УКРАЇНА

(19) UA (11) 38401 (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) u200810862
(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 після рівноважного перетворення ініціалізує початкове значення аргументу функції обчислення вектора-синдрому, а вихідні елементи послідовності псевдовипадкових чисел формуються шляхом зчитування значення функції обчислення вектора-синдрому за допомогою відповідних пристроїв, який **відрізняється** тим, що додатково вводять рекурентні перетворення, які дозволяють формувати послідовності псевдовипадкових чисел максимального періоду.

Запропонована корисна модель належить 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 вектору, який ініціалізує початкове значення аргументу функції модульного зведення у ступінь. Наступне значення аргументу функції обраховується за допомогою пристроїв модульного зведення у ступінь, а вихідні елементи послідовності псевдовипадкових чисел формуються шляхом зчитування значення функції модульного зведення за допомогою відповідних пристроїв. Задача вираховування функції, яка є зворотною до модульного зведення у ступінь 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 вектору x_0, який після рівноважного перетворення $\tilde{x} = \varphi(x)$ ініціалізує початкове значення аргументу функції $f(\tilde{x}) = f(\varphi(x)) = \varphi(x) \cdot H^T$ обчислення вектору-синдрому. У якості матриці H обирається перевірочна матриця лінійного блокового коду. Наступне значення аргументу функції обраховується за допомогою пристроїв обчислення вектору-синдрому та рівноважного перетворення $\varphi(x)$. Вихідні елементи послідовності псевдовипадкових чисел формуються шляхом зчитування значення функції обчислення вектору-синдрому за допомогою відповідних пристроїв, тобто шуканою послідовністю біт довжини буде послідовність

$b_0\ b_1\ b_2\ \ldots\ b_i\ \ldots\ b_{m-1}$,

де b_i - біти вектору-синдрому x_i,

$x_{i+1} = f(\tilde{x}_i) = f(\varphi(x_i)) = \varphi(x_i) \cdot H^T$.

Задача вираховування рівноважного вектору $\varphi(x_i)$ за відомим вектором-синдромом x_{i+1} є важкорозв'язувана теоретико-складна задача синдромного декодування. Тому цей спосіб формування послідовностей псевдовипадкових чисел є криптографічно стійким.

(19) UA (11) 38401 (13) U

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.

Суть запропонованого способу формування послідовностей псевдовипадкових чисел полягає в тому, що ключова послідовність подається у вигляді вектору x_0, який після рівноважного перетворення $\tilde{x} = \varphi(x)$ ініціалізує початкове значення аргументу функції $f(\tilde{x}) = f(\varphi(x)) = \varphi(x) \cdot H^T$ обчислення вектору-синдрому та початкове значення y_0 рекурентного перетворення $L(y)$, що реалізуються, наприклад, за допомогою лінійних рекурентних регістрів зі зворотними зв'язками. У якості матриці H обирається перевірочна матриця лінійного блокового коду. Наступне значення аргументу функції обраховується за допомогою пристроїв обчислення вектору-синдрому, рівноважного перетворення $\varphi(x)$ 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 обчислення вектору-синдрому за допомогою відповідних пристроїв, тобто шуканою послідовністю біт довжини буде послідовність

$b_0\ b_1\ b_2\ \dots\ b_i\ \dots\ b_{m-1}$,

де b_i - біти вектору-синдрому x_i,

$$x_{i+1} = f(\varphi(x_i + L(y_i))) = \varphi(x_i + L(y_i)) \cdot H^T.$$

Задача вираховування рівноважного вектору $\varphi(x_i + L(y_i))$ за відомим вектором-синдромом x_{i+1} є важкорозв'язувана теоретико-складна задача синдромного декодування. Тому цей спосіб формування послідовностей псевдовипадкових 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.

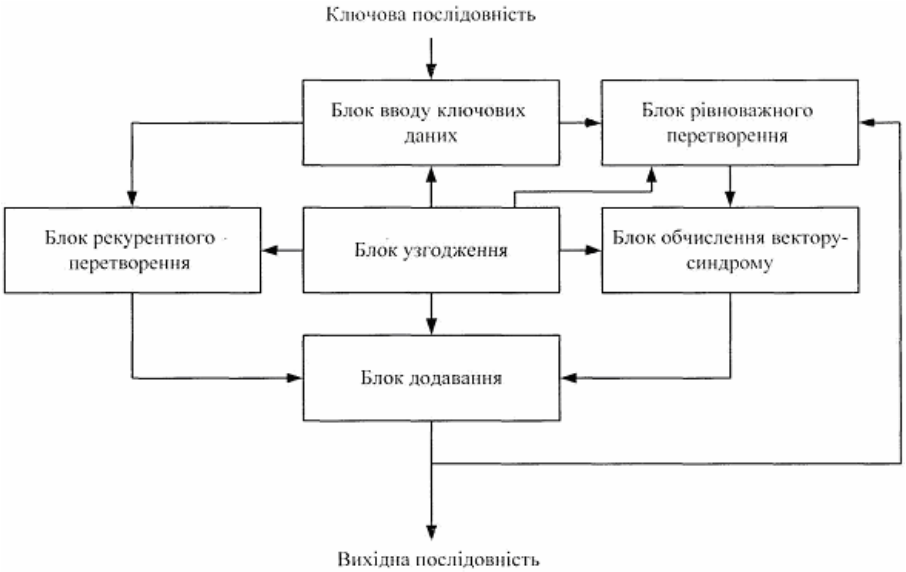
Запропонований спосіб може бути реалізовано у вигляді пристрою, схема електрична структурна якого зображена на Фіг.

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. Jean-Dernard Fisher, Jacques Stern. An efficient Pseudo-Random Generator Provably as Secure as Syndrome Decoding // EUROCRYPT'96 Proceeding, LNCS 1070. P.245-255.



Комп'ютерна верстка В. Мацело 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