УКРАЇНА

(19) UA (11) 117326 (13) U

(51) МПК (2017.01)
G09C 1/00

МІНІСТЕРСТВО ЕКОНОМІЧНОГО РОЗВИТКУ І ТОРГІВЛІ УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2016 13377**

(22) Дата подання заявки: **26.12.2016**

(24) Дата, з якої є чинними права на корисну модель: **26.06.2017**

(46) Публікація відомостей про видачу патенту: **26.06.2017, Бюл.№ 12**

(72) Винахідник(и):
Баришев Юрій Володимирович (UA)

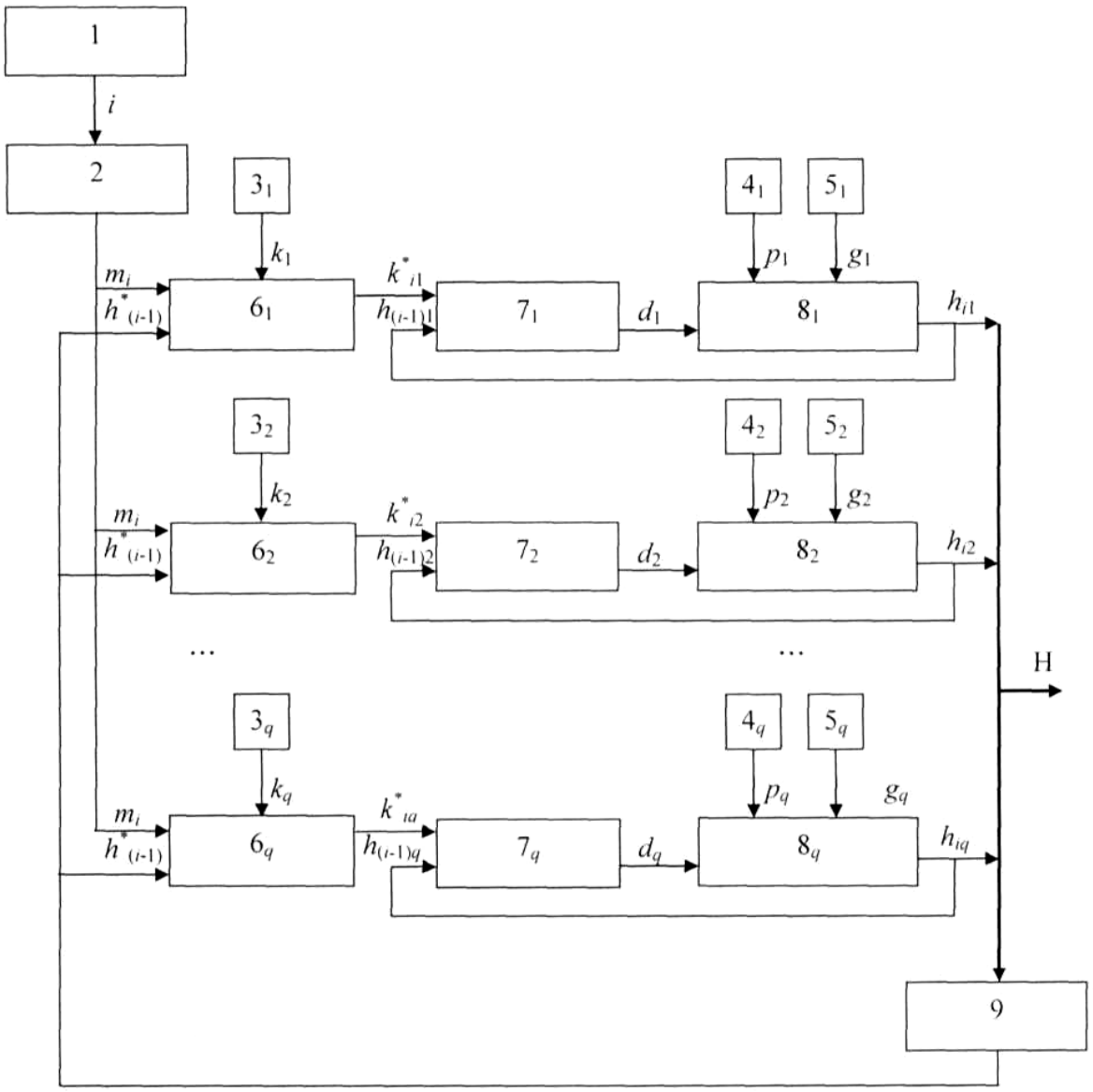
(73) Власник(и):
ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ,
Хмельницьке шосе, 95, м. Вінниця, 21021 (UA)

(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 у вигляді послідовності секретних чисел $\{k_1, k_2, \ldots, k_q\}$, гешування інформаційних даних виконують шляхом піднесення кожного з q великих чисел g_j (j=1, 2, …, q), яке є примітивним коренем за відповідним модулем p_j до степеня, за модулем p_j за допомогою пристрою піднесення до степеня за модулем, задача зламу ключа гешування зводиться до обчислення дискретного логарифма в полі простого числа, на виході j-го w-розрядного суматора отримують результат додавання значення елемента інформаційної послідовності m_i, отриманого з виходу оперативного запам'ятовуючого пристрою, значення суми результатів гешування попереднього елемента інформаційної послідовності $h^*_{(i-1)}$, яке отримують з виходу $(2\cdot q+1)$-го w-розрядного суматора ($w\in N$, $n=w\cdot q$, а n довжина вихідного геш-значення), значення секретного числа k_j, яке отримують з виходу регістра для зберігання j-і частини ключа. При цьому значення великого числа g_j, яке зберігають у регістрі для зберігання, j-го примітивного елемента, підносять до степеня, який отримують з виходу (q+j)-го w-розрядного суматора, внаслідок додавання за його допомогою результату піднесення до степеня за модулем $h^*_{(i-1)}$, яке отримують з виходу j-го пристрою піднесення до степеня, та значення, яке отримують з виходу j-го w-розрядного суматора, ключові дані доповнюють послідовністю секретних чисел $\{h_{01}, h_{02}, \ldots, h_{0q}\}$.

UA 117326 U


1
i
2
3₁
k₁
4₁
5₁
p₁
g₁
mᵢ
h*(i-1)
6₁
k*i1
h(i-1)1
7₁
d₁
8₁
hi1
3₂
k₂
4₂
5₂
p₂
g₂
mᵢ
h*(i-1)
6₂
k*i2
h(i-1)2
7₂
d₂
8₂
hi2
...
...
H
3q
kq
4q
5q
pq
gq
mᵢ
h*(i-1)
6q
k*iq
h(i-1)q
7q
dq
8q
hiq
9

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 М подають у вигляді послідовності $M=\{m_1,m_2,\ldots, m_l\}$, ключові дані К подають у вигляді великого секретного числа k, а хешування, в подальшому 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 якої виконують піднесення, є результатом додавання значення елемента інформаційної послідовності m_i та результату гешування попереднього елемента інформаційної послідовності.

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

Найбільш близьким є спосіб паралельного ключового гешування даних теоретично доведеної стійкості [Патент України № 94039 від 27.10.2014 р., М. кл. G09C 1/00, бюл. №20 2014 р.], який полягає в тому, що інформаційні дані М подають у вигляді послідовності $M=\{m_1,m_2,\ldots, m_l\}$, подають ключові дані К, 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, причому ключові дані К 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, значення суми результатів гешування попереднього елемента інформаційної послідовності та значення секретного числа k_i.

Недоліком прототипу є недостатня якість гешування даних, яка випливає з підвищеної швидкості зламу результату гешування. Це пов'язано з тим, що в j-му пристрої піднесення до степеня за модулем піднесення відбувається до степеня, значення якого відрізняється від значення степеня, до якого підносять в y-му пристрої піднесення до степеня за модулем ($y\in N$, $y\neq l$, $y\leq q$) на константу $[k_i-k_y)$ незалежно від значення ітерації і, що спрощує задачу зламу, оскільки для підбору цього значення необхідно $O(2^w)$ обчислень геш-значень за допомогою пристрою гешування, на якому здійснюють спосіб гешування, де w кількість розрядів регістра для зберігання значення секретного числа k_i.

В основу корисної моделі поставлена задача створити спосіб паралельного ключового гешування даних теоретично доведеної стійкості, який дозволить забезпечити підвищену якість гешування даних за рахунок введення операції додавання за допомогою w-розрядного суматора, яка дозволить внести невизначеність у різницю показників піднесення до степеня, що породить необхідність у $O(l\cdot 2^w)$ обчислень геш-значень за допомогою пристрою гешування, на якому здійснюють спосіб гешування.

Поставлена задача розв'язується за рахунок того, що інформаційні дані М подають у вигляді послідовності $M=\{m_1,m_2,\ldots, m_l\}$, подають ключові дані К у вигляді послідовності секретних чисел $\{k_1, k_2,\ldots,k_q\}$, гешування інформаційних даних виконують шляхом піднесення кожного з q великих чисел g_j (j=1, 2,…, q), яке є примітивним коренем за відповідним модулем p_i до степеня, за модулем p_i за допомогою пристрою піднесення до степеня за модулем, задача зламу ключа гешування зводиться до обчислення дискретного логарифма в полі простого числа, на виході j-го w-розрядного суматора отримують результат додавання значення елемента інформаційної послідовності m_i, отриманого з виходу оперативного запам'ятовуючого пристрою, значення суми результатів гешування попереднього елемента інформаційної послідовності $f^*_{(i-1)}$, яке отримують з виходу $(2\cdot q+1)$-го w-розрядного суматора ($y\in N$, $n=w\cdot q$, а n довжина вихідного геш-значення), значення секретного числа k_i, яке отримують з виходу регістра для зберігання j-і частини ключа, і згідно з корисною моделлю, значення великого числа g_i, яке зберігають у регістрі для зберігання, j-го примітивного елемента, підносять до степеня, який отримують з виходу $(q+j)$-го w-розрядного суматора, внаслідок додавання за його допомогою результату піднесення до степеня за модулем $h_{(i-1)i}$, яке отримують з виходу j-го пристрою піднесення до степеня, та значення, яке отримують з виходу j-го w-розрядного суматора, ключові дані доповнюють послідовністю секретних чисел $\{h_{01}, h_{02},\ldots,h_{0q}\}$.

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

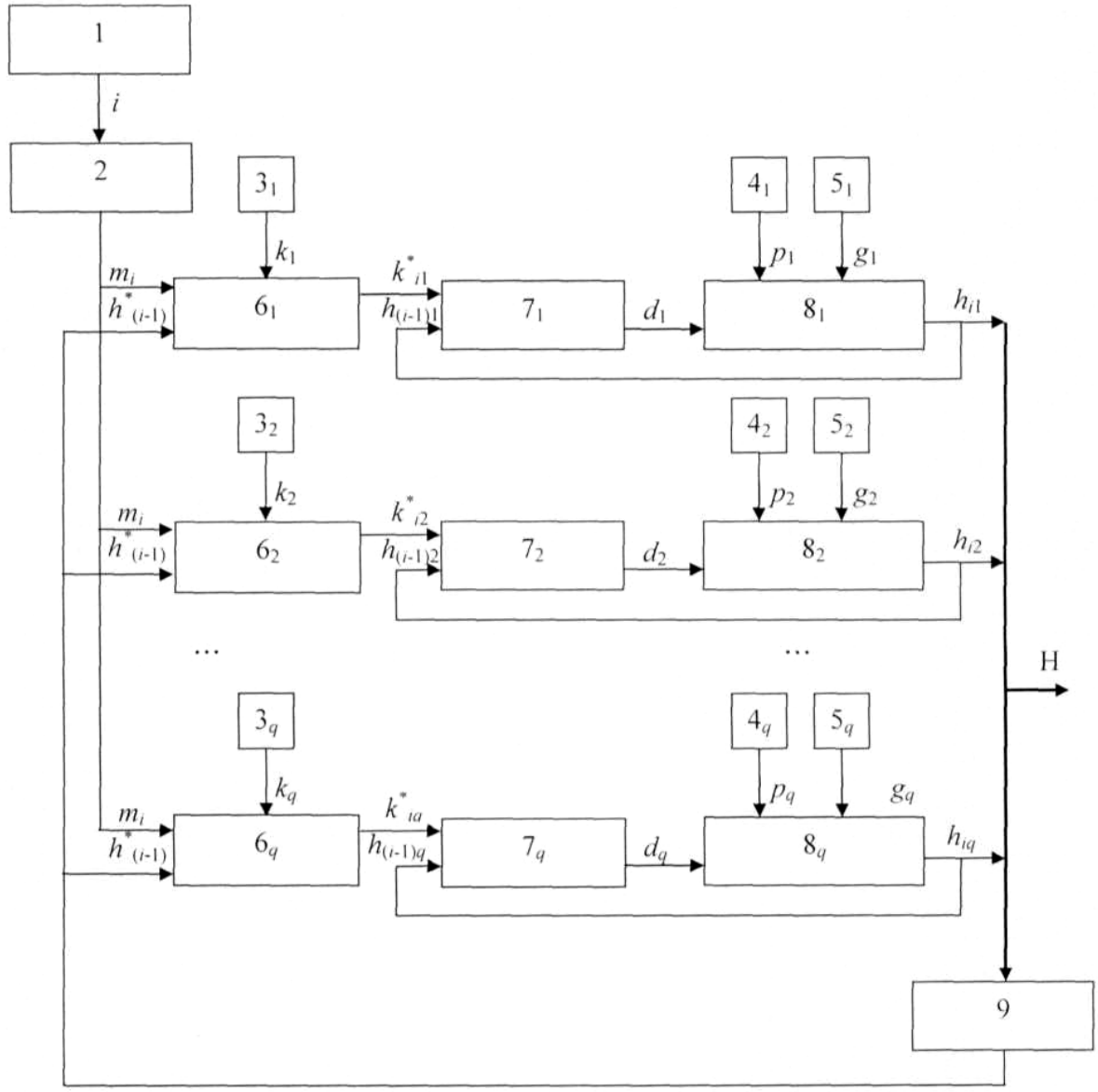
Пристрій містить лічильник 1 вихід, якого з'єднано з входом оперативно запам'ятовуючого пристрою 2, вихід якого є першим входом j-го w-розрядного суматора 6_j ($j \in N$, $j \leq 1$). Другим входом y-го w-розрядного суматора 6 є вихід $(2 \cdot q+1)$-го w-розрядного суматора 9, а третім є вихід регістра для зберігання j-ї частини ключа 3_j. Вихід j-го w-розрядного суматора 6_j з'єднано з першим входом (q+j)-го w-розрядного суматора 7_j. Другим входом (q+j)-го w-розрядного суматора 7_j є вихід j-го пристрою піднесення до степеня за модулем 8_j. Першим входом j-го пристрою піднесення до степеня за модулем 8_j є вихід (q+j)-го w-розрядного суматора 7_j. Другим входом j-го пристрою піднесення до степеня за модулем 8_j є вихід регістра для зберігання j-го значення модуля 4_j, а третім - вихід регістра для зберігання j-го примітивного елемента 5_j. Вихід j-го пристрою піднесення до степеня за модулем 8_j є j-м входом $(2 \cdot q+1)$-го w-розрядного суматора 9 та j-м виходом всього пристрою.

Спосіб паралельного ключовою гешування даних теоретично доведеної стійкості виконується на пристрої таким чином. Вихідне значення j-го пристрою піднесення до степеня 8_j встановлюють відповідно до значення секретного числа h_{0j}. Регістр для зберігання j-ї частини ключа 3_j встановлюють відповідно значення j-ї частини ключа k_j, регістр для зберігання j-го значення модуля 4_j встановлюють відповідно значення j-го модуля p_j, регістр для зберігання j-го примітивного елемента 5 встановлюють відповідно значення примітивного елемента g_j за модулем p_j. До оперативно запам'ятовуючий пристрій 2 заносять інформаційні дані, що підлягають гешуванню, представлені у вигляді послідовності $M=\{m_1,m_2,\ldots, m_l\}$, а лічильник 1 встановлюють в положення, що відповідає початковій адресі оперативно запам'ятовуючого пристрою 2, де зберігається перший елемент інформаційної послідовності m_1. Вихід $(2 \cdot q+1)$-го w-розрядного суматора 9 встановлюють рівним нулю. Починають ітеративний процес. З виходу лічильника 1 отримують адресу i-го елемента інформаційної послідовності m_i та надсилають її до оперативно запам'ятовуючого пристрою 2, з виходу якого отримують значення i-го елемента інформаційної послідовності m_i, яке надсилають на вхід j-го w-розрядного суматора 6_j. За допомогою j-го w-розрядного суматора 6_j додають значення i-го елемента інформаційної послідовності m_i, значення результату гешування попереднього елемента інформаційної послідовності $h^*_{(i-1)}$, яке отримують з виходу $(2 \cdot q+1)$-го w-розрядного суматора 9, та значення j-ї частини ключа k_j, яке отримують з виходу регістра для зберігання j- ї частини ключа 3_j. Значення, отримане з виходу j-го w-розрядного суматора 6_j, надсилають на перший вхід (q+j)-го w-розрядного суматора 7_j, де до нього додають результат піднесення до степеня за модулем $h_{(i-1)j}$, отриманий на попередній ітерації, який надсилають з виходу j-го пристрою піднесення до степеня за модулем 8_j. Значення d_{ij}, отримане з (q+j)-го w-розрядного суматора 7_j, надсилають на вхід j-го пристрою піднесення до степеня за модулем 8_j, де виконують піднесення значення примітивного елемента g_j, отриманого з виходу регістра для зберігання j-го примітивного елемента 5_j, до степеня d_{ij} за модулем p_j, значення якого отримують з виходу регістра для зберігання j-го значення модуля 4_j. Дані, отримані внаслідок виконання операції піднесення до степеня за модулем h_{ij}, отримані з виходу j-го пристрою піднесення до степеня за модулем 8_j, надсилають на j-й вхід $(2 \cdot q+1)$-го w-розрядного суматора 9. За допомогою $(2 \cdot q+1)$-го w-розрядного суматора 9 додають q значень результатів піднесення до степеня. Якщо $i \neq l$, то змінюють положення лічильника 1 відповідно адреси (i+1)-го елемента інформаційної послідовності m_{i+1} та починають наступну ітерацію, інакше зупиняють ітеративний процес. Після l-ї ітерації результат піднесення до степеня за модулем h_{ij}, який отримують з виходу j-го пристрою піднесення до степеня за модулем 8_j надсилають на j-й вихід всього пристрою, з якого зчитують j-ту частину геш-значення інформаційних даних M.

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 у вигляді послідовності секретних чисел $\{k_1, k_2, \ldots, k_q\}$, гешування інформаційних даних виконують шляхом піднесення кожного з q великих чисел g_j (j=1, 2, …, q), яке є примітивним коренем за відповідним модулем p_j до степеня, за модулем p_j за допомогою пристрою піднесення до степеня за модулем, задача зламу ключа гешування зводиться до обчислення дискретного логарифма в полі простого числа, на виході j-го w-розрядного суматора отримують результат додавання значення елемента інформаційної послідовності m_i, отриманого з виходу оперативного запам'ятовуючого пристрою, значення суми результатів гешування попереднього елемента інформаційної послідовності $h^*_{(i-1)}$, яке отримують з виходу

(2·q+1)-го w-розрядного суматора (w∈N, n=w·q, а n довжина вихідного геш-значення), значення секретного числа k_j, яке отримують з виходу регістра для зберігання j-і частини ключа, який **відрізняється** тим, що значення великого числа g_j, яке зберігають у регістрі для зберігання, j-го примітивного елемента, підносять до степеня, який отримують з виходу (q+j)-го w-розрядного суматора, внаслідок додавання за його допомогою результату піднесення до степеня за модулем $h^*_{(i-1)}$, яке отримують з виходу j-го пристрою піднесення до степеня, та значення, яке отримують з виходу j-го w-розрядного суматора, ключові дані доповнюють послідовністю секретних чисел $\{h_{01}, h_{02}, \ldots, h_{0q}\}$.



Комп'ютерна верстка В. Мацело

Міністерство економічного розвитку і торгівлі України, вул. М. Грушевського, 12/2, м. Київ, 01008, Україна

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