



УКРАЇНА

(19) UA (11) 25294 (13) A

(51) G 06 F 7/58

ДЕРЖАВНЕ  
ПАТЕНТНЕ  
ВІДОМСТВООПИС ДО ПАТЕНТУ  
НА ВІНАХІДбез проведення експертизи по суті  
на підставі Постанови Верховної Ради України  
№ 3769 XII від 23 XII 1993 рПублікується  
в редакції заявника

## (54) СПОСІБ ГЕНЕРАЦІЇ ВИПАДКОВИХ ЧИСЕЛ

1

- (21) 98073538  
(22) 06.07.98  
(24) 30.10.98  
(46) 25.12.98. Бюл. № 6  
(47) 30.10.98  
(56) 1. Бобнев М. П. Генерирование случайных сигналов. - М.: Энергия, 1971.  
2. Авторское свидетельство СССР № 1817094 // Бюл. № 19, 1993.  
3. Галлагер Р. Г. Теория информации и надежная связь. - М.: Советское радио, 1974.  
4. Santha M., Vazirani U. V. Generating Quasi-random Sequences from Semirandom Sources // Journal of computer and sciences - 1986. - № 33. - С. 75-87.  
(72) Горицький Віктор Михайлович, Іванченко Сергій Олександрович, Паршуков Святослав Станіславович

2

- (73) Горицький Віктор Михайлович, Іванченко Сергій Олександрович, Паршуков Святослав Станіславович  
(57) Спосіб генерації випадкових чисел полягає в тому, що беруть по одному числу з декількох послідовностей випадкових чисел від первинних генераторів, об'єднують їх в блок і перетворюють його, потім проводять аналогічні перетворення з наступними числами цих же послідовностей, на виході отримують послідовність випадкових чисел з покращеними статистичними характеристиками, який відрізняється тим, що сформовані блоки від первинних генераторів кодують блочним кодом і з отриманих блоків формують вихідну послідовність кодового генератора випадкових чисел.

Винахід відноситься до галузі генерації випадкових чисел в обчислювальній техніці, техніці зв'язку і може бути використаний для поліпшення статистичних характеристик випадкових чисел від первинних джерел, що мають широке застосування в криптографії, в моделюванні, методі "Монте-Карло", створенні штучних завод та ін.

Існуючі способи [1] генерації випадкових чисел, як правило, засновані на перетворенні існуючого в природі випадкового процесу (наприклад, шуму) в цифровий вигляд, або на використанні випадкових станів схеми після подачі на неї збурення.

Основним недоліком їх є наявність міжсимвольної кореляції і залежності частоти появи випадкових чисел від зовнішніх умов, температури, вологості, радіації, тиску, електроживлення та ін.

Найбільш близьким по суті до передбачуваного винаходу є спосіб вирівнювання статистичних характеристик шляхом одночасного додавання по модулю два декількох вхідних випадкових процесів, який реалізується в генераторі випадкових чисел [2].

Недоліком цього способу є незадовільні статистичні характеристики послідовності

(19) UA (11) 25294 (13) A

випадкових чисел. Наявність самої малої степені міжсимвольної кореляції, при збільшенні швидкості генерації, стає все більше вагомою негативною властивістю послідовності.

В основу винаходу поставлено задачу вдосконалення способу генерації випадкових чисел шляхом застосування кодування для отримання послідовностей рівномірних і взаємонезалежних випадкових чисел.

Суть цього способу генерації випадкових чисел полягає в кодуванні блочним кодом послідовностей випадкових чисел від первинних генераторів випадкових чисел (ПГВЧ), кількість яких визначає використаний код, і в формуванні кодової послідовності випадкових чисел з покращеними ймовірнісними характеристиками, максимально приближеними до ідеальних.

Структурна схема кодового генератора випадкових чисел (КГВЧ), який реалізує цей спосіб, зображена на фіг.1. ПГВЧ 1 синхронно генерують випадкові послідовності, які мають незадовільні статистичні характеристики. Вони надходять в кодувальний пристрій 2. Кодувальний пристрій 2 в кожному такті синхронізації об'єднує первинні випадкові числа в блок випадкових чисел, довжина якого відповідає кількості ПГВЧ, кодує його блочним кодом і з отриманих блоків формує вихідну послідовність КГВЧ. В процесі роботи КГВЧ кожному синхроімпульсу (випадковому числу від ПГВЧ) відповідає випадковий кодовий блок кодовий блок (випадкова комбінація чисел), довжина якого більше одиниці і менше кількості ПГВЧ. Швидкість генерації КГВЧ визначається довжиною кодового блоку і швидкістю ПГВЧ.

Поліпшення статистичних характеристик запропонованим способом генерації більш наочно демонструється за допомогою математичної моделі, зображеної на фіг.2. Вектор  $X^n$  довжиною  $n$  являє собою блок об'єднаних випадкових чисел від  $n$  ПГВЧ за один такт синхронізації. В результаті кодування здійснюються перехід випадкових векторів  $X^n$  в вектори  $Y^k$  довжиною  $k(k < n)$ , що утворюють вихідну послідовність КГВЧ в результаті його синхронної роботи.

Максимально досяжний результат і зв'язок його зі швидкістю генерації, при використанні як зазвичай ефективного коду в запропонованому способі, визначені теоремою Шеннона [3], яка говорить, що будь-яку послідовність  $X$  з ентропією  $H(X)$  (без умови однозначного декодування) можна закодувати в  $Y$ , так що:

$$\frac{k}{n} = \frac{H(X)}{H_{\max}(Y)} - \varepsilon, \quad (1)$$

де  $k$  – кількість символів в послідовності  $Y^k$ ;  
 $n$  – кількість символів в послідовності  $X^n$ ;

$H(X)$  – ентропія кодувальної послідовності  $X^n = \{x_1, x_2, x_3, \dots, x_n\}$ ;

$H_{\max}(Y)$  – максимально можлива ентропія закодованої послідовності  $Y^k = \{y_1, y_2, y_3, \dots, y_k\}$  (при основі логарифма – 2  $H_{\max}(Y) = 1$ );

$\varepsilon$  – як зазвичай мала позитивна величина.

Згідно з [4] ПГВЧ можна уявити в вигляді процесу підкидання монети зі зміщенням центром ваги –  $\delta$ , зміщення якого залежить від історії попередніх підкидань. Вихідна послідовність такого джерела напіввипадкова, тобто для неї виконується нерівність:

$$\delta \leq \Pr\{x_i=1/x_1, x_2, \dots, x_{i-1}\} \leq 1 - \delta, \quad (2)$$

де  $\delta = \text{const}$  ( $0 < \delta \leq 1/2$ );

$x_i$  – компонента з номером  $i$  випадкової послідовності, ( $i=1, 2, 3, \dots$ );

$\Pr\{x_i=1/x_1, x_2, \dots, x_{i-1}\}$  – умовна ймовірність того, що  $x_i=1$  за умови, що ряд попередніх підкидань складається з компонент  $\{x_1, x_2, \dots, x_{i-1}\}$

Нехай для простоти обчислень:

$$\Pr\{x_i=1/x_1, x_2, \dots, x_{i-1}\} = \delta \vee \Pr\{x_i=0/x_1, x_2, \dots, x_{i-1}\} = 1 - \delta, \quad (3)$$

де  $\Pr\{x_i=1/x_1, x_2, \dots, x_{i-1}\}$  і  $\Pr\{x_i=0/x_1, x_2, \dots, x_{i-1}\}$  – умовні ймовірності того, що  $x_i=1$  і  $x_i=0$  за умови, що ряд попередніх підкидань складається з компонент  $\{x_1, x_2, \dots, x_{i-1}\}$ ;

$x_i$  – компонента з номером  $i$  випадкової послідовності, ( $i=1, 2, 3, \dots$ ),

$\delta = \text{const}$  ( $0 < \delta \leq 1/2$ ).

Тоді розподіл ймовірностей комбінацій  $X^n$  визначається:

$$P(X^n) = \delta^a (1 - \delta)^{n-a}, \quad (4)$$

де  $P(X^n)$  – ймовірність появи вектора  $X^n$ ;

$X^n$  – вектор з  $n$  незалежних компонент  $\{x_1, x_2, \dots, x_n\}$ ;

$\delta = \text{const}$  ( $0 < \delta \leq 1/2$ );

$a$  – вага вектора  $X^n$ ;

$n$  – довжина його.

Згідно з [3] ентропія отриманого вектора  $Y^k$ :

$$H(Y) = \frac{1}{k} \sum_{j=1}^k \sum_{i=1}^{2^{n-k}} P(X^n_{ji}) \times$$

$$x \log_2 \frac{1}{\sum_{i=1}^{2^{n-k}} P(X_{ji}^n)} \quad (5)$$

$$\lim_{\delta_y \rightarrow \frac{1}{2}} H(Y) = \lim_{\sum_{j=1}^{2^{n-k}} P(X_{ji}^n) \rightarrow \frac{1}{2^k}} \frac{1}{k} \sum_{i=1}^{2^k} \sum_{j=1}^{2^{n-k}} x$$

$$x P(X_{ji}^n) \log_2 \frac{1}{\sum_{i=1}^{2^{n-k}} P(X_{ji}^n)} = 1, \quad (6)$$

де  $H(Y)$  – ентропія вектора  $Y^k$ ;

$k$  – довжина вектора  $Y^k$ ;

$P(X_{ji}^n)$  – ймовірність появи вектора  $X_{ji}^n$  довжиною  $n$ ;

$i$  – номер вектора  $X_{ji}^n$  в стовбці (фіг.1) ( $i=1, 2, 3, \dots, 2^{n-k}$ );

$j$  – номер вектора  $X_{ji}^n$  в рядку (фіг.1) ( $j=1, 2, 3, \dots, 2^k$ );

$\delta_y$  – результуюче зміщення вектора  $Y^k$ ;

Вираз (5) з врахуванням (3) і (4) дають оцінку способу кодової генерації випадкових чисел і можуть бути використані для розрахунку параметрів КГВЧ. Вираз (6) представляє умови для досягнення максимальної ефективності запропонованого способу, яким, порівняно з способом генерації шляхом додавання по модулю два, при використанні меншої кількості ПГВЧ, можна генерувати послідовність випадкових чисел, завдяки ефективності кодування, як завжди близьку до ідеально випадкової та з швидкістю більшою по відношенню до ПГВЧ. Найбільш ефективним для реалізації КГВЧ є код з відомим симетричним ваговим спектром суміжних класів.

На фіг. 1 показана структурна схема кодового генератора випадкових чисел, де: 1 – первинний генератор випадкових чисел;

2 – кодуєчий пристрій, який здійснює об'єднання водночас згенерованих чисел від  $n$  незалежних первинних генераторів випадкових чисел – 1 в векторі  $X^n$  довжиною  $n$  і кодування їх в відповідні  $Y^k$ .

На фіг.2 показана математична модель способу генерації випадкових чисел, де:  $X_{ji}^n$  – вектор з  $n$  незалежних компонент  $\{x_1, x_2, \dots, x_n\}$ ;  $n$  – довжина вектора  $X_{ji}^n$ ;  $i$  – номер вектора  $X_{ji}^n$  в стовбці (фіг.1) ( $i=1, 2, 3, \dots, 2^{n-k}$ );  $j$  – номер вектора  $X_{ji}^n$  в рядку (фіг.1) ( $j=1, 2, 3, \dots, 2^k$ ).

На фіг. 3 показана структурна схема східчастої конструкції кодового генератора випадкових чисел, де: 1 – первинний генератор випадкових чисел, 2 – кодуєчий пристрій. Для кожного проміжного ступеня в ролі первинного генератора випадкових чисел 1 виступає попередній кодовий генератор 2.

Спосіб генерації випадкових чисел реалізують програмно і апаратно. Конструктивно апаратна реалізація даного способу проста і може бути виготовлена на друкованій платі за структурною схемою, зображеною на фіг.1. Випадкові послідовності, синхронно сформовані кожним ПГВЧ 1 з застосуванням синхронізуючого пристрою, надходять в кодуєчий пристрій 2, який в кожному такті синхронізації об'єднує первинні випадкові числа в блоки випадкових чисел, кодує їх і з утворених блоків формує вихідну послідовність КГВЧ. Використані пристрої відомі і реалізація їх не викликає труднощів. Одним з технічних задач реалізації запропонованого способу є забезпечення незалежності первинних джерел, що не представляє великої складності.

Даний спосіб генерації припускає ступеневу конструкцію (фіг.3), яка складається з декількох ступеней кодування, що дозволяє досягнути будь-яких високих результатів за рахунок збільшення кількості незалежних первинних генераторів випадкових чисел.

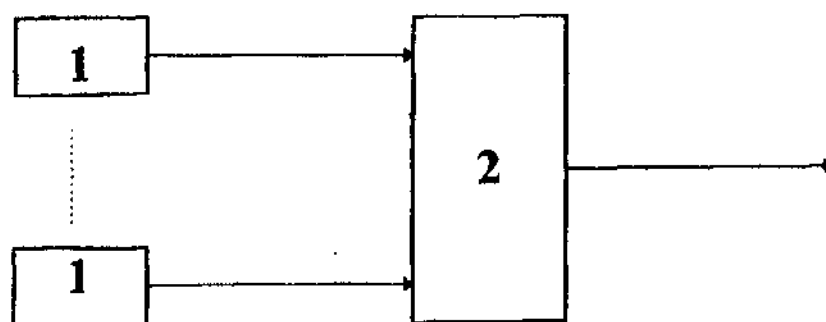


Fig. 1

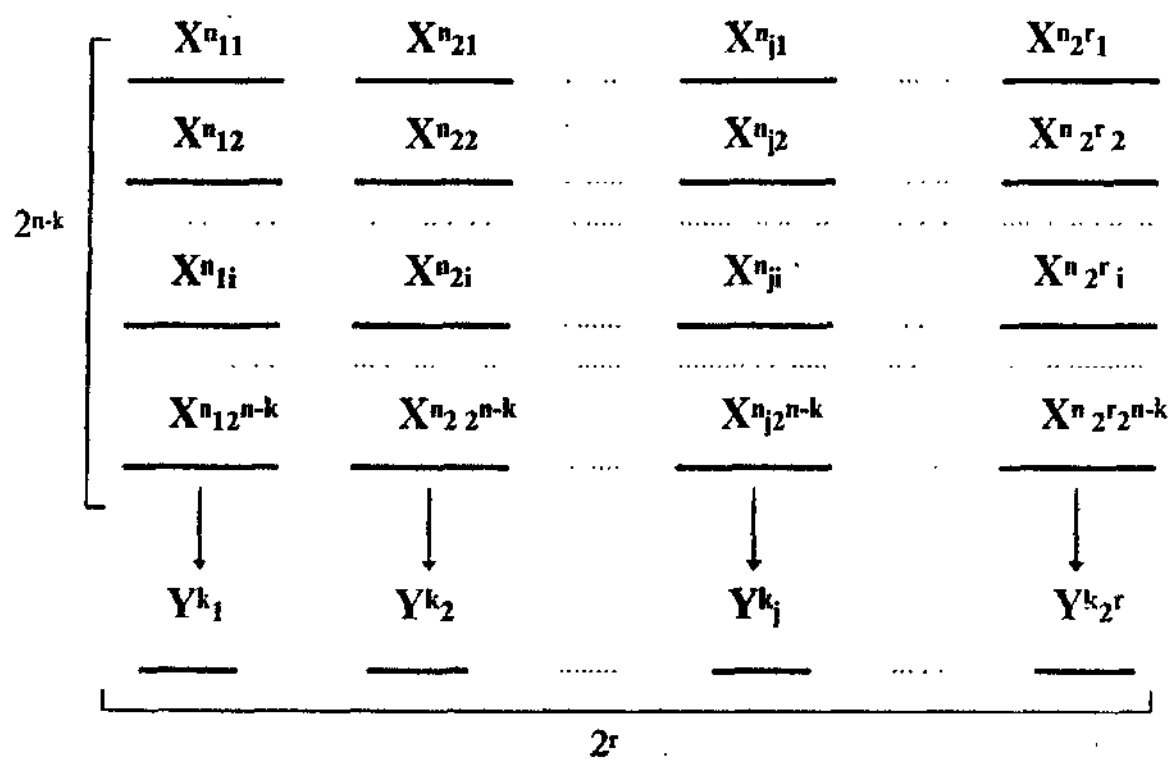
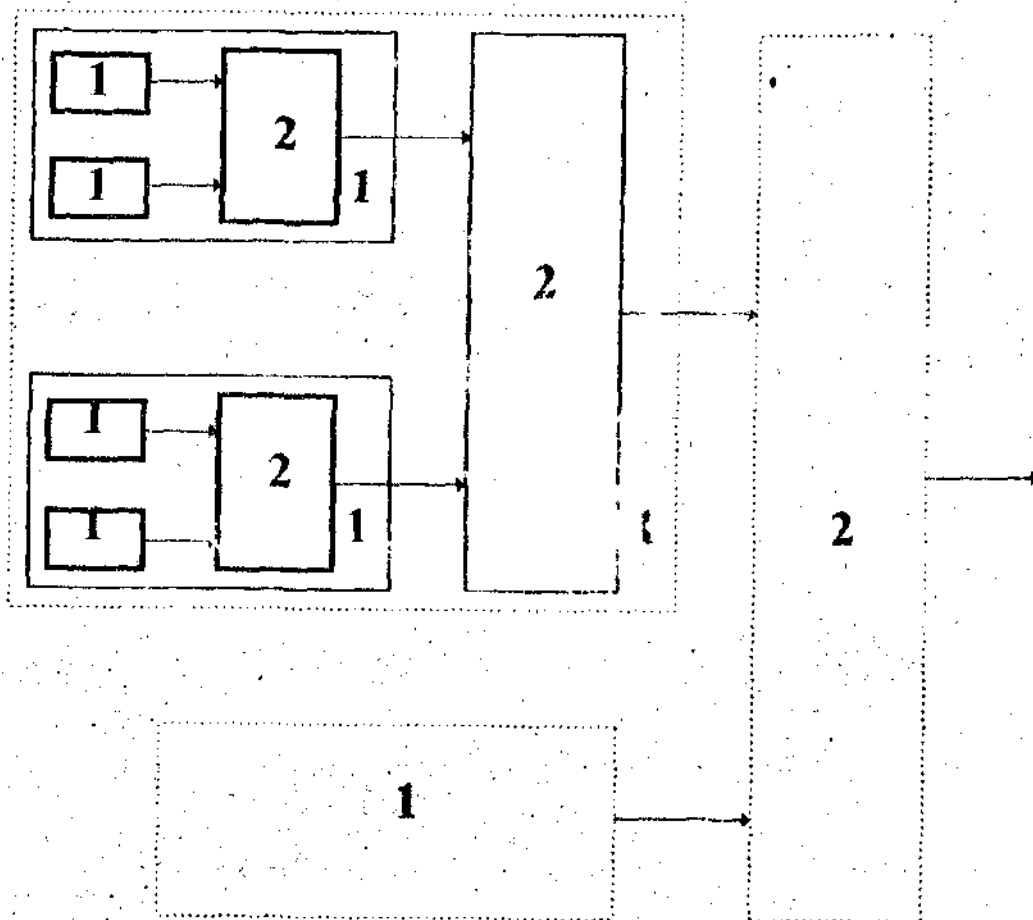


Fig. 2



Фіг. 3

Упорядник

Техред М.Келемеш

Коректор О. Обручар

Замовлення 4634

Тираж

Підписне

Державне патентне відомство України,  
254655, ГСП, Київ-53, Львівська пл., 8

Відкрите акціонерне товариство "Патент", м. Ужгород, вул. Гагаріна, 101

