УКРАЇНА

(19) UA (11) 54761 (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 БЕЗКЛЮЧОВОГО ХЕШУВАННЯ

(21) u201005395
(22) 05.05.2010
(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 безключового хешування, який полягає в тому, що інформаційні дані M подають у вигляді послідовності $M=\{m_1, m_2, ..., m_l\}$, хешування інформаційних даних виконують шляхом піднесення до степеня елементів m_i інформаційної послідовності M за модулем великого простого числа p за допомогою блока піднесення до степеня за модулем, степінь, до якого виконують піднесення за модулем, є результатом хешування попереднього елемента інформаційної послідовності h_{i-1}, а початкове заповнення h_0 є відкритим, який **відрізняється** тим, що 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 p_j, піднесення до степеня за модулем кожної частини m_{ij} 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 ключового хешування теоретично доведеної стійкості (Патент України №18693 від 15.11.2006р., М.кл. G09C1/00, бюл. №11, 2006р.), який полягає в тому, що інформаційні дані M подають у вигляді послідовності $M=\{m_1,m_2,...,m_l\}$, ключові дані K подають у вигляді великого секретного числа k, в подальшому початкове заповнення h_0, та особистого ключа k*, а хешування інформаційних даних виконують за допомогою пристрою множення, в подальшому пристрою піднесення до степеня за модулем, елементів m_i інформаційної послідовності M та елементів ключової послідовності K за ітеративним правилом піднесення до степеня значення блока даних за модулем великого простого числа p, степінь, до якого здійснюють піднесення, отримують шляхом додавання особистого ключа k* та результату попередньої ітерації хешування за допомогою пристрою додавання, ключові дані використовують як степінь ступеня в ітераційному правилі хешування, а задача зламу ключа хешування зводиться до обчислення дискретного логарифма в простому полі.

Недоліками цього способу є надмірна ключова інформація та наявність додаткових операції, які виконують над нею, що не дозволяє ефективно впровадити безключове хешування при автентифікації даних.

Найбільш близьким до способу, що пропонується є спосіб безключового хешування (Патент України №48410 від 10.03.2010р., М.кл. G09C1/00, бюл. №5 2010р.), який полягає в тому, що інформаційні дані M подають у вигляді послідовності $M=\{m_1, m_2,..., m_l\}$, хешування інформаційних даних виконують шляхом піднесення до степеня елементів m_i інформаційної послідовності M за модулем великого простого числа p 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 хешування попереднього елементу інформаційної послідовності h_{i-1}, а початкове заповнення h_0 є відкритим.

Недоліком прототипу є недостатня обчислювальна швидкість, яка полягає в тому, що піднесення до степеня за модулем відбувається для елемента m_i, інформаційної послідовності довжини повної розрядності та виконання для цього $O((\log_2 \max\{m_i\})^2)$ додавань.

В основу корисної моделі поставлена задача створити спосіб безключового хешування, який дозволить забезпечити підвищену швидкість хешування інформації за рахунок паралельного виконання операції піднесення до степеня за модулем для частин елементів інформаційної

(19) UA (11) 54761 (13) U

послідовності $(\log_2 \max\{m_i\})/q$ за $O((\log_2 \max\{m_i\})^2)/q^2)$ додавань.

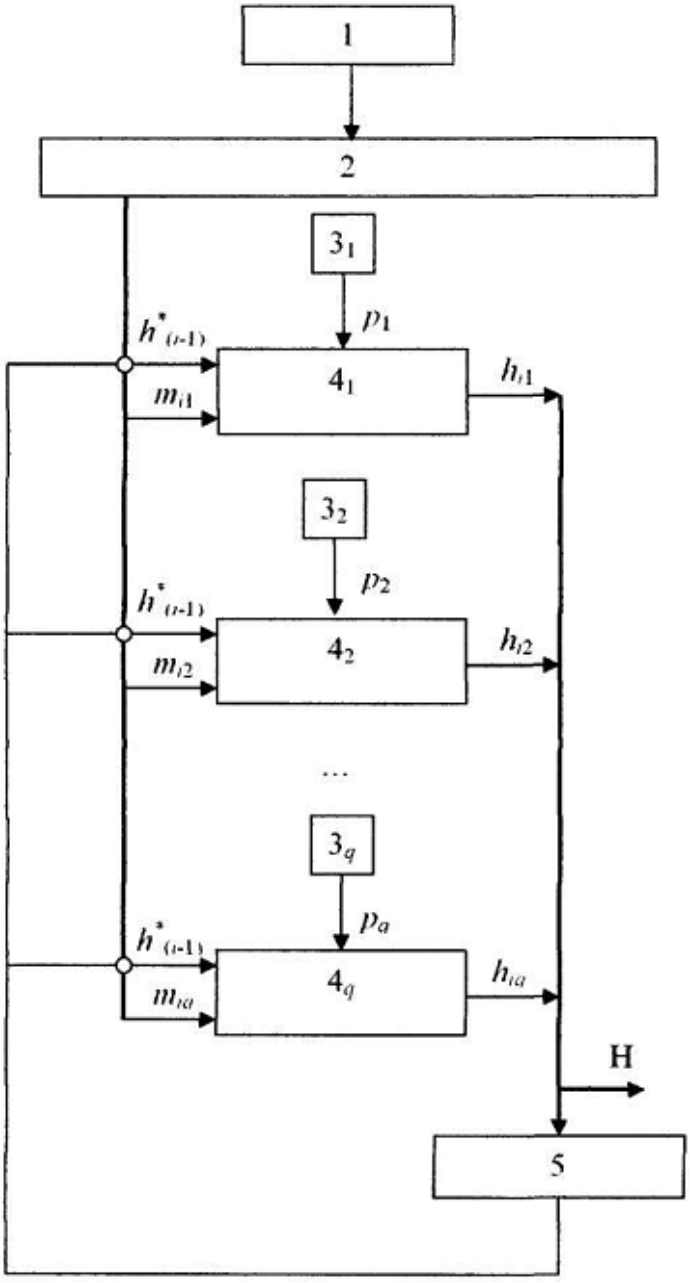
Поставлена задача вирішується за рахунок того, що в способі безключового хешування інформаційні дані M подають у вигляді послідовності $M=\{m_1, m_2,..., m_l\}$, хешування інформаційних даних виконують шляхом піднесення до степеня елементів m_i інформаційної послідовності M за модулем великого простого числа p за допомогою блока піднесення до степеня за модулем, степінь, до якого виконують піднесення за модулем, є результатом хешування попереднього елементу інформаційної послідовності h_{i-1}, а початкове заповнення h_0 є відкритим, причому 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 p_j, піднесення до степеня за модулем кожної частини m_{ij} елемента інформаційної послідовності m_i виконують паралельно.

На кресленні наведена схема пристрою, що реалізує спосіб безключового хешування.

Пристрій містить лічильник 1, вихід якого з'єднано з входом оперативно запам'ятовуючого пристрою 2, j-ий вихід якого з'єднано з першим входом j-го блока піднесення до степеня за модулем 4_j (j=1, 2,..., q). Другий вхід j-го блока піднесення до степеня за модулем 4_j з'єднано з виходом регістра зберігання модуля p_j 3_j, третій вхід j-го блока піднесення до степеня за модулем 4_j є виходом блока додавання 5. Вихід j-го блока піднесення до степеня за модулем 4_j є j-им входом блока додавання 5 та j-им виходом всього пристрою.

Спосіб безключового хешування здійснюється на пристрої таким чином.

До регістру зберігання модуля p_j 3_j заносять значення модуля p_j, встановлюють у початкове положення лічильник 1 згідно початкової адреси оперативно запам'ятовуючого пристрою 2, в який заносять інформаційні дані M, які подають у вигляді послідовності $M=\{m_1, m_2,..., m_l\}$, вихідне значення j-го блока піднесення до степеня за модулем 4_j встановлюють рівним j-ій частині початкового заповнення h_{0j}. Починають ітеративний процес. На вхід блока комутації 5 надсилають значення другого регістра 6. Починають ітеративний процес. З лічильника 1 отримують адресу i-го елемента інформаційної послідовності, яку надсилають до оперативно запам'ятовуючого пристрою 2, де на j-ому виході отримують значення j-ої частини i-го елемента інформаційної послідовності m_{ij}, яке надсилають до j-го блока піднесення до степеня за модулем 4_j та виконують піднесення j-ої частини i-го елемента інформаційної послідовності m_{ij} до степеня, значення якого надходить з виходу блока додавання 5, за модулем, отриманим з регістру зберігання модуля p_j 3_j. Значення з виходу j-го блока піднесення до степеня за модулем 4_j надсилають на j-ий вхід блока додавання 5 та на j-ий вихід усього пристрою. На l-ій ітерації на виході j-го блока піднесення до степеня за модулем 4_j отримують j-ту частину h_{lj} вихідного значення результату хешування $H=\{h_{l1}, h_{l2},..., h_{lq}\}$.



Комп'ютерна верстка А. Рябко 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