ДЕРЖАВНА СЛУЖБА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ УКРАЇНИ

УКРАЇНА **(19) UA** **(11) 102987** **(13) U**

(51) МПК (2015.01)
G09C 1/00

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2015 05650**

(22) Дата подання заявки: **08.06.2015**

(24) Дата, з якої є чинними права на корисну модель: **25.11.2015**

(46) Публікація відомостей про видачу патенту: **25.11.2015, Бюл.№ 22**

(72) Винахідник(и):
Баришев Юрій Володимирович (UA),
Комаров Андрій Олегович (UA)

(73) Власник(и):
ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ,
Хмельницьке шосе, 95, м. Вінниця, 21021 (UA)

(54) СПОСІБ ПАРАЛЕЛЬНОГО КЛЮЧОВОГО ГЕШУВАННЯ ДАНИХ ТЕОРЕТИЧНО ДОВЕДЕНОЇ СТІЙКОСТІ

(57) Реферат:

Спосіб паралельного ключового гешування даних теоретично доведеної стійкості полягає в тому, що інформаційні дані M подають у вигляді послідовності $M=\{m_1, m_2 \ldots m_i\}$, подають ключові дані K. Гешування інформаційних даних виконують шляхом піднесення до степеня за модулем за допомогою пристрою піднесення до степеня за модулем. Задача зламу ключа гешування зводиться до обчислення дискретного логарифма в полі простого числа. Підносять до степеня, який є результатом додавання значення і-го елемента інформаційної послідовності m_i (i=1, 2,…, 1), значення блоку даних, номер якого відрізняється від і на значення псевдовипадкового числа, яке обчислюють за допомогою пристрою генерування псевдовипадкових значень адреси на основі значення і-го елемента інформаційної послідовності m_i та значення (i-l)-го елемента інформаційної послідовності m_{i-1}, значення суми результатів гешування попереднього елемента інформаційної послідовності та значення секретного числа k_j.

UA 102987 U

Корисна модель належить до галузі криптографічного захисту інформації і може бути використана при розробці механізмів забезпечення цілісності даних.

Відомий спосіб ключового хешування теоретично доведеної стійкості [Патент України № 50818 від 25.06.2010 р., М. кл. G09C 1/00, бюл. № 12, 2010 р.], який полягає в тому, що інформаційні дані M подають у вигляді послідовності $M=\{m_1, m_2 \ldots m_i\}$, ключові дані K подають у вигляді великого секретного числа k, а гешування інформаційних даних виконують шляхом піднесення до степеня за модулем великого простого числа p за допомогою пристрою піднесення до степеня за модулем, велике секретне число k використовують як початкове заповнення h_0, задача зламу ключа гешування зводиться до обчислення дискретного логарифма в простому полі, підносять велике число g, яке є примітивним коренем за модулем p, степінь, до якого виконують піднесення, є результатом додавання значення елемента інформаційної послідовності m_i та результату гешування, в подальшому гешування, попереднього елемента інформаційної послідовності.

Недоліком цього способу є недостатня обчислювальна швидкість гешування, оскільки для піднесення w-розрядного великого числа g за допомогою w-розрядного пристрою піднесення до степеня за модулем ($n=w \cdot q$, $q \geq 1$) необхідно виконати $O(q^2)$ операцій піднесення до степеня для кожного елемента інформаційної послідовності m_i.

Найбільш близьким до способу, що пропонується, є спосіб паралельного ключового гешування даних теоретично доведеної стійкості [Патент України № 94039 від 27.10.2014 р., М. кл. G 09 C 1/00, бюл. № 20, 2014 р.], який полягає в тому, що інформаційні дані M подають у вигляді послідовності $M=\{m_1, m_2, \ldots, m_i\}$, подають ключові дані K, гешування інформаційних даних виконують шляхом піднесення до степеня за модулем за допомогою пристрою піднесення до степеня за модулем, задача зламу ключа гешування зводиться до обчислення дискретного логарифму в полі простого числа, підносять число, яке є примітивним коренем за модулем, причому ключові дані K подають у вигляді послідовності секретних чисел $\{k_1, k_2, \ldots, k_q\}$, підносять кожне з q великих чисел g_j (j=1, 2,…, q), яке є примітивним коренем за відповідним модулем p_i, до степеня, який є результатом додавання значення елемента інформаційної послідовності m_i, випадкового значення суми результатів гешування попереднього елемента інформаційної послідовності та значення секретного числа k_i.

Недоліком найближчого аналога є недостатня стійкість гешування, оскільки для зламу необхідно лише знаходження ключа, яке зводиться до знаходження m_1 блока даних.

В основу корисної моделі поставлена задача створити спосіб ключового гешування теоретично доведеної стійкості, який дозволить забезпечити підвищену обчислювальну стійкість гешування інформації за рахунок ускладнення задачі зламу ключа гешування шляхом введення додаткових операцій.

Поставлена задача вирішується тим, що інформаційні дані M подають у вигляді послідовності $M=\{m_1, m_2, \ldots, m_i\}$, подають ключові дані K, гешування інформаційних даних виконують шляхом піднесення до степеня за модулем за допомогою пристрою піднесення до степеня за модулем, задача зламу ключа гешування зводиться до обчислення дискретного логарифма в полі простого числа, підносять число, яке є примітивним коренем за модулем, згідно з корисною моделлю, ключові дані K подають у вигляді послідовності секретних чисел $\{k_1, k_2, \ldots, k_q\}$, підносять кожне з q великих чисел g_j (j=1, 2,…, q), яке є примітивним коренем за відповідним модулем p_i, до степеня, який є результатом додавання значення і-го елемента інформаційної послідовності m_i (i=1, 2,…, l), значення блока даних, номер якого відрізняється від і на значення псевдовипадкового числа, яке обчислюють за допомогою пристрою генерування псевдовипадкових значень адреси на основі значення і-го елемента інформаційної послідовності m_i та значення (i-l)-го елемента інформаційної послідовності m_{i-l}, значення суми результатів гешування попереднього елемента інформаційної послідовності та значення секретного числа k_i.

Технічний результат, який може буде отриманий при здійсненні корисної моделі, полягає в підвищенні складності задачі зламу ключа гешування без збільшення розрядності геш-функції.

На кресленні наведена схема пристрою, що реалізує спосіб паралельного ключового гешування даних теоретично доведеної стійкості.

Пристрій містить лічильник 1, вихід якого з'єднано першим входом першого блока додавання 2 та з першим входом першого блока комутації 3, вихід якого з'єднано з другим входом першого блока комутації 3. Вихід першого блока комутації 3 є входом оперативно запам'ятовуючого пристрою 4, вихід якого є третім входом (j+l)-го пристрою додавання 8_j ($j \in N$, $j \in [1; q]$), входом блока зберігання попереднього елемента інформаційної послідовності 11 та першим входом пристрою генерування псевдовипадкових значень адреси 12, вихід якого є другим входом першого блока додавання 2. Другим входом пристрою генерування

псевдовипадкових значень адреси 12 є вихід блока зберігання попереднього елемента інформаційної послідовності 11. Першим входом (j+1)-го пристрою додавання 8_i є вихід (q+2)-го пристрою додавання 10, а другим - вихід блока зберігання j-ї частини ключа 5_i. Вихід (j+1)-го пристрою додавання 8_i з'єднано з першим входом j-го пристрою піднесення до степеня за модулем 9_i. Другим входом j-го пристрою піднесення до степеня за модулем 9_i є вихід блока зберігання j-го значення модуля 6_i, а третім - вихід блока зберігання j-го примітивного елемента 7_i.

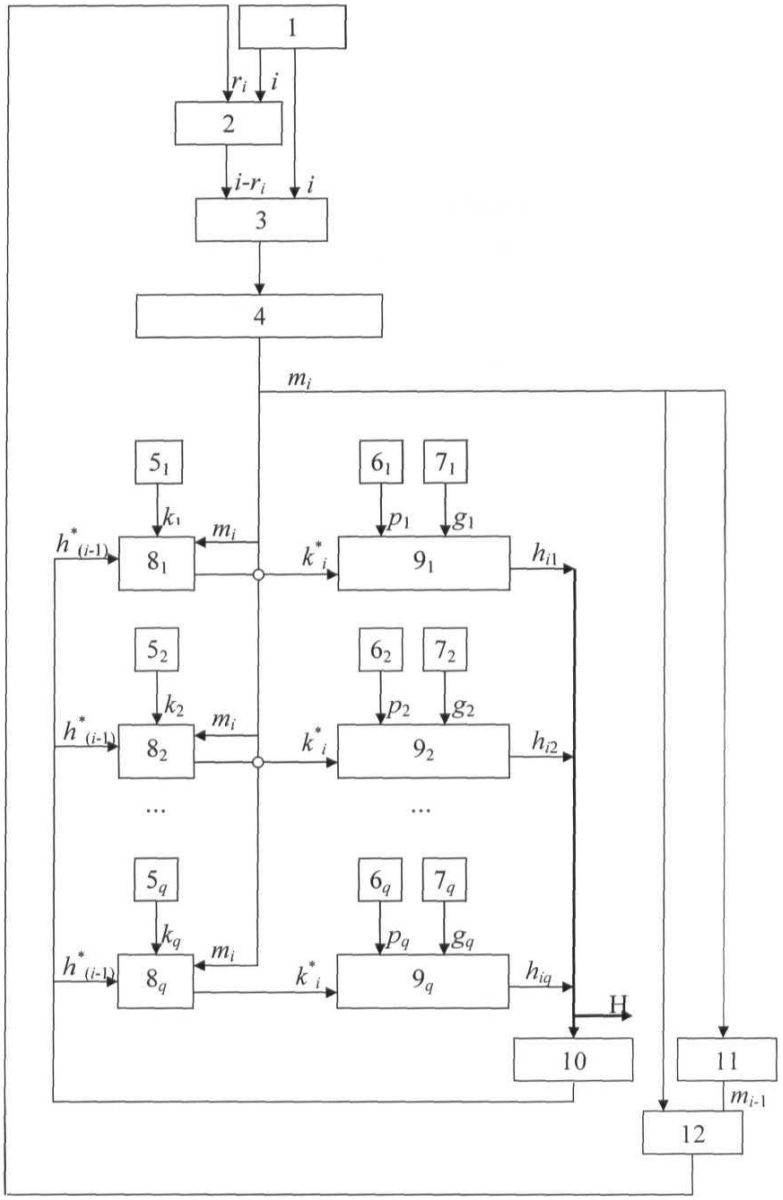
Вихід j-го пристрою піднесення до степеня за модулем 9_i, є j-м входом (q+2)-го пристрою додавання 10 та j-м виходом всього пристрою.

Спосіб паралельного ключового гешування даних теоретично доведеної стійкості виконується на пристрої таким чином. В блок зберігання j-ї частини ключа 5_i надсилають значення j-ї частини ключа k_i, в блок зберігання j-го значення модуля 6_i - значення j-го модуля p_i, блок зберігання j-го примітивного елемента 7_i - значення примітивного елемента g_i за модулем p_i. В оперативно запам'ятовуючий пристрій 4 заносять інформаційні дані, що підлягають гешуванню, представлені у вигляді послідовності $\{m_1, m_2 \ldots m_i\}$, а лічильник 1 встановлюють в положення, що відповідає початковій адресі оперативно запам'ятовуючого пристрою 4, де зберігається перший елемент інформаційної послідовності m_1. Вихід (q+2)-го пристрою додавання 10 встановлюють рівним нулю. В блок зберігання попереднього елемента інформаційної послідовності 11 заносять значення останнього елемента інформаційної послідовності m_1. Починають ітеративний процес. З виходу лічильника 1 отримують адресу i-го елемента інформаційної послідовності m_i та через блок комутації 3 надсилають її до оперативно запам'ятовуючого пристрою 4, з виходу якого отримують значення i-го елемента інформаційної послідовності m_i, яке надсилають на вхід блока зберігання попереднього елемента інформаційної послідовності 11, пристрою генерування псевдовипадкових значень адреси 12 та на третій вхід (j+l)-го пристрою додавання 8_i, в якому це значення зберігається. З виходу пристрою генерування псевдовипадкових значень адреси 12 отримують значення зміщення адреси r_i, яке віднімають від вихідного значення лічильника 1 за модулем l за допомогою першого блока додавання 2. Отримане значення адреси через блок комутації 3 надсилають до оперативно запам'ятовуючого пристрою 4, з виходу якого отримують значення (i-r_i)modl-го елемента інформаційної послідовності $m_{(i-r_i) \bmod l}$, яке надсилають до входу (j+1)-го пристрою додавання 8_i. За допомогою (j+1)-го пристрою додавання 8_i додають значення (i-r_i)modl-го елемента інформаційної послідовності $m_{(i-r_i) \bmod l}$, значення i-го елемента інформаційної послідовності m_i, значення $h^*_{(i-1)}$, яке отримують з виходу (q+2)-го пристрою додавання 10, та значення j-ї частини ключа k_i, яке отримують з виходу блока зберігання j-ї частини ключа 5_i. Значення показника степеня k^*_{ij}, отримане з виходу (j+1)-го пристрою додавання 8_i надсилають на перший вхід j-го пристрою піднесення до степеня за модулем 9_i, де виконують піднесення значення примітивного елемента g_i за модулем p_i, отриманого з виходу блока зберігання j-го примітивного елемента 7_i, до степеня k^*_{ij}, за модулем p_i, значення якого отримують з виходу блока зберігання j-го значення модуля 6_i. Значення результату піднесення до степеня за модулем h_{ii}, отримане з виходу j-го пристрою піднесення до степеня за модулем 9_i надсилають на j-й вхід (q+2)-го пристрою додавання 10. За допомогою (q+2)-го пристрою додавання 10 додають q значень результатів піднесення до степеня. Якщо i≠1, то змінюють положення лічильника 1 відповідно адреси (i+1)-го елемента інформаційної послідовності та починають наступну ітерацію, інакше зупиняють ітеративний процес. Після l-ї ітерації частину результуючого геш-значення h_{li} отриману на виході j-го пристрою піднесення до степеня за модулем 9_j надсилають на j-й вихід всього пристрою.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Спосіб паралельного ключового гешування даних теоретично доведеної стійкості, який полягає в тому, що інформаційні дані M подають у вигляді послідовності $M=\{m_1, m_2 \ldots m_i\}$, подають ключові дані K, гешування інформаційних даних виконують шляхом піднесення до степеня за модулем за допомогою пристрою піднесення до степеня за модулем, задача зламу ключа гешування зводиться до обчислення дискретного логарифма в полі простого числа, ключові дані K подають у вигляді послідовності секретних чисел $\{k_1, k_2, \ldots, k_q\}$, підносять кожне з q великих чисел g_j (j=1, 2,…, q), яке є примітивним коренем за відповідним модулем p_j, який **відрізняється** тим, що підносять до степеня, який є результатом додавання значення i-го

елемента інформаційної послідовності m_i (i=1, 2,…, 1), значення блока даних, номер якого відрізняється від і на значення псевдовипадкового числа, яке обчислюють за допомогою пристрою генерування псевдовипадкових значень адреси на основі значення і-го елемента інформаційної послідовності m_i та значення (i-l)-го елемента інформаційної послідовності m_{i-1}, значення суми результатів гешування попереднього елемента інформаційної послідовності та значення секретного числа k_j.



Комп'ютерна верстка І. Скворцова

Державна служба інтелектуальної власності України, вул. Василя Липківського, 45, м. Київ, МСП, 03680, Україна

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