

УКРАЇНА



ПАТЕНТ

НА КОРИСНУ МОДЕЛЬ

№ 123375

**СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ
ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ ПОДОВЖЕНИХ КОДІВ**

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

Зареєстровано в Державному реєстрі патентів України на корисні моделі **26.02.2018.**

Заступник міністра економічного
розвитку і торгівлі України

М.І. Тітарчук





МІНІСТЕРСТВО
ЕКОНОМІЧНОГО
РОЗВИТКУ І ТОРГІВЛІ
УКРАЇНИ

УКРАЇНА

(19) **UA** (11) **123375** (13) **U**
(51) МПК (2018.01)
G09C 1/00

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2017 08985**
(22) Дата подання заявки: **11.09.2017**
(24) Дата, з якої є чинними права на корисну модель: **26.02.2018**
(46) Публікація відомостей про видачу патенту: **26.02.2018, Бюл.№ 4**

(72) Винахідник(и):
Євсєєв Сергій Петрович (UA),
Грищук Руслан Валентинович (UA),
Король Ольга Григорівна (UA),
Коц Григорій Павлович (UA),
Корольов Роман Володимирович (UA),
Ковтун Владислав Юрійович (UA),
Ковтун Марія Григорівна (UA),
Охріменко Андрій Олександрович (UA)
(73) Власник(и):
Євсєєв Сергій Петрович,
вул. Героїв Праці, 21-а, кв. 26, м. Харків,
61144 (UA),
Грищук Руслан Валентинович,
вул. Чуднівська, 108-в, кв. 3, м. Житомир,
10005 (UA),
Король Ольга Григорівна,
вул. Героїв Праці, 21-а, кв. 26, м. Харків,
61144 (UA),
Коц Григорій Павлович,
вул. 8-го Березня, 9-а, смт Хорошево,
Харківський р-н., 62466 (UA),
Корольов Роман Володимирович,
просп. Науки, 22-а, к. 449, м. Харків, 03028
(UA),
Охріменко Андрій Олександрович,
вул. Луначарського, 8, кв. 6, м. Васильків,
Київська обл., 08600 (UA),
Ковтун Владислав Юрійович,
вул. Олени Пчілки, 4, кв. 508, м. Київ, 02081
(UA),
Ковтун Марія Григорівна,
вул. Олени Пчілки, 4, кв. 508, м. Київ, 02081
(UA)

(54) СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ ПОДОВЖЕНИХ КОДІВ

(57) Реферат:

Спосіб криптографічного перетворення інформації з використанням модифікованих еліптичних кодів, який полягає в тому, що інформаційні дані перетворюються у кодове слово, яке маскується під випадкову послідовність (криптограму) за допомогою пристроїв кодування замаскованого лінійного блокового (n,k,d) еліптичного коду над $GF(q)$, причому в канал зв'язку надходить кодограма, сформована шляхом заміни визначених символів "обнуління" вектора ініціалізації на символи інформаційної послідовності відкритого тексту.

UA 123375 U

Запропонована корисна модель належить до галузі криптографічного захисту інформації за допомогою кодів і може бути використана в засобах шифрування у системах обробки інформації для розширення їх можливостей.

Відомий спосіб несиметричного криптографічного перетворення з використанням алгебраїчних кодів [1], який ґрунтується на тому, що відомий лінійний блоковий код маскується невиродженою матрицею X розміру $k \times k$ з елементами із $GF(q)$, діагональною матрицею D з ненульовими на діагоналі елементами із $GF(q)$, переставною матрицею P розміру $n \times n$ елементами із $GF(q)$ а інформаційні данні перетворюються у криптограму (кодове слово, що замасковане під випадкову послідовність) за допомогою пристроїв кодування замаскованого коду. Матриці X , P і D використовуються як секретний ключ, а матриця $X \cdot G \cdot P \cdot D$ - як відкритий ключ. Недоліком цього способу є те, що для криптографічного перетворення інформації необхідно зберігати великий обсяг ключових даних - для зберігання відкритого ключа, у загальному випадку, потрібно зберігати $k \times n$ елементів із $GF(q)$.

Найбільш близьким до запропонованого технічним рішенням, вибраним як прототип, є спосіб несиметричного криптографічного перетворення з використанням модифікованих алгебро-геометричних кодів [2], який полягає в тому, що маскування лінійного блокового (n, k, d) еліптичного коду над $GF(q)$ та перетворення інформаційних даних у кодове слово, яке маскується під випадкову послідовність (криптограму). Як закритий ключ для маскування коду використовується багаточлен

$$y^2z + a_1xyz + a_2yz^2 = x^3 + a_3x^2z + a_4xz + a_5z^3,$$

який задає вигляд еліптичної кривої та вигляд породжувальної матриці G еліптичного коду.

Для зберігання параметрів багаточлену кривої потрібно зберігати п'ять символів a_i із $GF(q)$, що значно менше ніж для зберігання секретних параметрів матриць X , P і D .

Недоліком способу-прототипу є значні енергетичні витрати при реалізації несиметричної крипто-кодової конструкції над $GF(2^{10} - 2^{13})$ для забезпечення безпеки інформації, яка передається.

В основу корисної моделі поставлена задача створити спосіб криптографічного перетворення інформації з використанням модифікованих алгебро-геометричних кодів, побудованих за еліптичними кривими (еліптичних кодів), який за рахунок використання вектора ініціалізації, який визначає кількість символів "обнуління" кодового слову на основі вектора ініціалізації та заміни "нулів" на символи інформаційної послідовності.

Поставлена задача вирішується за рахунок "обнуління" символів кодового слову на основі символів вектора ініціалізації та формування кодового слову, шляхом використання відповідних пристроїв, заміною "нулів" символами інформаційної послідовності.

Технічний результат, який може бути отриманий при здійсненні полягає в значному зменшенні енергетичних витрат при реалізації несиметричної крипто-кодової конструкції над $GF(2^6 - 2^8)$ та збільшенням об'єму кодограми зі збереженням стійкості несиметричної крипто-кодової конструкції.

Алгоритм формування кодограми (криптограми), що реалізовується за допомогою відповідних пристроїв кодування та полягає у виконанні наступних кроків:

1. Фіксування кінцевого поля $GF(q)$. Фіксування еліптичної кривої $y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz + a_6z^3$ і набір її точок $EC(GF(q)) : (P_1, P_2, \dots, P_N)$ над $GF(q)$. Фіксування підмножини точок $h(GF(q)) : (P_{x1}, P_{x2}, \dots, P_{xx})$, $h \subseteq EC(GF(q))$, $|h| = x$ і зберігаємо його в секреті.

2. Фіксування вектора ініціалізації $IV = EC - h_j$, h_j - інформаційні символи рівні нулю, $|h| = \frac{1}{2}k$, $I_i = 0$, $\forall I_i \in h$.

3. За введеним інформаційним вектором I формування кодового слову c . Якщо (n, k, d) код над $GF(q)$ заданий породжу вальною матрицею, то $c = I \cdot G$.

4. Формування випадкового вектора помилки є такий, що $w(e) \leq t$, $t = \lfloor (d-1)/2 \rfloor$. Отримання кодового слову шляхом додавання сформованого вектора до кодового слову:

$$C_j = \varphi_u(M_i, G_X^u) = M_i \cdot (G_X^u)^T + e.$$

5. Формування кодограми, шляхом заміни символів "обнуління" вектора ініціалізації на символи інформаційної послідовності відкритого тексту, яка надходить у канал зв'язку:

$$C_j^* = C_j - C_{k-h_j} + C_{h_j}.$$

Алгоритм розкодування кодограми (криптограми), що реалізовується за допомогою відповідних пристроїв кодування, та полягає у виконанні наступних кроків:

1. Введення кодограми, що підлягає розкодування шляхом заміни символи подовження на

10 нульові інформаційні символи: $C_j^* = C_{h_j} \rightarrow C_{k-h_j}$.

2. Розкодування отриманого вектора у відповідних пристроях за алгоритмом Берлекемпа-Мессі: $C = M_i \cdot (X^u)^T \cdot (G^{BC})^T + e \cdot (D^u)^{-1} \cdot (P^u)^{-1}$, кодограма - суть кодове слово з помилками еліптичного коду. Вага вектора помилок $w(e) \leq t$.

3. Формування інформаційного вектора. Для цього у відповідних пристроях отриманий

15 результат розкодування $M_i \cdot (X^u)^T$ слід помножити на $(X^u)^{-1} : (M_i \cdot (X^u)^T) \cdot (X^u)^{-1} = M_i$.

Таким чином використовуючи вектор ініціалізації при формуванні кодограми забезпечується "обнуління" символів кодового слова та побудова кодограми шляхом заміни визначених символів "нулів" на символи інформаційної послідовності відкритого тексту, що забезпечує зменшення енергетичних витрат при реалізації несиметричної крипто-кодової конструкції, збільшення об'єму кодограми при збереженні рівня стійкості.

Джерела інформації:

1. R.J. McEliece. A Public-Key Cryptosystem Based on Algebraic Theory. // DGN Progres Report 42-44, Jet Propulsi on Lab. Pasadena, CA. January - February, 1978. - P. 114-116.

25 2. Yevseiev S. Development of mceliece modified asymmetric crypto-code system on elliptic truncated codes // S. Yevseiev, K. Rzayev, O. Korol, Z. Imanova / Eastern-European Journal of Enterprise Technologies. - Kharkiv. - 2016. - V. 4. 9 (82). - P. 18-26.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

30 Спосіб криптографічного перетворення інформації з використанням модифікованих еліптичних кодів, який полягає в тому, що інформаційні дані перетворюються у кодове слово, яке маскується під випадкову послідовність (криптограму) за допомогою пристроїв кодування замаскованого лінійного блокового (n,k,d) еліптичного коду над $GF(q)$, який **відрізняється** тим,

35 що в канал зв'язку надходить кодограма, сформована шляхом заміни визначених символів "обнуління" вектора ініціалізації на символи інформаційної послідовності відкритого тексту.