УКРАЇНА

(19) UA (11) 38402 (13) U

(51) МПК (2006)
G09C 1/00

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

ОПИС
ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

видається під відповідальність власника патенту

(54) СПОСІБ ФОРМУВАННЯ ПОСЛІДОВНОСТЕЙ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

(21) u200810861
(22) 03.09.2008
(24) 12.01.2009
(46) 12.01.2009, Бюл.№ 1, 2009 р.
(72) КУЗНЕЦОВ ОЛЕКСАНДР ОЛЕКСАНДРОВИЧ, UA, ЄВСЕЄВ СЕРГІЙ ПЕТРОВИЧ, UA, РЯБУХА ЮРІЙ МИКОЛАЙОВИЧ, UA, КОРОЛЬОВ РОМАН ВІКТОРОВИЧ, UA, ПУДОВ ВІТАЛІЙ АНАТОЛІЙОВИЧ, UA
(73) ЄВСЕЄВ СЕРГІЙ ПЕТРОВИЧ, UA
(57) Спосіб формування послідовностей псевдовипадкових чисел, який полягає у тому, що ключова послідовність подається у вигляді вектора, що ініціалізує початкове значення аргументу функції модульного піднесення до степеня, а вихідні елементи послідовності псевдовипадкових чисел формуються шляхом зчитування значення функції модульного піднесення за допомогою відповідних пристроїв, який **відрізняється** тим, що додатково вводять рекурентні перетворення, які дозволяють формувати послідовності псевдовипадкових чисел максимального періоду.

Запропонована корисна модель відноситься до галузі криптографічного захисту інформації і може бути використана в засобах шифрування та генераторах послідовностей псевдовипадкових чисел у системах обробки інформації для розширення їх можливостей.

Відомий спосіб формування послідовностей псевдовипадкових чисел [1], який ґрунтується на тому, що ключова послідовність подається у вигляді вектора, який ініціалізує початкове значення аргументу функції модульного піднесення до ступеня. Наступне значення аргументу функції обраховується за допомогою пристроїв модульного піднесення до ступеня, а вихідні елементи послідовності псевдовипадкових чисел формуються шляхом зчитування значення функції модульного піднесення за допомогою відповідних пристроїв. Задача вираховування функції, яка є зворотною до модульного піднесення до ступеня є важкорозв'язуваною теоретико-складною задачею дискретного логарифмування, щодо вирішення якої на сьогоднішній день невідомо ефективних алгоритмів вираховування дискретних логарифмів великих чисел. Тому цей спосіб формування послідовностей псевдовипадкових чисел є криптографічно стійким.

Недоліком цього способу є те, що він не дозволяє формувати послідовності псевдовипадкових чисел максимального періоду, що суттєво зменшує його ефективність та обмежує можливості щодо практичного використання.

Найбільш близьким, до запропонованого технічним рішенням, обраним як прототип, є спосіб формування послідовностей псевдовипадкових чисел [2], який ґрунтується на тому, що ключова послідовність подається у вигляді вектора x_0, який ініціалізує початкове значення аргументу функції $f(x) = x^e \bmod n$ модульного піднесення до ступеня. У якості модуля n обирається добуток великих простих чисел p і q, у якості ступеня e обирається число, взаємно просте з $(p-1)\cdot(q-1)$. Наступне значення аргументу функції обраховується за допомогою пристроїв модульного піднесення до ступеня, а вихідні елементи послідовності псевдовипадкових чисел формуються шляхом зчитування значення функції модульного піднесення за допомогою відповідних пристроїв, тобто шуканою послідовністю біт довжини m буде послідовність

$$b_0\ b_1\ b_2\ \dots\ b_i\ \dots\ b_{m-1}, i = \overline{0,(m-1)},$$

(19) UA (11) 38402 (13) U

де b_i - молодший біт числа x_i,

$x_{i+1} = f(x_i) = x_i^e \bmod n$.

Задача вираховування функції $f(x)^{-1}$, яка є зворотною до функції модульного піднесення до ступеня $f(x) = x^e \bmod n$, тобто вирахування деякого значення x_i за відомим значенням x_{i+1} є важкорозв'язуваною теоретико-складною задачею дискретного логарифмування, щодо вирішення якої на сьогоднішній день невідомо ефективних алгоритмів вираховування дискретних логарифмів великих чисел. Тому цей спосіб формування послідовностей псевдовипадкових чисел є криптографічно стійким.

Недоліком способу-прототипу є те, що він не дозволяє формувати послідовності псевдовипадкових чисел максимального періоду, що суттєво зменшує його ефективність та обмежує можливості щодо практичного використання.

В основу корисної моделі поставлена задача створити спосіб формування послідовностей псевдовипадкових чисел який, за рахунок додаткового введення рекурентних перетворень, що реалізуються, наприклад, за допомогою лінійних рекурентних регістрів зі зворотними зв'язками, дозволить формувати послідовності псевдовипадкових чисел максимального періоду, що підвищить його ефективність та розширить можливості щодо практичного використання.

Поставлена задача вирішується за рахунок додаткового введення рекурентних перетворень які дозволяють формувати послідовності псевдовипадкових чисел максимального періоду.

Технічний результат, який може бути отриманий при здійснені корисної моделі полягає в отриманні можливості формувати послідовності псевдовипадкових чисел максимального періоду, що підвищує ефективність та розширює його можливості.

Сутність запропонованого способу формування послідовностей псевдовипадкових чисел полягає в тому, що ключова послідовність подається у вигляді вектора x_0, який ініціалізує початкове значення аргументу функції $f(x) = x^e \bmod n$ модульного піднесення до ступеня та початкове значення y_0 рекурентного перетворення $L(y)$, що реалізуються, наприклад, за допомогою лінійних рекурентних регістрів зі зворотними зв'язками. У якості модуля n обирається добуток великих простих чисел p і q, у якості ступеня e обирається число, взаємно просте з $(p-1)\cdot(q-1)$. Наступне значення аргументу функції обраховується за допомогою пристроїв модульного піднесення до ступеня та за допомогою рекурентного перетворення, що реалізується, наприклад, за допомогою лінійних рекурентних регістрів зі зворотними зв'язками. Вихідні елементи послідовності псевдовипадкових чисел формуються шляхом зчитування значення функції модульного піднесення за допомогою відповідних пристроїв, тобто шуканою послідовністю біт довжини m буде послідовність

$b_0\ b_1\ b_2\ \ldots\ b_i\ \ldots\ b_{m-1}, i = \overline{0,(m-1)}$,

де b_i - молодший біт числа x_i,

$x_{i+1} = f(x_i + L(y_i)) = (x_i + L(y_i))^e \bmod n$.

Задача вираховування функції $f(x)^{-1}$, яка є зворотною до функції модульного піднесення до ступеня $f(x) = x^e \bmod n$, тобто вирахування деякого значення $(x_i + L(y_i)$ за відомим значенням x_{i+1} є важкорозв'язуваною теоретико-складною задачею дискретного логарифмування, щодо вирішення якої на сьогоднішній день невідомо ефективних алгоритмів вираховування дискретних логарифмів великих чисел. Тому цей спосіб формування послідовностей пссвдовипадкових чисел є криптографічно стійким. Додатково введене рекурентне перетворення $L(y)$, що реалізуються, наприклад, за допомогою лінійних рекурентних регістрів зі зворотними зв'язками, дозволяє формувати послідовності псевдовипадкових чисел максимального періоду.

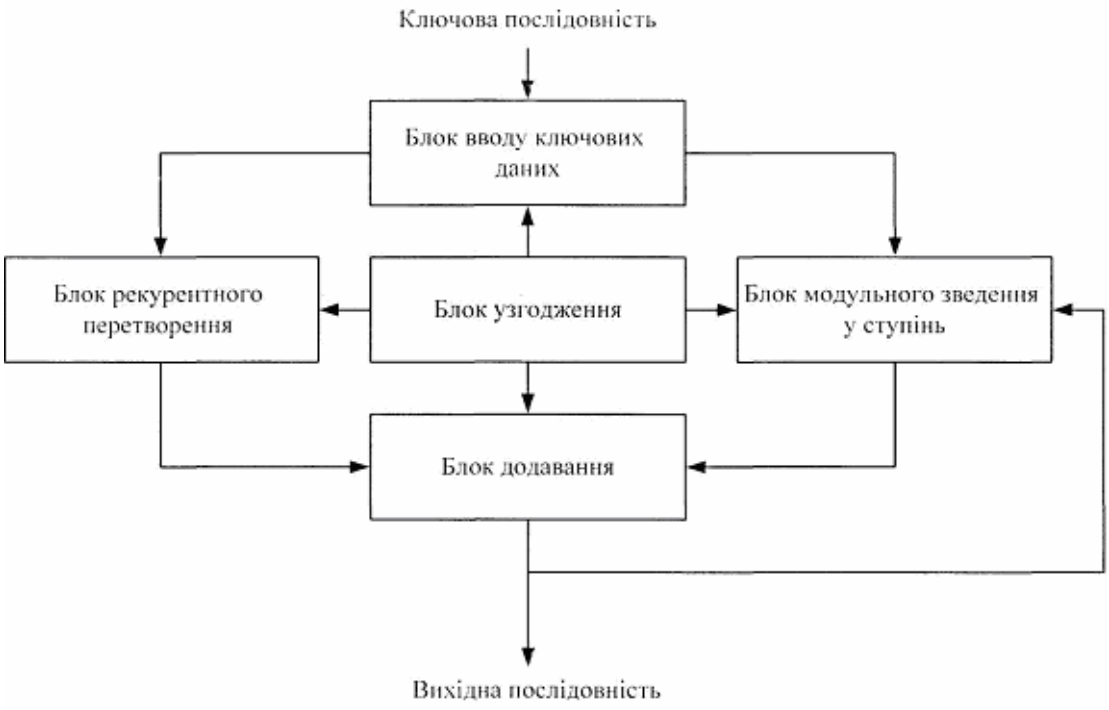
Запропонований спосіб може бути реалізовано у вигляді пристрою, схема електрична структурна якого зображена на Фіг.

Таким чином, за рахунок додаткового введення рекурентних перетворень, що реалізуються, наприклад, за допомогою лінійних рекурентних регістрів зі зворотними зв'язками, вдається формувати послідовності псевдовипадкових чисел максимального періоду, що підвищує ефективність та розширює можливості практичного використання.

Джерела інформації:

1. Shamir, A. On the generation of cryptographically strong pseudorandom sequences. // ACM Transactions on Computer Systems, vol.1., 1983, pp.38-34.

2. Blum, M., Micali, S. How to generate cryptographically strong sequences of pseudo-random bits. // SIAM Journal on Computing, vol.13, 1984, pp.850-864.



Фіг.

Комп'ютерна верстка О. Рябко Підписне Тираж 28 прим.

Міністерство освіти і науки України
Державний департамент інтелектуальної власності, вул. Урицького, 45, м. Київ, МСП, 03680, Україна

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