МІНІСТЕРСТВО ЕКОНОМІЧНОГО РОЗВИТКУ І ТОРГІВЛІ УКРАЇНИ

УКРАЇНА **(19) UA** **(11) 117327** **(13) U**

(51) МПК (2017.01)
G09C 1/00

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2016 13378**

(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)

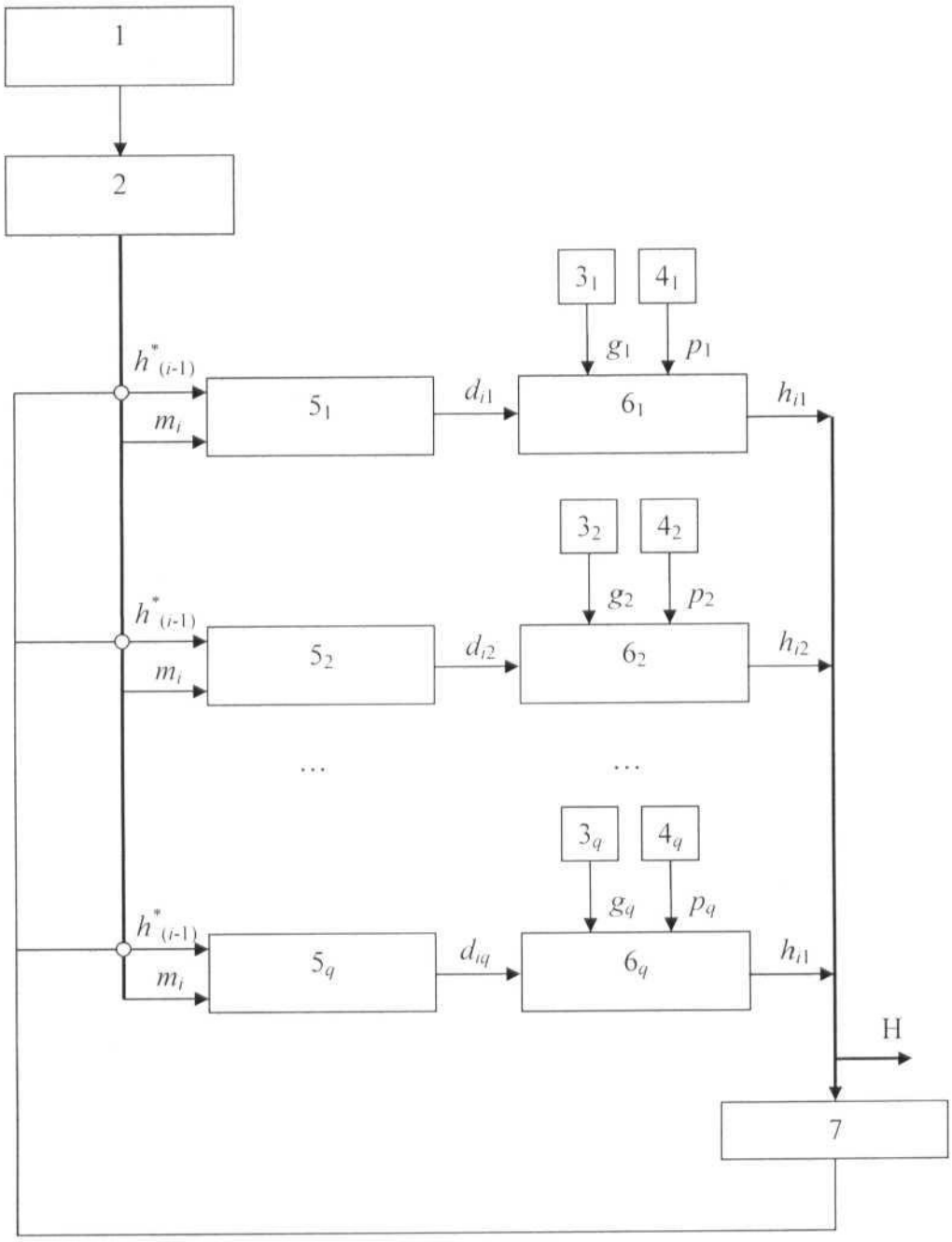
(73) Власник(и):
ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ,
Хмельницьке шосе, 95, м. Вінниця, 21021 (UA)

(54) СПОСІБ ПАРАЛЕЛЬНОГО БЕЗКЛЮЧОВОГО ГЕШУВАННЯ ДАНИХ ТЕОРЕТИЧНО ДОВЕДЕНОЇ СТІЙКОСТІ

(57) Реферат:

Спосіб паралельного безключового гешування теоретично доведеної стійкості полягає в тому, що інформаційні дані M подають у вигляді послідовності $M=\{m_1, m_2,\ldots, m_i\}$, гешування інформаційних даних виконують шляхом піднесення до степеня за модулем великого простого числа ρ за допомогою пристрою піднесення до степеня за модулем. Початкове заповнення h_0 є відкритим. На виході (q+1)-го w-розрядного суматора ($w\in N$, $n=w\cdot q$, a n - довжина вихідного геш-значення) отримують результат додавання всіх результатів піднесення до степеня, отриманих на попередньому кроці, за модулем простого числа ρ_j, отриманого з виходу регістра для зберігання j-го значення модуля, піднесення до степеня за модулем виконують паралельно. За допомогою j-го пристрою піднесення до степеня за модулем підносять значення примітивного елемента g_j за модулем ρ_i, який отримують з регістра для зберігання j-го примітивного елемента, до степеня, який отримують з виходу j-го w-розрядного суматора, за допомогою якого додають значення, отримане з виходу (q+1)-го w-розрядного суматора та значення i-го елемента інформаційної послідовності m_i, яке отримують з оперативно запам'ятовуючого пристрою.

UA 117327 U


1
2
3_1
4_1
g_1
p_1
$h^*_{(i-1)}$
m_i
5_1
d_{i1}
6_1
h_{i1}
3_2
4_2
g_2
p_2
$h^*_{(i-1)}$
m_i
5_2
d_{i2}
6_2
h_{i2}
...
...
3_q
4_q
g_q
p_q
$h^*_{(i-1)}$
m_i
5_q
d_{iq}
6_q
h_{i1}
H
7

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

Відомий спосіб безключового хешування [Патент України №48410 від 10.03.2010 р., М. кл. G09C 1/00, бюл. № 5 2010 р.], який полягає в тому, що інформаційні дані М подають у вигляді послідовності $M= \{m_1, m_2,\ldots, m_l\}$, хешування, в подальшому гешування, інформаційних даних виконують шляхом піднесення до степеня елементів m_i інформаційної послідовності М за модулем великого простого числа ρ за допомогою пристрою піднесення до степеня за модулем, в подальшому блока піднесення до степеня за модулем, степінь, до якого виконують піднесення за модулем, є результатом гешування попереднього елемента інформаційної послідовності h_{i-1}, а початкове заповнення h_0 є відкритим.

Недоліком цього способу є недостатня обчислювальна швидкість, яка полягає в тому, що піднесення до степеня за модулем відбувається для елемента інформаційної послідовності довжини n розрядів та виконання для цього $O(n^2)$ додавань.

Найбільш близьким до способу, що пропонується, є спосіб безключового хешування [Патент України №54761 від 25.11.2010 р., М. кл. G09C 1/00, бюл. №22 2010 р.], який полягає в тому, що інформаційні дані М подають у вигляді послідовності $M= \{m_1, m_2,\ldots, m_l\}$, гешування інформаційних даних виконують шляхом піднесення до степеня елементів τ_i інформаційної послідовності М за модулем великого простого числа ρ за допомогою блока піднесення до степеня за модулем, в подальшому пристрою піднесення до степеня за модулем, степінь, до якого виконують піднесення за модулем, є результатом гешування попереднього елемента інформаційної послідовності h_{i-1}, а початкове заповнення h_0 є відкритим, елемент інформаційної послідовності m_i (i=1, 2,…, l) розбивають на q частин, кожну з яких m_{ij} (j=1, 2,…, q) підносять до степеня, який отримують шляхом додавання всіх результатів піднесення до степеня, отриманих на попередньому кроці, за модулем простого числа ρ_i, піднесення до степеня за модулем кожної частини m_{ij} елемента інформаційної послідовності m_i виконують паралельно.

Недоліком прототипу є недостатня якість гешування даних, яка випливає з підвищеної швидкості знаходження колізії. Це пов'язано з тим, що для кожного значення модуля ρ_i, яке зберігається в регістрі для зберігання модуля, не всі частини інформаційних даних m_{ij} дозволяють отримати повну множину вихідних значень (від 1 до ρ_i-1). Оскільки не всі вони є примітивними елементами за модулем ρ_i, то це робить можливим для зловмисника, у випадках, коли значення частини інформаційних даних m_{ij} не є примітивним елементом за модулем ρ_i, швидко здійснити пошук колізії (зокрема, використовуючи елементи інформаційної послідовності зі значеннями 1), тому задача зламу не зводиться до реалізації обчислень теоретично доведеної складності при використанні пристрою, на якому виконують даний спосіб гешування.

В основу корисної моделі поставлена задача створити спосіб паралельного безключового гешування теоретично доведеної стійкості, який дозволить забезпечити підвищену якість гешування даних за рахунок введення операції додавання, яку виконують за допомогою w-розрядного суматора ($w\in N$, $n=w\cdot q$), та використання регістрів, що зберігають значення наперед обчислених примітивних елементів g_i, за модулем ρ_i, чим звести задачу зламу до задачі дискретного логарифмування в полі простого числа розрядності w.

Поставлена задача вирішується за рахунок того, що в способі паралельного безключового гешування теоретично доведеної стійкості інформаційні дані М подають у вигляді послідовності $M= \{m_1, m_2,\ldots, m_l\}$, гешування інформаційних даних виконують шляхом піднесення до степеня за модулем великого простого числа ρ за допомогою пристрою піднесення до степеня за модулем, початкове заповнення h_0 є відкритим, на виході (q+1)-го w-розрядного суматора ($w\in N$, $n=w\cdot q$, а n - довжина вихідного геш-значення) отримують результат додавання всіх результатів піднесення до степеня, отриманих на попередньому кроці, за модулем простого числа ρ_i, отриманого з виходу регістра для зберігання і-го значення модуля, піднесення до степеня за модулем виконують паралельно, і згідно корисної моделі, за допомогою і-го пристрою піднесення до степеня за модулем підносять значення примітивного елемента q_i за модулем ρ_i, який отримують з регістра для зберігання j-го примітивного елемента, до степеня, який отримують з виходу j-го w-розрядного суматора, за допомогою якого додають значення, отримане з виходу (g+1)-го w-розрядного суматора та значення і-го елемента інформаційної послідовності m_i, яке отримують з оперативно запам'ятовуючого пристрою.

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

Пристрій містить лічильник 1, вихід якого з'єднано з входом оперативно запам'ятовуючого пристрою 2, j-ий вихід якого (j=1, 2,…, q) з'єднано з першим входом j-го w-розрядного суматора 5_j, другим входом якого є вихід (q+i)-го w-розрядного суматора 7. Вихід j-го w-розрядного

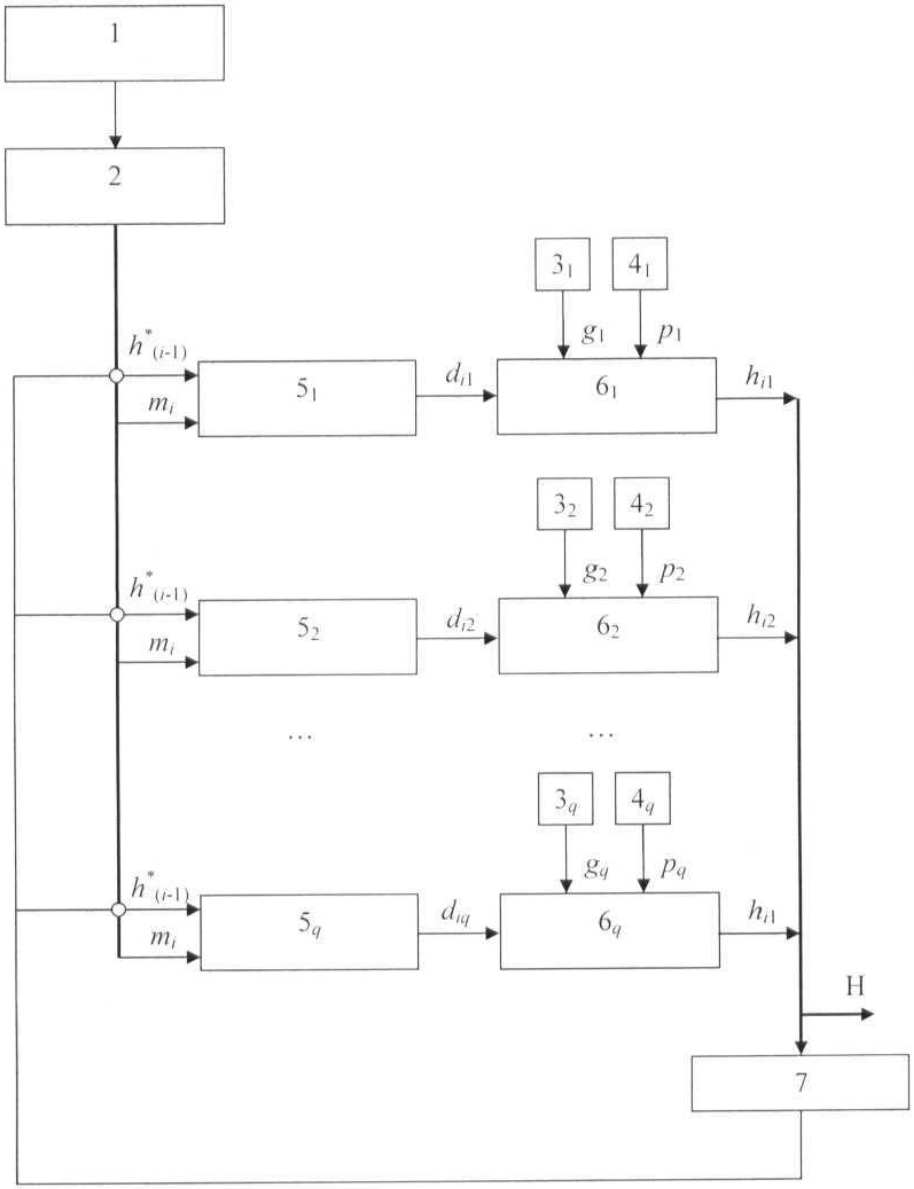
суматора 5_i з'єднано з першим входом j-го пристрою піднесення до степеня за модулем 6_i. Другий вхід j-го пристрою піднесення до степеня за модулем 6, з'єднано з виходом регістра для зберігання j-го примітивного елемента 3_i.Третій вхід j-го пристрою піднесення до степеня за модулем 6_i є виходом 4 регістра для зберігання j-го значення модуля 4_i. Вихід j-го пристрою піднесення до степеня за модулем 6_i є j-им входом (q + 1)-го w-розрядного суматора 7 та j-им виходом всього пристрою.

Спосіб паралельного безключового гешування теоретично доведеної стійкості здійснюється на пристрої таким чином.

Регістр для зберігання j-го значення модуля 4_i встановлюють відповідно значення j-го модуля ρ_i, регістр для зберігання j-го примітивного елемента 3, встановлюють відповідно значення примітивного елемента 3_i за модулем ρ_i. До оперативно запам'ятовуючого пристрою 2 заносять інформаційні дані, що підлягають гешуванню, представлені у вигляді послідовності $\{m_1, m_2,\ldots, m_l\}$, а лічильник 1 встановлюють в положення, що відповідає початковій адресі оперативно запам'ятовуючого пристрою 2, де зберігається перший елемент інформаційної послідовності m_1. Вихідне значення у-го пристрою піднесення до степеня за модулем 6_i встановлюють рівним j-ій частині початкового заповнення h_0. 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_1, яке надсилають на вхід j-го w-розрядного суматора 5_i. За допомогою j-го w-розрядного суматора 5_i додають значення i-го елемента інформаційної послідовності m_i, значення результату гешування попереднього елемента інформаційної послідовності $h^*_{(i-1)}$, яке отримують з виходу (q+1)-го w-розрядного суматора 7. Значення d_{ij}, яке отримують з виходу j-го w-розрядного суматора 5_i, надсилають на вхід j-го пристрою піднесення до степеня за модулем 6, де виконують піднесення значення примітивного елемента g_i, отриманого з виходу регістра для зберігання j-го примітивного елемента 3_i, до степеня d_{ij} за модулем p_i, значення якого отримують з виходу регістра для зберігання j-го значення модуля 4_i. Дані h_{ij}, отримані внаслідок виконання операції піднесення до степеня за модулем, отримані з виходу j-го пристрою піднесення до степеня за модулем 6_i, надсилають на j-й вхід (q+1)-го w-розрядного суматора 7. За допомогою (q+1)-го w-розрядного суматора 7 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 6_i, надсилають на j-й вихід всього пристрою, з якого зчитують j-ту частину геш-значення інформаційних даних M.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Спосіб паралельного безключового гешування теоретично доведеної стійкості, який полягає в тому, що інформаційні дані M подають у вигляді послідовності $M=\{m_1, m_2,\ldots, m_l\}$, гешування інформаційних даних виконують шляхом піднесення до степеня за модулем великого простого числа ρ за допомогою пристрою піднесення до степеня за модулем, початкове заповнення h_0 є відкритим, на виході (q+1)-го w-розрядного суматора ($w\in N$, $n=w\cdot q$, a n - довжина вихідного геш-значення) отримують результат додавання всіх результатів піднесення до степеня, отриманих на попередньому кроці, за модулем простого числа ρ_j, отриманого з виходу регістра для зберігання j-го значення модуля, піднесення до степеня за модулем виконують паралельно, який **відрізняється** тим, що за допомогою j-го пристрою піднесення до степеня за модулем підносять значення примітивного елемента g_j за модулем ρ_i, який отримують з регістра для зберігання j-го примітивного елемента, до степеня, який отримують з виходу j-го w-розрядного суматора, за допомогою якого додають значення, отримане з виходу (q+1)-го w-розрядного суматора та значення i-го елемента інформаційної послідовності m_i, яке отримують з оперативно запам'ятовуючого пристрою.



Комп'ютерна верстка О. Рябко

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