УКРАЇНА UKRAINE

ПАТЕНТ

НА КОРИСНУ МОДЕЛЬ

№ 53792

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 **25.10.2010.**

Голова Державного департаменту інтелектуальної власності М.В. Паладій

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

(11) **53792**

(19) **UA**

(51) **МПК** (2009)
G09C 1/00

(21) Номер заявки: **u 2009 13201**

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

(24) Дата, з якої є чинними права на корисну модель: **25.10.2010**

(46) Дата публікації відомостей про видачу патенту та номер бюлетеня: **25.10.2010, Бюл. № 20**

(72) Винахідники:
Кузнецов Олександр Олександрович, UA,
Євсеєв Сергій Петрович, UA,
Рябуха Юрій Миколайович, UA,
Ковтун Владислав Юрійович, UA,
Мінухін Сергій Володимирович, 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 ключова послідовність подається у вигляді вектору, який ініціалізує початкове значення аргументу функції перетворення а вихідні елементи послідовності псевдовипадкових чисел формуються шляхом зчитування значення цієї функції за допомогою відповідних пристроїв, який **відрізняється** тим, що додатково вводять перетворення у групі точок еліптичної кривої, що реалізуються за допомогою пристроїв скалярного множення точок еліптичної кривої і дозволяють значно скоротити довжину ключової послідовності та спростити побудову відповідних пристроїв формування послідовностей псевдовипадкових чисел.

УКРАЇНА

(19) UA (11) 53792 (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) u200913201
(22) 18.12.2009
(24) 25.10.2010
(46) 25.10.2010, Бюл.№ 20, 2010 р.
(72) КУЗНЕЦОВ ОЛЕКСАНДР ОЛЕКСАНДРОВИЧ, ЄВСЕЄВ СЕРГІЙ ПЕТРОВИЧ, РЯБУХА ЮРІЙ МИКОЛАЙОВИЧ, КОВТУН ВЛАДИСЛАВ ЮРІЙОВИЧ, МІНУХІН СЕРГІЙ ВОЛОДИМИРОВИЧ
(73) ЄВСЕЄВ СЕРГІЙ ПЕТРОВИЧ
(57) Спосіб формування послідовностей псевдовипадкових чисел, який полягає у тому, що ключова послідовність подається у вигляді вектору, який ініціалізує початкове значення аргументу функції перетворення а вихідні елементи послідовності псевдовипадкових чисел формуються шляхом зчитування значення цієї функції за допомогою відповідних пристроїв, який **відрізняється** тим, що додатково вводять перетворення у групі точок еліптичної кривої, що реалізуються за допомогою пристроїв скалярного множення точок еліптичної кривої і дозволяють значно скоротити довжину ключової послідовності та спростити побудову відповідних пристроїв формування послідовностей псевдовипадкових чисел.

1

[3] 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.

2

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 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: $p \equiv 3 \bmod 4$, $g \equiv 3 \bmod 4$, $n=p \cdot q$ (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) 53792 (13) U

Недоліком способу-прототипу 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 точок еліптичної 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 точки еліптичної кривої

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

де P - базова точка еліптичної кривої (загальносистемний параметр), яка належить групі точок EC_n порядку n. У якості P обирається елемент групи точок еліптичної кривої з якомога більшим порядком.

Наступне значення x_i аргументу функції f(x) обчислюється за допомогою пристроїв скалярного множення x_{i-1} на базову точку P

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

та перетворення $\varphi(Q)$ координат отриманої точки Q_i, $Q_i \in EC_n$ за допомогою відповідних пристроїв (наприклад, x_i може дорівнюватися значенню однієї з координат точки 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,

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

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

При однаковій довжині ключової послідовності задача дискретного логарифмування в групі точок еліптичної кривої значно складніша за теоретико-складну задачу факторизації або класичну задачу дискретного логарифмування. Тому додатково введене у запропонованому способі перетворення у групі точок еліптичної кривої, що реалізуються за допомогою пристроїв скалярного множення точок еліптичної 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 точок еліптичної кривої, що реалізуються за допомогою пристроїв скалярного множення точок еліптичної кривої, вдається значно скоротити довжину ключової послідовності та спростити побудову відповідних пристроїв формування послідовностей псевдовипадкових чисел.

Можливість здійснення винаходу підтверджується визначеністю операції скалярного множення для кожної точки, яка належить групі точок EC_n еліптичної кривої. Якщо $P \in C_n$, $x \in Z^+$ (тобто x - позитивне ціле), тоді скалярне множення

де (+) - операція додавання точок еліптичної кривої, яка виконується за допомогою послідовної дії пристроїв „ДОБУТОК", „ПІДНЕСЕННЯ ДО КВАДРАТУ" та „ДОДАВАННЯ" елементів кінцевого поля, над яким визначено еліптичну криву.

На практиці для визначення суми двох точок еліптичної кривої EC над кінцевим полем $GF(2^n)$ користуються проективними координатами Лопеса-Дахаба [3]. У цьому випадку проективній точці $P=(X:Y:Z)$, $Z \neq O$, ставиться у відповідність точка з афінними координатами $(X/Z,\ Y/Z^2)$. Еліптична крива EC над $GF(2^n)$ має вигляд

$$Y^2+XYZ=X^3Z+aX^2Z^2+bZ^4,$$

де $a, b \in GF(2^n)$ при $b \neq 0$.

Процедура додавання двох точок кривої

$$P_3(X_3:Y_3:Z_3)=P_1(X_1:Y_1:Z_1)+P_2(X_2:Y_2:Z_2)$$

у проективних координатах у випадку

$$P_1(X_1:Y_1:Z_1)+P_2(X_2:Y_2:Z_2)$$

виконується згідно виразів:

$$X_3=A^2+B^2 \cdot (D+a \cdot C^2)+A \cdot D;$$

$$Y_3=Z_3 \cdot (X_3+B^2 \cdot Y_2 Z^2)+A \cdot B \cdot (X_1 Z_2 \cdot Z_3+X_3 \cdot B^2);$$

$$Z_3=D^2,$$

де

$A = Y_1 \cdot Z_2^2 + Y_2 \cdot Z_1^2$

$B=X_1 \cdot Z_2+X_2 \cdot Z_1$;

$C=Z_1 \cdot Z_2$;

у випадку

$P_1(X_1:Y_1:Z_1)=P_2(X_2:Y_2:Z_2)$

й

$P_1\left(X_1 / Z_1, Y_1 / Z_1^2\right)=P_2\left(X_2 / Z_2, Y_2 / Z_2^2\right)$

процедура додавання (подвоєння) виконується згідно виразів

$X_3= X_1^4 +b- Z_1^4$;

$Y_3 =b Z_1^4 -Z_3+X_3 \cdot (a-Z_3+ Y_1^2 +b Z_1^4)$;

$Z_3=(X_1-Z_1)^2$,

у випадку, коли одна з точок подана у проективних координатах, а інша в афінних координатах

$P_1(X_1:Y_1:Z_1)$,

$P_2(X_2:Y_2:1)$,

$P_1(X_1/Z_1, Y_1/ Z_1^2)\neq P_2(X_2/Z_2, Y_2/ Z_2^2)$

процедура додавання (у змішаних координатах) виконується згідно виразів

$X_3=A^2+A \cdot C+(C+a \cdot Z_1^2) \cdot B^2$;

$Y_3=(X_2 \cdot Z_3+X_3) \cdot AC+(X_3+Y_2 \cdot Z_3) \cdot Z_3$;

$Z_3=C^2$,

де

$A=Y_1+Y_2 \cdot Z^2$;

$B=X_1+X_2 \cdot Z_1$,

$C=Z_1 \cdot B$.

У таблиці 1 наведено кількість пристроїв „ДОБУТОК", „ПІДНЕСЕННЯ ДО КВАДРАТУ" та „ДОДАВАННЯ" елементів поля $GF(2^n)$. У таблиці позначено: «^2» - кількість операцій піднесення до квадрату; «*» - кількість операцій добутку; «+» - кількість операцій додавання.

Таблиця 1

Кількість операцій над елементами двійкового розширеного поля для виконання операцій над точками еліптичної кривої

Система координат	Загальне додавання			Загальне додавання (змішані координати)			Подвоєння		
	^2	*	+	^2	*	+	^2	*	+
Проективні координати Лопеса-Дахаба	6	15	8	4	10	8	6	5	4

Виконання послідовної дії пристроїв „ДОБУТОК", „ПІДНЕСЕННЯ ДО КВАДРАТУ" та „ДОДАВАННЯ" елементів кінцевого поля дозволяє реалізувати обчислення операцій додавання точок еліптичної кривої і, відповідно, операцій скалярного множення. Цим підтверджується можливість здійснення запропонованого винаходу, його практичної реалізації через послідовну дію відповідних пристроїв.

Джерела інформації

1. Blum, M., Micali, S. How to generate cryptographically strong sequences of pseudo-random bits. // SLAM 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.

3. J.Lopez and R. Dahab, Improved algorithms for elliptic curve arithmetic's in $Gf(2^n)$, Selected Areas in Cryptography -SAC'98, LNCS 1556, 1999, 201-212.

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