УКРАЇНА UKRAINE

П А Т Е Н Т

НА КОРИСНУ МОДЕЛЬ

№ 51869

СПОСІБ ФОРМУВАННЯ ПОСЛІДОВНОСТЕЙ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

Видано відповідно до Закону України "Про охорону прав на винаходи і корисні моделі".

Зареєстровано в Державному реєстрі патентів України на корисні моделі **10.08.2010.**

Голова Державного департаменту інтелектуальної власності М.В. Паладій

Міністерство освіти і науки України * Державний департамент інтелектуальної власності * № 1

(11) **51869**

(19) **UA**

(51) **МПК** (2009)
G09C 1/00

(21) Номер заявки: **u 2009 13226**

(22) Дата подання заявки: **18.12.2009**

(24) Дата, з якої є чинними права на корисну модель: **10.08.2010**

(46) Дата публікації відомостей про видачу патенту та номер бюлетеня: **10.08.2010, Бюл. № 15**

(72) Винахідники:
Кузнецов Олександр Олександрович, UA,
Євсеєв Сергій Петрович, UA,
Рябуха Юрій Миколайович, UA,
Ковтун Владислав Юрійович, UA,
Щербаков Олександр Всеволодович, UA

(73) Власник:
Євсеєв Сергій Петрович,
вул.Ком.Корка,12,кв.212,
м.Харків, 61148, Україна, UA

(54) Назва корисної моделі:

СПОСІБ ФОРМУВАННЯ ПОСЛІДОВНОСТЕЙ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

(57) Формула корисної моделі:

Спосіб формування послідовностей псевдовипадкових чисел, який полягає у тому, що ключову послідовність подають у вигляді вектора, який ініціалізує початкове значення аргументу функції перетворення, а вихідні елементи послідовності псевдовипадкових чисел формують шляхом зчитування значення цієї функції за допомогою відповідних пристроїв, який **відрізняється** тим, що додатково вводять перетворення у групі дивізорів гіпереліптичної кривої, що реалізуються за допомогою пристроїв скалярного множення дивізорів гіпереліптичної кривої і дозволяють значно скоротити довжину ключової послідовності та спростити побудову відповідних пристроїв формування послідовностей псевдовипадкових чисел.

УКРАЇНА

(19) UA (11) 51869 (13) U

(51) МПК (2009)
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) u200913226
(22) 18.12.2009
(24) 10.08.2010
(46) 10.08.2010, Бюл.№ 15, 2010 р.
(72) КУЗНЕЦОВ ОЛЕКСАНДР ОЛЕКСАНДРОВИЧ, ЄВСЕЄВ СЕРГІЙ ПЕТРОВИЧ, РЯБУХА ЮРІЙ МИКОЛАЙОВИЧ, КОВТУН ВЛАДИСЛАВ ЮРІЙОВИЧ, ЩЕРБАКОВ ОЛЕКСАНДР ВСЕВОЛОДОВИЧ
(73) ЄВСЕЄВ СЕРГІЙ ПЕТРОВИЧ
(57) Спосіб формування послідовностей псевдовипадкових чисел, який полягає у тому, що ключову послідовність подають у вигляді вектора, який ініціалізує початкове значення аргументу функції перетворення, а вихідні елементи послідовності псевдовипадкових чисел формують шляхом зчитування значення цієї функції за допомогою відповідних пристроїв, який **відрізняється** тим, що додатково вводять перетворення у групі дивізорів гіпереліптичної кривої, що реалізуються за допомогою пристроїв скалярного множення дивізорів гіпереліптичної кривої і дозволяють значно скоротити довжину ключової послідовності та спростити побудову відповідних пристроїв формування послідовностей псевдовипадкових чисел.

1 2

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 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 для забезпечення необхідної стійкості використовується велика довжина ключової послідовності (послідовності, що ініціює початкове значення аргументу функції) а відповідні перетворення потрібно виконувати над дуже великими числами що значно ускладнює побудову відповідних пристроїв формування послідовностей псевдовипадкових чисел.

Найбільш близьким до запропонованого технічним рішенням, є спосіб формування послідовностей псевдовипадкових чисел [2], який ґрунтується на тому, що ключова послідовність подається у вигляді вектору x_0, який ініціалізує початкове значення аргументу функції $f(x)=x^2 \bmod n$ модульного зведення у квадрат. У якості модуля n обирається добуток великих простих чисел p і q, які тотожні трьом за модулем чотири, тобто: $p \equiv 3 \bmod 4$, $q \equiv 3 \bmod 4$, $n=p \cdot q$ (ціле число Блюма). Наступне значення аргументу функції обраховується за допомогою пристроїв модульного зведення у квадрат а вихідні елементи послідовності псевдовипадкових чисел формуються шляхом зчитування значення функції модульного зведення 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,

$x_{i+1}=f(x_i)= x_i^2 \bmod n$.

Задача вираховування примітивних квадратних коренів за модулем числа n обчислювально еквівалентна задачі розкладення цього числа на множники, тобто важкорозв'язуваної теоретико-складної задачі факторизації. Тому цей спосіб формування послідовностей псевдовипадкових чисел є криптографічно стійким.

(19) UA (11) 51869 (13) U

Недоліком способу – найближчого аналогу є те, що для забезпечення необхідної стійкості використовується велика довжина ключової послідовності (послідовності, що ініціює початкове значення аргументу функції) а відповідні перетворення потрібно виконувати над дуже великими числами що значно ускладнює побудову відповідних пристроїв формування послідовностей псевдовипадкових чисел.

В основу корисної моделі поставлена задача створити спосіб формування послідовностей псевдовипадкових чисел який, за рахунок застосування пристроїв скалярного множення точок еліптичної кривої при порівняних показниках стійкості дозволив би значно скоротити довжину ключової послідовності (послідовності, що ініціює початкове значення аргументу функції) а відповідні перетворення потрібно було б виконувати над значно меншими числами що значно спрощує побудову відповідних пристроїв формування послідовностей псевдовипадкових чисел.

Поставлена задача вирішується за рахунок додаткового введення пристроїв скалярного множення дивізорів гіпереліптичної кривої які дозволяють при порівняних показниках стійкості значно скоротити довжину ключової послідовності та спростити побудову відповідних пристроїв формування послідовностей псевдовипадкових чисел.

Технічний результат, який може бути отриманий при здійснені корисної моделі полягає в отриманні можливості значно скоротити довжину ключової послідовності (послідовності, що ініціює початкове значення аргументу функції) та спростити побудову відповідних пристроїв формування послідовностей псевдовипадкових чисел.

Сутність запропонованого способу формування послідовностей псевдовипадкових чисел полягає в тому, що ключова послідовність подається у вигляді вектору x_0, який ініціалізує початкове значення аргументу функції скалярного добутку дивізору гіпереліптичної кривої

$f(x)=x\cdot D$,

де D - приведений дивізор гіпереліптичної кривої (загальносистемний параметр), який належить групі дивізорів гіпереліптичної кривої C_n порядку n. У якості D обирається елемент групи дивізорів гіпереліптичної кривої з якомога більшим порядком.

Наступне значення x_i аргументу функції f(x) обчислюється за допомогою пристроїв скалярного множення x_{i-1} на базовий дивізор D

$Q_i=x_{i-1}\cdot D$

та перетворення $\varphi(D)$ отриманого дивізора Q_i, $Q_i \in C_n$ за допомогою відповідних пристроїв (наприклад, x_i може дорівнюватися значенню координат точок, що належать дивізору Q_i).

Вихідні елементи послідовності псевдовипадкових чисел формуються шляхом зчитування значення функції скалярного добутку 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,

$x_i=\varphi(f(x))=\varphi(x_{i-1}\cdot D)$

Задача вираховування функції $f(x)^{-1}$, яка є зворотною до функції скалярного добутку дивізору гіпереліптичної кривої $f(x)=x\cdot D$, тобто вирахування деякого значення x_{i-1} за відомим значенням x_i, є важкорозв'язуваною теоретико-складною задачею дискретного логарифмування в групі дивізорів гіпереліптичної кривої. Щодо її вирішення на сьогоднішній день невідомо ефективних алгоритмів вираховування дискретних логарифмів для базових дивізорів великого порядку. Тому цей спосіб формування послідовностей псевдовипадкових чисел є криптографічно стійким.

При однаковій довжині ключової послідовності задача дискретного логарифмування в групі дивізорів гіпереліптичної кривої значно складніша за теоретико-складну задачу факторизації або класичну задачу дискретного логарифмування. Тому додатково введене у запропонованому способі перетворення у групі дивізорів гіпереліптичної кривої, що реалізуються за допомогою пристроїв скалярного множення дивізорів гіпереліптичної кривої, при порівняних показниках стійкості дозволяє значно скоротити довжину ключової послідовності (послідовності, що ініціює початкове значення аргументу функції) а відповідні перетворення потрібно виконувати над значно меншими числами що значно спрощує побудову відповідних пристроїв формування послідовностей псевдовипадкових чисел.

Таким чином, за рахунок додаткового введення перетворень у групі дивізорів гіпереліптичної кривої, що реалізуються за допомогою пристроїв скалярного множення дивізорів гіпереліптичної кривої, вдається значно скоротити довжину ключової послідовності та спростити побудову відповідних пристроїв формування послідовностей псевдовипадкових чисел.

Джерела інформації

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

2. Blum, L., Blum, M, Shub, M. A simple unpredictable pseudorandom number generator. // SIAM Journal on Computing, vol. 15, 1986, pp. 364 - 383.

Комп'ютерна верстка А. Крижанівський Підписне Тираж 26 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