, тобто $a=b_0$, - період повторення дорівнює 392448; якщо $s>0$, тобто для випадків $a=b_0 \oplus b_1, a=b_0 \oplus b_1 \oplus b_2$ і т.д., - період повторення є більшим від 10^9 .

На Фіг. 3 наведені результати аналізу статистичних характеристик пристроїв за допомогою тестів NIST - пакета статистичних тестів, який розроблений Лабораторією інформаційних технологій Національного Інституту Стандартів і Технологій США (NIST). Пакет NIST STS включає в себе 15 статистичних тестів, які розроблені для перевірки гіпотези про випадковість двійкових послідовностей довільної довжини, що генеруються. Кожен з даних тестів спрямований на виявлення різноманітних дефектів випадковості. Обчислюється 188 значень ймовірності P , які можна розглядати як результат роботи окремих тестів. Тест вважається пройденим, коли ймовірність проходження тесту P потрапить у межі від 0,98 до 1,00. Якщо ж ймовірність P буде знаходитись нижче 0,98, вважається, що тест не пройдено. Тестування проводилося при рівні значущості $\alpha=0,01$, який рекомендований розробниками NIST STS.

Тестуванню підлягала псевдовипадкова бітова послідовність що формується на виході молодшого розряду регістра 2^0 - розряду b_0 .

Результати тестування пристрою-прототипу представлені на Фіг. 3а, а запропонованого пристрою - на Фіг. 3б. Отже, запропонований пристрій значно переважає пристрій-прототип за своїми статистичними характеристиками, оскільки стосовно останнього ціла група тестів є не пройденою, а в запропонованому пристрою вихідний псевдовипадковий сигнал відповідає усім вимогам тестування.

Таким чином, в запропонованому пристрої, у порівнянні з відомим, істотно збільшений період повторення псевдовипадкових послідовностей вихідних чисел і бітів і покращені їх статистичні характеристики, що значно покращує характеристики систем захисту інформації і інших систем, де використовуються такі пристрої, в цілому.

ФОРМУЛА ВИНАХОДУ

- 5 Адитивний генератор Фібоначчі із запізненням, який містить комбінаційний суматор та $q+1$ реєстрів пам'яті, тактові входи яких підключені до тактового входу пристрою, інформаційні входи кожного наступного реєстра пам'яті з'єднані з виходами попереднього реєстра пам'яті, виходи p -го реєстра пам'яті підключені до першої групи входів комбінаційного суматора, друга група входів якого з'єднана з виходами q -го реєстра пам'яті, а виходи комбінаційного суматора підключені до інформаційних входів 0-го реєстра пам'яті, який **відрізняється** тим, що
- 10 додатково містить логічну схему, інформаційні входи якої з'єднані з виходами 0-го реєстра пам'яті і виходами пристрою, керуючі входи підключені до керуючих входів пристрою, а її вихід з'єднаний з входом переносу комбінаційного суматора.

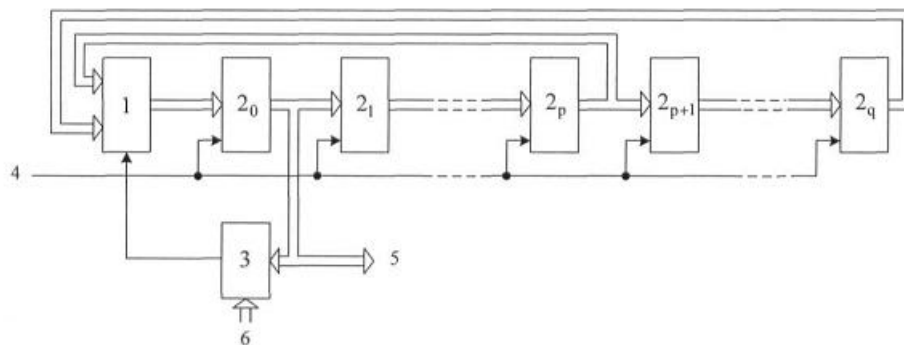


Fig. 1

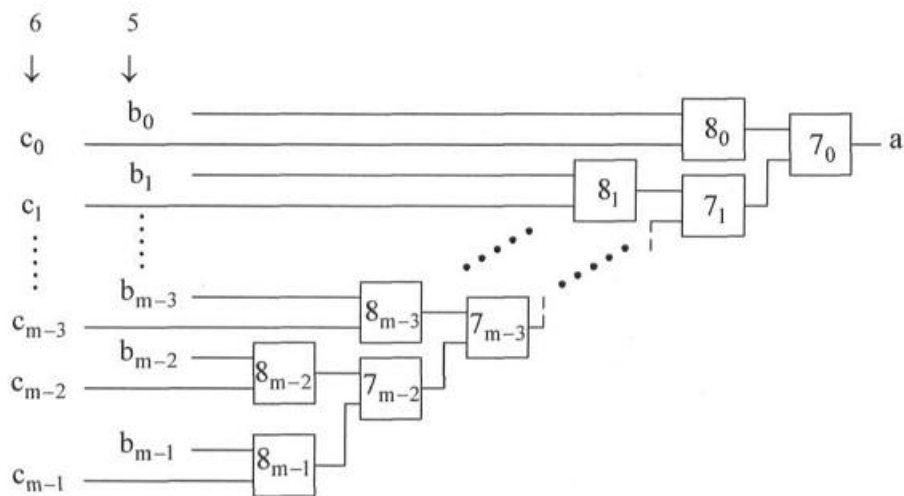
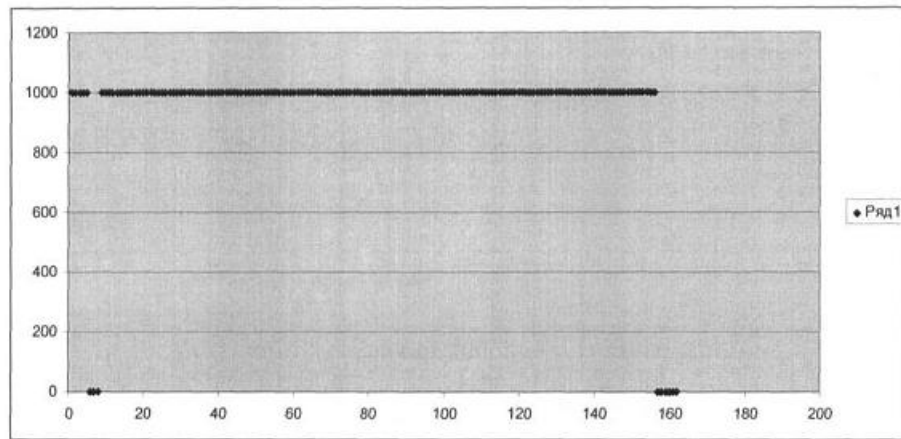
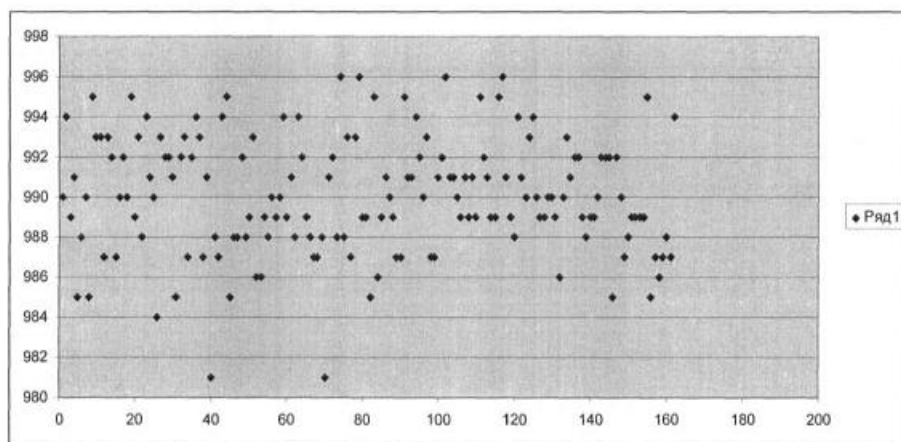


Fig. 2



а



б

Fig. 3

Комп'ютерна верстка О. Рябко

Державна служба інтелектуальної власності України, вул. Василя Липківського, 45, м. Київ, МСП, 03680, Україна

ДП "Український інститут інтелектуальної власності", вул. Глазунова, 1, м. Київ – 42, 01601