УКРАЇНА

(19) UA (11) 54813 (13) U

(51) МПК (2009)
G09C 1/00

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

ОПИС
ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

видається під відповідальність власника патенту

(54) СПОСІБ ПАРАЛЕЛЬНОГО КЛЮЧОВОГО ХЕШУВАННЯ

(21) u201006156
(22) 21.05.2010
(24) 25.11.2010
(46) 25.11.2010, Бюл.№ 22, 2010 р.
(72) ЛУЖЕЦЬКИЙ ВОЛОДИМИР АНДРІЙОВИЧ, БАРИШЕВ ЮРІЙ ВОЛОДИМИРОВИЧ
(73) ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
(57) Спосіб паралельного ключового хешування, який полягає в тому, що інформаційні дані M подають у вигляді послідовності $M = (m_1, m_2, ..., m_l)$, а хешування інформаційних даних M виконують шляхом піднесення до степеня елементів інформаційної послідовності та елементів ключової послідовності K за модулем простого числа за допомогою блока піднесення до степеня за модулем, степінь, до якої здійснюють піднесення, отримують шляхом додавання особистого ключа та результату попередньої ітерації хешування за допомогою блока додавання, ключові дані K представляють у вигляді послідовності $K = (k_1, k_2, ..., k_q)$, 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 за допомогою j-го блока додавання елемента ключової послідовності k_j та значення результату об'єднання h^*_{i-1} результатів піднесення до степеня за модулем простого числа, отриманих на попередньому кроці, піднесення до степеня за модулем кожної частини m_{ij} елемента інформаційної послідовності m_i виконують паралельно, який **відрізняється** тим, що об'єднання h^*_{i-1} результатів піднесення до степеня за модулем отримують шляхом множення всіх значень h_{i-1j} результатів піднесення до степеня за модулем частин m_{i-1j} елементів інформаційного повідомлення за модулем p_j, а результуючим хеш-значенням є результат об'єднання h^*_l результатів піднесення до степеня за модулем, отриманий після останньої ітерації.

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

Відомий спосіб ключового хешування теоретично доведеної стійкості [Патент України №18693 від 15.11.2006р., М. кл. G 09 C 1/00, бюл. №11 2006р.], який полягає в тому, що інформаційні дані M подаються у вигляді послідовності $M=\{m_1, m_2, ..., m_l\}$, ключові дані K подаються у вигляді великого секретного числа k, а хешування інформаційних даних виконується за допомогою пристрою множення елементів m_i інформаційної послідовності M та елементів ключової послідовності K за ітеративним правилом піднесення до степеня за модулем великого простого числа p, ключові дані, в подальшому особистий ключ k*, використовуються як степінь ступеня в ітераційному правилі хешування, а задача зламу ключа хешування зводиться до обчислення дискретного логарифма в простому полі.

Недоліком даного способу є недостатня стійкість хешування, оскільки для зламу необхідно лише знаходження ключа, яке зводиться до знаходження m_1 блоку даних.

Найбільш близьким до способу, що пропонується, є спосіб ключового хешування теоретично доведеної стійкості [Патент України №41313 від 12.05.2009р., М. кл. G 09 C 1/00, бюл. №9 2009р.], який полягає в тому, що інформаційні дані M подають у вигляді послідовності $M=\{m_1, m_2, ..., m_l\}$, а хешування інформаційних даних M виконують за допомогою пристрою множення, в подальшому блока піднесення до степеня, елементів інформаційної послідовності та елементів ключової послідовності K за ітеративним правилом піднесення до

(19) UA (11) 54813 (13) U

степеня значення елемента m_i інформаційної послідовності за модулем простого числа, степінь, до якого здійснюють піднесення, отримують шляхом додавання особистого ключа та результату попередньої ітерації хешування за допомогою пристрою додавання, в подальшому блока додавання, ключові дані K представляють у вигляді послідовності $K=\{k_1, k_2, \ldots, k_q\}$, 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 за допомогою j-го пристрою додавання, в подальшому j-го блока додавання, елемента ключової послідовності k_j та суми результатів піднесення до степеня, отриманих на попередньому кроці, за модулем простого числа p_i, піднесення до степеня за модулем кожної частини m_{ij} елемента інформаційної послідовності m_i виконують паралельно.

Недоліком прототипу є недостатня стійкість хешування, пов'язана з тим, що результат хешування отримують шляхом конкатенації результатів піднесення до степеня частин елементів інформаційного повідомлення m_{ij}, яка дає лінійний приріст складності з ростом кількості блоків піднесення до степеня, а об'єднання проміжних результатів хешування h_{ij} виконують за допомогою лінійної операції додавання.

В основу корисної моделі поставлена задача створити спосіб паралельного ключового хешування, який дозволить забезпечити підвищену обчислювальну стійкість хешування інформації за рахунок об'єднання проміжних результатів хешування h_{ij} за допомогою нелінійної операції та використання результату об'єднання як результуючого значення хешування за рахунок введення нових операцій.

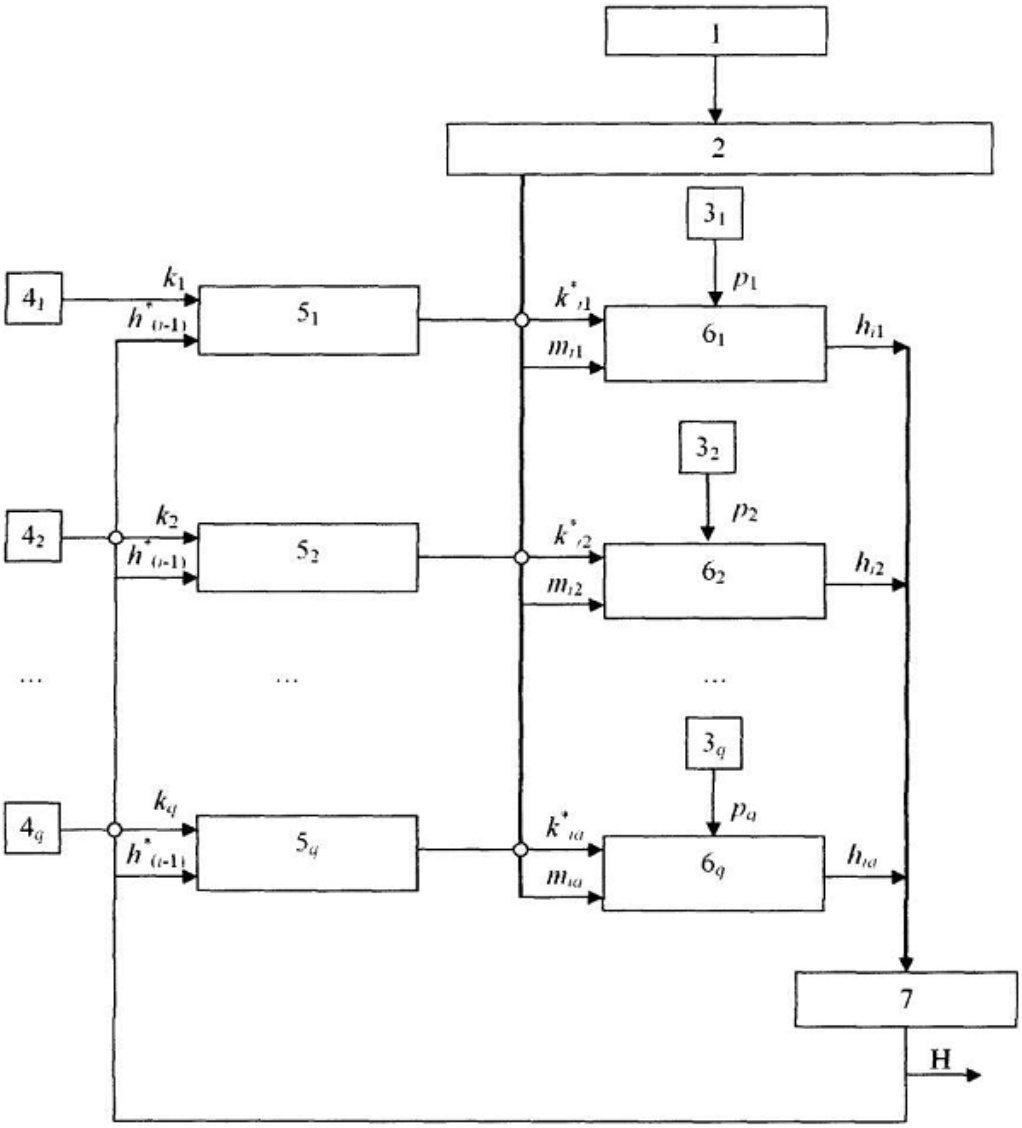
Поставлена задача вирішується за рахунок того, що інформаційні дані M подають у вигляді послідовності $M=\{m_1, m_2, \ldots, m_l\}$, а хешування інформаційних даних M виконують шляхом піднесення до степеня елементів інформаційної послідовності та елементів ключової послідовності K за модулем простого числа за допомогою блока піднесення до степеня за модулем, степінь, до якої здійснюють піднесення, отримують шляхом додавання особистого ключа та результату попередньої ітерації хешування за допомогою блоку додавання, ключові дані K представляють у вигляді послідовності $K=\{k_1, k_2, \ldots, k_q\}$, 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 за допомогою j-го блока додавання елемента ключової послідовності k_j та значення результату об'єднання h^*_{i-1} результатів піднесення до степеня за модулем простого числа, отриманих на попередньому кроці, піднесення до степеня за модулем кожної частини m_{ij} елемента інформаційної послідовності m_i виконують паралельно, причому об'єднання h^*_{i-1} результатів піднесення до степеня за модулем отримують шляхом множення всіх значень h_{i-1j} результатів піднесення до степеня за модулем частин h_{i-1j} елементів інформаційного повідомлення за модулем p_i, а результуючим хеш-значенням є результат об'єднання h^*_l результатів піднесення до степеня за модулем отриманий після останньої ітерації.

На кресленні наведена схема пристрою, що реалізує спосіб паралельного ключового хешування.

Пристрій містить лічильник 1 вихід якого є входом оперативно запам'ятовуючого пристрою 2, j-ий вихід якого з'єднано з першими входом j-го блока піднесення до степеня за модулем 6_j, вихід якого є j-им входом блока множення 7. Вихід блока множення 7 є виходом усього пристрою та першим входом j-го блока додавання 5_j, другим входом якого є вихід j-го регістру зберігання частини ключа k_j 4_j. Вихід j-го блока додавання 5_j є другим входом j-го блока піднесення до степеня за модулем 6_j. Третім входом j-го блока піднесення до степеня за модулем 6_j є вихід j-го регістру зберігання модуля p_j 3_j.

Спосіб паралельного ключового хешування виконують на пристрої так.

У j-ий регістр зберігання модуля p_j 3_j заносять значення модуля p_j, в j-ий регістр зберігання частини ключа k_j 4_j заносять значення частину ключа k_j, встановлюють в початкове положення лічильник 1 згідно початкової адреси оперативно запам'ятовуючого пристрою 2, в який заносять інформаційні дані M, що подають у вигляді послідовності $M=\{m_1, m_2, \ldots, m_l\}$. Починають ітеративний процес. З лічильника 1 отримують значення адреси i-го елемента інформаційної послідовності та надсилають його до оперативно запам'ятовуючого пристрою 2, на j-му виході якого отримують j-ту частину i-го елемента інформаційної послідовності m_{ij}, яку надсилають на вхід j-го блока піднесення до степеня за модулем 6_j. Одночасно за допомогою j-го блока додавання 5_j додають значення частини ключа k_j, що надсилають з регістра зберігання частини ключа k_j 4_j, та значення h^*_{i-1} з виходу блока множення 7, отримане значення результату додавання k^*_{iu} надсилають на другий вхід j-го блока піднесення до степеня за модулем 6_j. На третій вхід j-го блока піднесення до степеня за модулем 6_j надсилають значення виходу регістра зберігання модуля p_j 3_j. За допомогою кожного j-го блока піднесення до степеня за модулем 6_j паралельно виконують піднесення j-ої частини i-го елемента інформаційної послідовності m_{ij} до степеня k^*_{ij} за модулем p_j, отриманий результат h_{ij} надсилають на j-ий вхід блока множення 7, за допомогою якого отримують значення добутку h^*_i всіх h_{ij}. Результуючим хеш-значенням H буде значення добутку h^*_l, отримане після завершення l-ої ітерації.



Комп'ютерна верстка М. Ломалова Підписне Тираж 26 прим.

Міністерство освіти і науки України
Державний департамент інтелектуальної власності, вул. Урицького, 45, м. Київ, МСП, 03680, Україна

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