УКРАЇНА

(19) UA (11) 48279 (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) u200909901
(22) 28.09.2009
(24) 10.03.2010
(46) 10.03.2010, Бюл.№ 5, 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 $M = (m_1, m_2, \ldots, m_t)$, хешування інформаційних даних M виконують за допомогою пристрою множення елементів інформаційної послідовності та елементів ключової послідовності K за ітеративним правилом піднесення до степеня значення елемента 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, ключові дані K представляють у вигляді послідовності $K = (k_1, k_2, \ldots, k_w)$, а елемент інформаційної послідовності $m_i (i = 1,2,\ldots,t)$ розбивають на w частин, кожну з яких $m_{iu} (u = 1,2,\ldots,w)$ підносять до степеня, який отримують шляхом додавання за допомогою u-го пристрою додавання елемента ключової послідовності k_u та суми результатів піднесення до степеня, отриманих на попередньому кроці, за модулем простого числа p_u, піднесення до степеня за модулем кожної частини m_{iu} елемента інформаційної послідовності m_i виконують паралельно, який **відрізняється** тим, що степінь, до якого підносять частину елемента інформаційної послідовності m_{iu}, отримують шляхом додавання результатів піднесення до степеня, отриманих на попередньому кроці на u-му та (u-1)mod w -му блоках піднесення за модулем.

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 подають у вигляді послідовності $M = (m_1, m_2, \ldots, m_t)$, ключові дані K подають у вигляді великого секретного числа k, а хешування інформаційних даних виконують за допомогою пристрою множення елементів інформаційної послідовності $m_i (i = 1,2,\ldots,t)$ та елементів ключової послідовності K за ітеративним правилом піднесення до степеня за модулем великого простого числа p, ключові дані k^*, використовують як степінь ступеня в ітераційному правилі хешування, а задача зламу ключа хешування зводиться до обчислення дискретного логарифма в полі простого числа.

Недоліком аналогу є низька швидкість хешування, в зв'язку з тим, що для обробки i-го елементу інформаційної послідовності необхідно попередньо обчислити хеш-значення для всіх попередніх i-1 елементів інформаційної послідовності, а отже необхідно t ітерацій піднесення до степеня для обробки всіх елементів інформаційної послідовності m_i.

Найбільш близьким до способу, що заявляється є спосіб паралельного 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 $M = (m_1, m_2, \ldots, m_t)$, хешування інформаційних даних M виконують за допомогою пристрою множення елементів інформаційної послідовності та елементів ключової послідовності K за ітератив-

(19) UA (11) 48279 (13) U

ним правилом піднесення до степеня значення елемента 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, а ключові дані K представляють у вигляді послідовності $K=(k_1,k_2,\ldots,k_w)$, а елемент інформаційної послідовності m_i розбивають на w частин, кожну з яких $m_{iu}\ (u=1,2,\ldots,w)$ підносять до степеня, який отримують шляхом додавання за допомогою u-го пристрою додавання елемента ключової послідовності k_u та суми результатів піднесення до степеня, отриманих на попередньому кроці, за модулем простого числа p_u, піднесення до степеня за модулем кожної частини m_{iu} елемента інформаційної послідовності m_i, виконують паралельно.

В основу корисної моделі поставлена задача створення такого способу паралельного ключового хешування, який дозволить забезпечити підвищену швидкість хешування за рахунок паралельного обчислення степеня, до якого підносять елементи інформаційної послідовності на кожній ітерації.

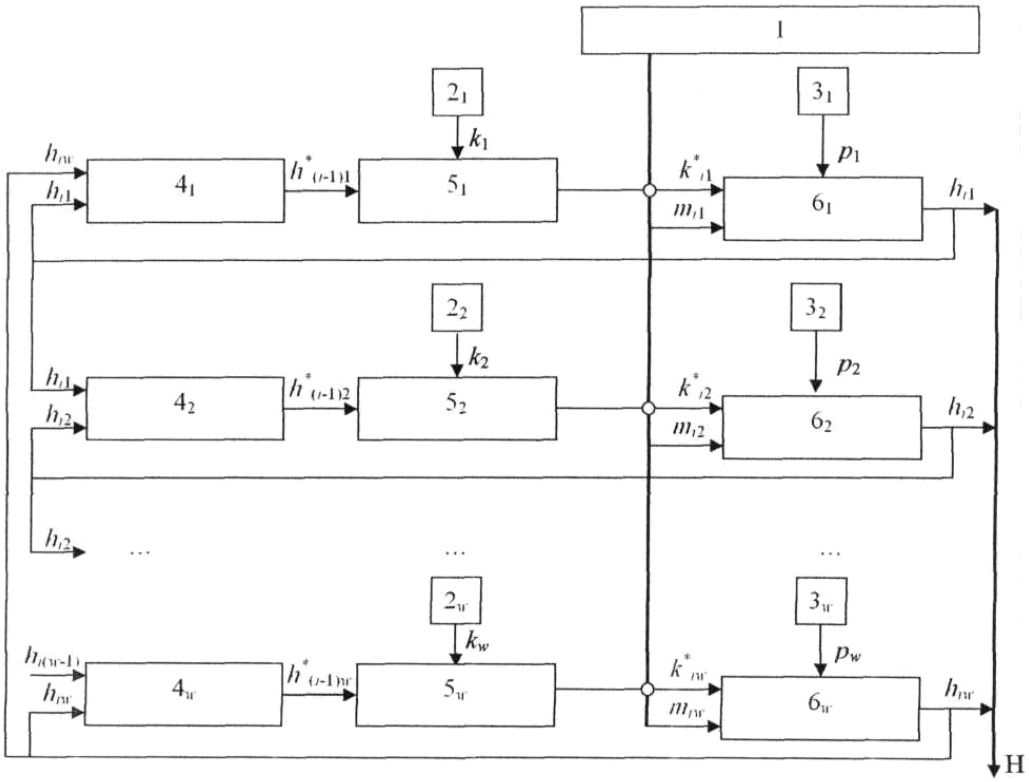
Технічний результат, який може буде отриманий при здійсненні корисної моделі, полягає в підвищенні швидкості обчислення хеш-значення.

Поставлена задача вирішується за рахунок того, що в способі паралельного ключового хешування інформаційні дані M подають у вигляді послідовності $M=(m_1,m_2,\ldots,m_t)$, хешування інформаційних даних M виконують за допомогою пристрою множення елементів інформаційної послідовності та елементів ключової послідовності K за ітеративним правилом піднесення до степеня значення елемента 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, ключові дані K представляють у вигляді послідовності $K=(k_1,k_2,\ldots,k_w)$, а елемент інформаційної послідовності $m_i\ (i=1,2,\ldots,t)$ розбивають на w частин, кожну з яких $m_{iu}\ (u=1,2,\ldots,w)$ підносять до степеня, який отримують шляхом додавання за допомогою u-го пристрою додавання елемента ключової послідовності k_u та суми результатів піднесення до степеня, отриманих на попередньому кроці, за модулем простого числа p_u, піднесення до степеня за модулем кожної частини m_{iu} елемента інформаційної послідовності m_i виконують паралельно, причому степінь, до якого підносять частину елемента інформаційної послідовності m_{iu}, отримують шляхом додавання результатів піднесення до степеня, отриманих на попередньому кроці на u-му та (u-1)mod w-му блоках піднесення за модулем.

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

Пристрій містить блок інформаційних даних $M=(m_1,m_2,\ldots,m_t)$ 1, u-ий вихід якого з'єднано з першими входом u-го блока піднесення за модулем 6_u, вихід якого є першим входом u-го пристрою додавання 4_u, другим входом (u+1)mod w-го пристрою додавання $4_{(u+1)\bmod w}$ та є u-им виходом всього пристрою. Вихід u-го пристрою додавання 4_u є першим входом для (w+u)-го пристрою додавання 5_u. Вихід (w+u)-го пристрою додавання 5_u є другим входом для u-го блока піднесення за модулем 6_u. Третім входом u-го блока піднесення за модулем 6_u є вихід u-го блока зберігання модуля 3_u. Другим входом (w+u)-го пристрою додавання 5_u є вихід u-го блока зберігання ключа 2_u.

Спосіб паралельного ключового хешування виконується на пристрої таким чином. В кожний u-ий блок зберігання ключа 2_u надсилають відповідні частини ключової інформації k_u та в кожний u-ий блок зберігання модуля 3_u надсилають відповідні значення модулів p_u. Значення виходу u-го пристрою додавання 4_u встановлюють рівним нулю. Починають ітеративний процес. З блока інформаційних даних $M=(m_1,m_2,\ldots,m_t)$ 1 надсилають значення u-ої частини елементу інформаційної послідовності m_{iu} на вхід кожного u-го блока піднесення за модулем 6_u. Одночасно за допомогою кожного u-го пристрою додавання 5_u додають складову ключа k_u, що надсилають з кожного (w+u)-го блока зберігання ключа 2_u, та значення виходу u-го пристрою додавання 4_u, отримане значення результату додавання k_{iu}^* надсилають на другий вхід u-го блока піднесення за модулем 6_u. На третій вхід u-го блока піднесення за модулем 6_u надсилають значення виходу u-го блока зберігання модуля 3_u. На кожному u-му блоці піднесення за модулем 6_u паралельно виконують піднесення частини елементу інформаційної послідовності m_{iu} до степеня k_{iu}^* за модулем p_u, отриманий результат h_{iu} надсилають на перший вхід u-го пристрою додавання 4_u, другий вхід (u+1)mod w-го пристрою додавання $4_{(u+1)\bmod w}$, та на u-ий вихід всього пристрою. Результуючим хеш-значенням H буде результат конкатенації всіх h_{tu}.



Фіг.

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