УКРАЇНА

(19) UA (11) 41313 (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 ТЕОРЕТИЧНО ДОВЕДЕНОЇ СТІЙКОСТІ

(21) u200900489
(22) 23.01.2009
(24) 12.05.2009
(46) 12.05.2009, Бюл.№ 9, 2009 р.
(72) ЛУЖЕЦЬКИЙ ВОЛОДИМИР АНДРІЙОВИЧ, UA, БАРИШЕВ ЮРІЙ ВОЛОДИМИРОВИЧ, UA, ДМИТРИШИН ОЛЕКСАНДР ВАСИЛЬОВИЧ, UA
(73) ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ, UA
(57) Спосіб паралельного ключового хешування теоретично доведеної стійкості, який полягає в тому, що інформаційні дані M подають у вигляді послідовності $M=\{m_1, m_2, ..., m_t\}$, а 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, який **відрізняється** тим, що ключові дані K представляють у вигляді послідовності $K=\{k_1, k_2, ..., k_w\}$, а елемент інформаційної послідовності m_i (i=1, 2, ..., t) розбивають на w частин, кожну з яких m_{iu} (u=1, 2, ..., 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.

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

Відомий спосіб хешування даних (Halevi S., Krawczyk H. MMH: Software Message Authentication in the Gbit/second Rates // J. of Computing, Vol. 16. - No. 2. - P. 133-140) ґрунтується на тому, що інформаційні дані подаються у вигляді послідовності блоків, в подальшому елементів інформаційної послідовності, $M=\{m_1, m_2 ... m_t\}$, ключові дані подаються у вигляді послідовності блоків $X=\{x_1, x_2, ... x_t\}$, а хешування інформаційних даних виконується за допомогою пристроїв множення за ітераційним правилом:

$$g_X(m) = \sum_{i=1}^{t} m_i x_i \bmod p$$

що реалізує відображення вигляду:

$$MMH = \left\{ g_X : Z_p^t \to Z_p \mid M \in Z_p^t \right\},$$

де $g_x(m)$ - хеш-код;

Z_p^t - кільце цілих чисел за модулем p;

p - просте число.

Недоліками цього способу є залежність обчислювальної стійкості хешування від властивостей та періоду генератора випадкових послідовностей, за допомогою якого формується ключова послідовність $X=\{x_1, x_2, ... x_t\}$ та неспроможність теоретичного доведення обчислювальної стійкості ключового хешування.

Найбільш близьким до способу, що пропонується, є спосіб ключового хешування теоретично доведеної стійкості (Патент України №18693 від 15.11.2006р., М. кл. G09C 1/00, бюл. №11 2006р.), який полягає в тому, що інформаційні дані M подаються у вигляді послідовності $M=\{m_1, m_2 ... m_t\}$, ключові дані K подаються у вигляді великого секретного числа k, а хешування інформаційних даних виконується за допомогою пристрою множення елементів інформаційної послідовності m_i (i=1, 2, ..., t) та елементів ключової послідовності K за ітеративним правилом піднесення до степеня за модулем великого простого числа p, ключові дані k*, використовуються як степінь ступеня в ітераційному правилі хешування, а задача зламу ключа хешування зводиться до обчислення дискретного логарифма в полі простого числа.

Недоліком прототипу є те, що не досягається висока швидкість хешування, в зв'язку з тим, що

(19) UA (11) 41313 (13) U

для обробки і-го елементу інформаційної послідовності необхідно попередньо обчислити хеш-значення для всіх попередніх і-1 елементів інформаційної послідовності, а отже необхідно t ітерацій піднесення до степеня для обробки всіх елементів інформаційної послідовності m_i.

В основу корисної моделі поставлена задача створити спосіб паралельного ключового хешування теоретично доведеної стійкості, який дозволить забезпечити підвищену швидкість обчислення за рахунок паралельної обробки елементів інформаційної послідовності.

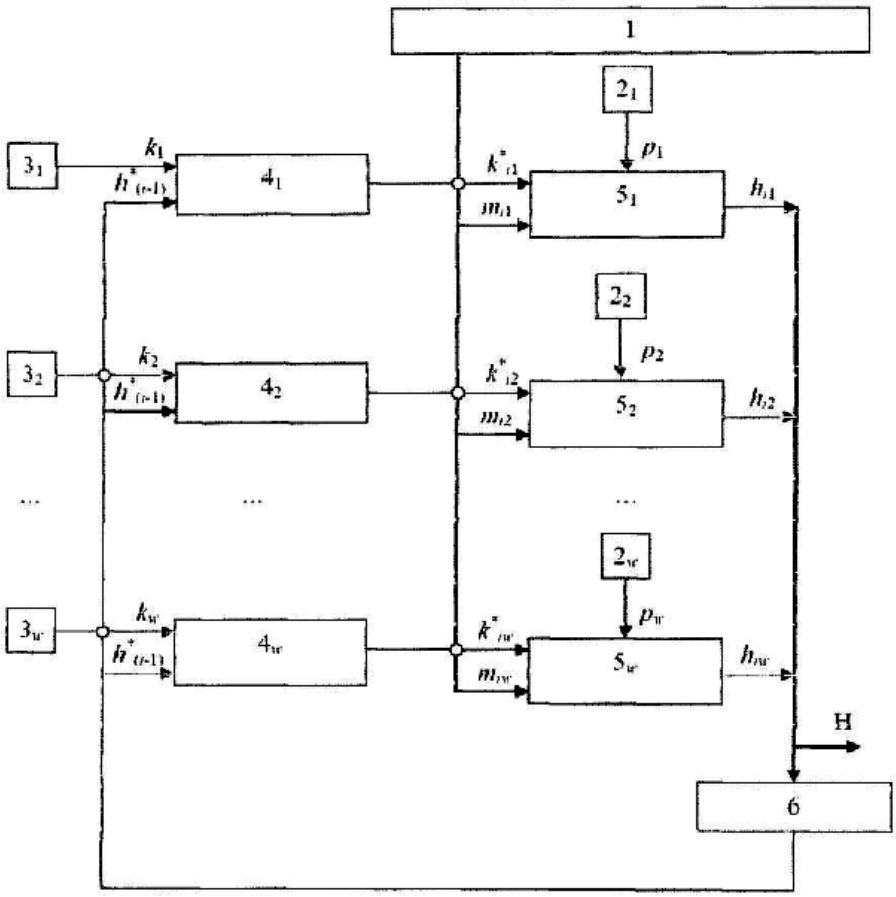
Технічний результат, який може буде отриманий при здійсненні корисної моделі, полягає в підвищенні швидкості обчислення хеш-значення.

Поставлена задача вирішується за рахунок того, що інформаційні дані M подають у вигляді послідовності $M=\{m_1, m_2, ..., m_t\}$, а 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 якої здійснюють піднесення, отримують шляхом додавання особистого ключа та результату попередньої ітерації хешування за допомогою пристрою додавання, причому 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, ..., 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.

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

Пристрій містить блок інформаційних даних $M=\{m_1, m_2, ..., m_t\}$ 1, u-ий вихід якого з'єднано з першими входом u-го (u=1, 2, ..., w) блока піднесення за модулем 5_u, вихід якого є u-им входом (w+1)-го пристрою додавання 6 та є u-им виходом всього пристрою. Вихід (w+1)-го пристрою додавання 6 є першим входом для w пристроїв додавання $4_1, 4_2, ..., 4_w$. Вихід u-го пристрою додавання 4_u є другим входом для u-го блока піднесення за модулем 5_u. Третім входом u-го блока піднесення за модулем 5_u є вихід u-го блока зберігання модуля 2_u. Другим входом u-го пристрою додавання 4_u є вихід u-го блока зберігання ключа 3_u.

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



Комп'ютерна верстка М. Ломалова Підписне Тираж 28 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