**УКРАЇНА**

**(19) UA (11) 147560 (13) U**

**(51)** МПК (2021.01)
**G09C 1/00**
***H04L 9/16*** (2006.01)

**НАЦІОНАЛЬНИЙ ОРГАН ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ**
**ДЕРЖАВНЕ ПІДПРИЄМСТВО "УКРАЇНСЬКИЙ ІНСТИТУТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ"**

## (12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

**(21)** Номер заявки: **u 2020 08363**

**(22)** Дата подання заявки: **28.12.2020**

**(24)** Дата, з якої є чинними права інтелектуальної власності: **20.05.2021**

**(46)** Публікація відомостей про державну реєстрацію: **19.05.2021, Бюл.№ 20**

**(72)** Винахідник(и):
**Авраменко Віктор Васильович (UA),**
**Бондаренко Микита Олегович (UA),**
**Лаврик Тетяна Володимирівна (UA)**

**(73)** Володілець (володільці):
**СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ**, вул. Римського-Корсакова, буд. 2, м. Суми, 40007 (UA)

**(74)** Представник:
**ГУДКОВ СЕРГІЙ МИКОЛАЙОВИЧ**

# (54) СПОСІБ ШИФРУВАННЯ ДАНИХ ЗА ДОПОМОГОЮ СУМИ ФУНКЦІЙ ДІЙСНОЇ ЗМІННОЇ

**(57)** Реферат:

Спосіб шифрування даних за допомогою суми функцій дійсної змінної, який полягає в тому, що для шифрування як ключ застосовують математичну функцію дійсної змінної. Кожний із елементів вхідного повідомлення шифрують за допомогою суми функцій дійсних змінних, отриманих при однаковому кроці зміни аргументу функцій-ключів дійсної змінної.

UA 147560 U

Корисна модель належить до галузі електрозв'язку і обчислювальної техніки та систем передачі інформації із використанням симетричних закритих ключів.

В основному алгоритми криптографії із закритими ключами використовують функції перестановок та підстановок і не використовують математичні функції на множині дійсних чисел.

Як аналог розглядаються асиметричні криптосистеми. До них належить криптосистема RSA, яка використовує функцію піднесення в степінь [С. Коутинхо. Введение в теорию чисел. Алгоритм RSA. Москва: Постмаркет. 2001.-с.18-21]. Недоліком цього способу є необхідність вибору ключів довжини не менше 1024-2048 бітів, що зменшує швидкість роботи алгоритму, та вимагає вибору двох великих простих чисел, що є досить громіздким завданням.

Аналогом способу, що заявляється є "Спосіб шифрування даних із використанням функції дійсної змінної" [Патент України №143734, МПК H041 9/00, заявл. 20.02.2020, опубл. 10.08.2020]. Недоліком цього способу є використання лише однієї функції дійсної змінної як ключа, що полегшує спробу зламати криптосистему.

Найбільш близьким за способом, що заявляється, є "Спосіб шифрування даних" [Патент України №42957, H041 9/00, заявл. 16.03.2009, опубл. 27.07.2009]. В ньому використовуються як ключі m математичних функцій на множині дійсних чисел. Шифрування інформації здійснюється за допомогою суми функцій-ключів із випадковими коефіцієнтами перед ними. В залежності від символу, що шифрується, в цю суму входили тільки певні функції-ключі. На приймальній стороні, за допомогою обчислення функцій непропорційності по похідній першого порядку визначалися, які із цих функцій входять в суму і по цьому відбувалося дешифрування.

Цей спосіб має недолік. Внаслідок використання для дешифрування функції непропорційності, по похідній першого порядку, виникає необхідність застосовувати чисельні методи для отримання похідних. Це значно ускладнює алгоритм криптосистеми і призводить до того, що шифр значно перевищує довжину повідомлення.

В основу корисної моделі поставлена задача розробки способу шифрування на основі m функцій-ключів на множині дійсних чисел, який не потребує обчислення похідних, створює більш коротке зашифроване повідомлення, має відносно простий алгоритм, і при цьому забезпечує високу крипостійкість.

Поставлена задача вирішується тим, що спосіб шифрування даних, за допомогою суми функцій дійсної змінної, який полягає в тому, що для шифрування як ключа застосовують математичну функцію дійсної змінної. Кожний із елементів вхідного повідомлення шифрують за допомогою суми функцій дійсних змінних, отриманих при однаковому кроці зміни аргументу функцій-ключів дійсної змінної, при цьому значення матриці з вхідних повідомлень та функцій-ключів дійсної змінної розраховують:

$$y(j,i) = \sum_{q=1}^{m} k_{qj} f_q(i),$$

де $y(j,i)$ - значення елементів матриці шифрів вхідних повідомлень,

$j = 1,2,...T$ - номер елемента з масиву вхідного повідомлення,

$T$ - розмір масиву елементів вхідного повідомлення,

$i = 1,2,\cdots N \geq 2^m$ - масив значень функцій ключів,

$N$ - кількість елементів масиву, який є шифром вхідного символу,

$f_q(i) = f_q(ih)$ - значення q-ї функції-ключа при аргументі $ih$,

$h$ - постійний крок зміни аргументу,

$q = 1,2,...m$ - номер функції-ключа,

$m$ - кількість функцій-ключів,

$k_{qj}$ - коефіцієнти, які генерують під час шифрування j-го елемента і можуть бути або рівними нулю, або генерують, як випадкові числа і невідомі одержувачу, а також при дешифруванні j-го елемента повідомлення використовують інтегральні функції непропорційності першого порядку $y(j,i)$ по одній із довільно вибраних функції-ключа $f_1(i)$, непропорційності усіх інших $m-1$ функцій-ключів по $f_1(i)$, а також непропорційності одних, раніше обчислених, непропорційності по інших, які мають вигляд:

$$@I\ {}^{(1)}_{f_1^{(i)}}\ y(j,i)=\frac{y(j,i-1)+y(j,i)}{f_1(i-1)+f_1(i)}-\frac{y(j,i)}{f_1(i)},$$

де $@I\ {}^{(1)}_{f_1^{(i)}}\ y(j,i)$ – позначення інтегральної непропорційності першого порядку,

$f_1(i)$ - довільно задана функція-ключ.

Завдяки такому рішенню, зникає необхідність застосування чисельних методів отримання похідних, стає простішим алгоритм, зменшується довжина зашифрованого повідомлення. При цьому залишається висока криптостійкість системи при атаці методом підбирання, завдяки тому, що для перехоплення потрібно не тільки підібрати види усіх функцій-ключів, але і значення їхніх параметрів. На множині дійсних чисел такий підбір набагато складніший, ніж для цілих чисел.

Високій криптостійкості також сприяє те, що один і той же елемент шифрується по-різному в залежності від його порядкового номеру в повідомленні.

Спосіб здійснюється таким чином.

Вибирають m функцій-ключів дійсної змінної $f_q(x)$, q=1,2,…m. Вони можуть бути як дискретними, так і неперервними. Якщо функції-ключі неперервні, отримують одновимірні масиви $f_q(i)$ q=1,2,…m розміром N значень, шляхом обчислення їхніх значень для x=ih, де i=1,2,…N≥$2^m$, а h - крок, із яким змінюється аргумент x. Цей крок повинен бути однаковим для всіх функцій-ключів. Якщо елементи повідомлення представлені цілими числами, то вибирають h=1.

Попередньо передавальна та приймальна сторони узгоджують нумерацію функцій-ключів, а також, сумою яких із них шифрують символи алфавіту, які застосовують. Тобто кожний символ представляють у вигляді бінарного коду, в якому для забезпечення криптостійкості не менше двох одиниць. Таким чином в шифрі будь-якого символу присутні не менше двох функцій-ключів із випадковими коефіцієнтами.

Шифрування повідомлення (1):

1. Обчислюють масиви з N≥$2^m$ значень функцій-ключів $f_q(x)$, q=1,2,…m.

2. Зчитують із файла або вводять із клавіатури послідовність елементів повідомлення. В залежності від того, яким символом представлений j-й елемент, для кожної функції-ключа генерується або нуль, або випадкове число, яке відрізняється від нуля. Обчислюють шифр j-го елемента у вигляді масиву з N значень y(j, i), i=1,2,…N:

$y(j,i)=k_{1j}f_1(i)+k_{2j}f_2(i)+\ldots+k_{mj}f_m(i)$, (3)

де i=1,2,…N, N - кількість елементів у повідомленні.

Послідовність отриманих масивів для кожного елемента передають по відкритому каналу зв'язку.

Дешифрування:

1. Обчислюють масиви з N≥$2^m$ значень функцій-ключів $f_q(x)$, q=1,2,…m.

2. Отримують із каналу зв'язку T одновимірних масивів, в кожному із яких по N-значень y(j, i), j=1,2,…T, i=1,2,…N.

В подальшому, з метою спрощення, процес дешифрування приводиться на прикладі, коли використовують лише три функції-ключі: $f_1(x)$, $f_2(x)$, $f_3(x)$. Тобто m=3. Відповідно j-й елемент повідомлення шифрується як:

$y(j,i)=k_{1j}f_1(i)+k_{2j}f_2(i)+k_{3j}f_3(i)$, i=1,2,…N=$2^3$=8.

3. Обчислюють масив не пропорційностей (2) по $f_1(i)$:

$$F_{01}(j,i)=@I\ {}^{(1)}_{f_1^{(i)}}\ y(j,i)=\frac{y(j,i-1)+y(j,i)}{f_1(i-1)+f_1(i)}-\frac{y(j,i)}{f_1(i)},\quad (4)$$

де i=2,3,…N.

Також обчислюють непропорційності:

$$F_{r1}(j,i)=@I\ {}^{(1)}_{f_1^{(i)}}\ f_r(j,i)=\frac{f_r(j,i-1)+f_r(j,i)}{f_1(i-1)+f_1(i)}-\frac{f_r(j,i)}{f_1(i)},\quad \partial e\, r=2,3. \quad (5)$$

Враховуючи, що непропорційність функції відносно самої себе нульова, отримують:

$$F_{01}(j,i)=k_{2j}F_{21}(j,i)+k_{3j}F_{31}(j,i). \quad (6)$$

4. Обчислюють непропорційність:

$$F_{0121}(j,i) = @I^{(1)}_{F_{21}(j,i)} F_{01}(j,i) = \frac{F_{01}(j,i-1)+F_{01}(j,i)}{F_{21}(j,i-1)+F_{21}(j,i)} - \frac{F_{01}(j,i)}{F_{21}(i)}, \quad (7)$$

$$F_{3121}(j,i) = @I^{(1)}_{F_{21}(j,i)} F_{31}(j,i) = \frac{F_{31}(j,i-1)+F_{31}(j,i)}{F_{21}(j,i-1)+F_1(j,i)} - \frac{F_{31}(j,i)}{F_{21}(i)}, \quad (8)$$

$$F_{0121}(j,i) = k_{3j} F_{3121}(j,i). \quad (9)$$

Як видно із (9), між $F_{0121}(j, i)$ та $F_{3121}(j, i)$ існує пропорціональний зв'язок. Внаслідок цього непропорційність $F_{0121}(j, i)$ по $F_{3121}(j, i)$

$$F_{01213121}(j,i) = @I^{(1)}_{F_{3121}(j,i)} F_{0121}(j,i) = \frac{F_{0121}(j,i-1)+F_{0121}(j,i)}{F_{3121}(j,i-1)+F_{3121}(j,i)} - \frac{F_{0121}(j,i)}{F_{3121}(i)} = 0. \quad (10)$$

Цей факт дозволяє обчислити $k_{3j}$ із (9) а також $k_{2j}$ $k_{1j}$ для j-го елемента повідомлення.

$$k_{3j} = \frac{F_{0121}(j,i)}{F_{3121}(i)}, \quad (11)$$

$$k_{2j} = \frac{F_{01}(j,i) - k_{3j} F_{31}(j,i)}{F_{21}(i)}, \quad (12)$$

$$k_{1j} = \frac{y(j,i) - k_{2j} f_2(i) - k_{3j} f_3(i)}{f_1(i)}, \quad (13)$$

В залежності від того, які із цих коефіцієнтів ненульові, а які дорівнюють нулю, відбувається дешифрування j-го елемента повідомлення.

На практиці необхідно враховувати, що є похибки обчислення. Тому обчислену, на останньому етапі, непропорційність (10) порівнюють по модулю не строго із нулем, а з наближеним до нього числом ε. Наприклад, це може бути $\varepsilon=10^{-4}$. Наприклад і, якщо $|F_{01213121}(j, i)|\leq\varepsilon$, то вважають, що вона нульова. Його значення визначають під час тестування криптосистеми. Теоретично, ця непропорційність дорівнює нулю для усіх i=2,3,…N, але, враховуючи похибки обчислення, рекомендується розрахунки по формулах (11-13) робити для і, при якому модуль непропорційності (10) мінімальний.

Обмеження на ключові функції:

1. Функція задається на множині дійсних чисел.

2. Функція не повинна бути константою і не приймати нульові значення.

3. При використанні функції-ключа не повинна виникати ситуація, коли відбувається ділення на число, наближене до нуля, що призводить до появи неприйнятної похибки обчислення. З цією метою рекомендується протестувати криптосистему для всього алфавіту символів, які застосовують в повідомленнях.

4. Перед відправленням зашифрованого повідомлення попередньо перевіряють як виглядає дешифроване, щоб уникнути помилок, які можуть трапитися внаслідок неврахування попередніх пунктів.

Приклад роботи способу шифрування:

Розглядається приклад шифрування бінарного коду, коли достатньо шифрувати символи "0", "1", « »- пропуск та «\n" - перехід на інший рядок. Будь-який інший символ буде сприйматися як перехід на інший рядок "/n".

Нехай функції-ключі мають вигляд:

$$f_1(x) = 100\sin\sin\left((\alpha_1-\beta_1)x\right)\cos\cos(15\beta_1 x);$$

$$f_2(x) = 100\exp\exp(0{,}1\alpha_2 x)\sin\sin(10\beta_2 x)\cos\cos\left((\alpha_2+\beta_2)x\right);$$

$$f_3(x) = 100\exp\exp(-\alpha_3 x)\sin\sin(400\beta_3 x),$$

де $\alpha_1=1$, $\alpha_2=0{,}15$, $\alpha_3=0{,}5$, $\beta_1=0{,}1$, $\beta_2=1{,}5$, $\beta_3=0{,}7$, x=ih, i=1,2,…8, h=1.

При шифруванні символу в суму (3) входять не менше двох функцій-ключів, які помічені одиницею в табл. 1.

Таблиця 1

| Символ | $f_1$ | $f_2$ | $f_3$ |
|---|---|---|---|
| «0» | 0 | 1 | 1 |
| «1» | 1 | 1 | 1 |
| « » | 1 | 1 | 0 |
| “\n” | 1 | 0 | 1 |

Коефіцієнти при них вибираються випадковими в межах від нуля до одиниці із рівномірним законом розподілу. за допомогою відповідної функції в комп'ютерній програмі.

Робота криптосистеми може бути ілюстрована прикладом. Шифрується повідомлення у вигляді послідовності бінарних ASCII-кодів букв A, B, C, D, O із пропусками, переходами на наступний рядок та символами z, p, які теж сприймаються, як "\n".

Оригінальне повідомлення:

z01000001 01000010p 01000011

01000100

01001111

Результати дешифрування:

01000001 01000010

01000011

01000100

01001111

Очевидно, що прийняте повідомлення цілком збігається із відправленим.

Наступний приклад ілюструє шифрування однакових елементів повідомлення.

В табл. 2 приведені одновимірні масиви, які є шифром, розміщених у повідомленні рядом двох нулів та двох одиничок.

Таблиця 2

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| “0” | -0,12669 | 1,16394 | 0,05489 | -0,27695 | 0,076085 | -0,9544 | -0,37939 | 0,621132 |
| “0” | -1,86653 | 34,6256 | 3,65796 | -10,0606 | 3,11164 | -30,6907 | -11,9794 | 19,7775 |
| “1” | -11,3619 | 1,70127 | -11,5307 | -14,6593 | -13,8983 | 6,90854 | -8,58664 | 36,5966 |
| “1” | -23,5254 | 76,641 | -12,392 | -17,4283 | -6,72795 | -47,3575 | -26,111 | 54,3673 |

Із неї видно, що однакові символи шифруються по-різному. Ця властивість значно ускладнює можливість "зламати" систему.

Також розглядається випадок, коли стороні, яка намагається зламати систему, став відомий вид функцій-ключів і залишається тільки підібрати значення констант, маючи перехоплене зашифроване повідомлення. При цьому у функції-ключа $f_3$, замість константи 400, було при дешифруванні підібрано значення 400,0001. В цьому випадку, замість кодів букв A, B, C, D, O, отримується наступний результат:

01111111 11111111 1111111111111111

Якщо у функції-ключа $f_2$, замість $\sin\sin(10\beta_2 x)$ дешифруванні буде $\sin\sin(9{,}9999\beta_2 x)$, а всі інші параметри правильні, це приведе до того, що відповідь буде складатися тільки із одиниць.

Наведений приклад свідчить про високу стійкість способу шифрування, який пропонується.

## ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Спосіб шифрування даних за допомогою суми функцій дійсної змінної, який полягає в тому, що для шифрування як ключ застосовують математичну функцію дійсної змінної, який **відрізняється** тим, що кожний із елементів вхідного повідомлення шифрують за допомогою суми функцій дійсних змінних, отриманих при однаковому кроці зміни аргументу функцій-ключів дійсної змінної, при цьому значення матриці з вхідних повідомлень та функцій-ключів дійсної змінної розраховують:

$$y(j,i) = \sum_{q=1}^{n} k_{qj} f_q(i),$$

де $y(j,i)$ - значення елементів матриці шифрів вхідних повідомлень,

$j = 1,2,...T$ - номер елемента з масиву вхідного повідомлення,

$T$ - розмір масиву елементів вхідного повідомлення,

$i = 1,2,\cdots N \geq 2^m$ - масив значень функцій ключів,

$N$ - кількість елементів масиву, який є шифром вхідного символу,

$f_q(i) = f_q(ih)$ - значення q-ї функції-ключа при аргументі $ih$,

$h$ - постійний крок зміни аргументу,

$q = 1,2,...m$ - номер функції-ключа,

$m$ - кількість функцій-ключів,

$k_{qj}$ - коефіцієнти, які генерують під час шифрування j-го елемента і можуть бути або рівними нулю, або генерують, як випадкові числа і невідомі одержувачу, а також при дешифруванні j-го елемента повідомлення використовують інтегральні функції непропорційності першого порядку $y(j,i)$, по одній із довільно вибраних функції-ключа $f_1(i)$, непропорційності усіх інших $m-1$ функцій-ключів по $f_1(i)$, а також непропорційності одних, раніше обчислених, непропорційності по інших (1), які мають вигляд

$$@I^{(1)}_{f_1(i)} y(j,i) = \frac{y(j,i-1) + y(j,i)}{f_1(i-1) + f_1(i)} - \frac{y(j,i)}{f_1(i)},$$

де $@I^{(1)}_{f_1(i)} y(j,i)$ - позначення інтегральної непропорційності першого порядку,

$f_1(i)$ - довільно задана функція-ключ.

Комп'ютерна верстка І. Скворцова

ДП “Український інститут інтелектуальної власності”, вул. Глазунова, 1, м. Київ – 42, 01601