УКРАЇНА

(19) UA (11) 48681 (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) u200911028
(22) 02.11.2009
(24) 25.03.2010
(46) 25.03.2010, Бюл.№ 6, 2010 р.
(72) ЛУЖЕЦЬКИЙ ВОЛОДИМИР АНДРІЙОВИЧ, БАРИШЕВ ЮРІЙ ВОЛОДИМИРОВИЧ, ДМИТРИШИН ОЛЕКСАНДР ВАСИЛЬОВИЧ
(73) ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
(57) Спосіб паралельного ключового хешування, який полягає в тому, що інформаційні дані *M* подають у вигляді послідовності $M = (m_1, m_2, ..., m_t)$, ключові дані *K* подають у вигляді великого секретного ключа *k*, секретного числа *a* і секретного простого числа *q*, а хешування інформаційних даних виконують за допомогою пристрою піднесення до степеня елементів m_i, *(i = 1,2,..., t)* інформаційної послідовності *M* та елементів ключової послідовності *K* за ітеративним правилом піднесення до степеня за модулем великого простого числа *p* результату додавання значення елемента інформаційної послідовності m_i та значення елемента інформаційної послідовності, номер якого відрізняється від *i* на число, яке обчислюють за допомогою пристрою піднесення до степеня за модулем до степеня *a* значення елемента інформаційної послідовності m_i, за модулем *q*, великий секретний ключ *k* представляють у вигляді послідовності $k = (k_1, k_2, ..., k_w)$, а результат додавання розбивають на *w* частин, кожну з яких паралельно підносять до степеня, який отримують шляхом додавання за допомогою пристрою додавання, елемента ключової послідовності k_j *(j = 1,2, ...,w)* та суми результатів піднесення до степеня, яка підраховується за допомогою пристрою додавання, отриманих на попередньому кроці, за модулем простого числа p_j, який **відрізняється** тим, що степінь, до якого підносять частину суми елементів інформаційної послідовності $m_i - m_{i-u_i}$, отримують шляхом додавання результатів піднесення до степеня, отриманих на попередньому кроці на *(j+1)*-му та *((j-1)*mod *w+1)*-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 №37465 від 25.11.2008р., М. кл. G 09 C 1/00, бюл. №22, 2008р.), який полягає в тому, що інформаційні дані M подають у вигляді послідовності $M = (m_1, m_2, ..., m_t)$, ключові дані K подають у вигляді великого секретного числа k та особистого ключа k*, а хешування інформаційних даних виконують за допомогою пристрою множення 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 доповнюють секретним числом a та секретним простим числом q, а ітеративне правило піднесення до степеня за модулем здійснюють для результату додавання значення блоку даних m_i та значення блоку даних, номер якого відрізняється від і на число, яке обчислюють за допомогою пристрою множення як результат піднесення до степеня a значення блоку даних m_i за модулем q.

Недоліком аналогу є недостатня швидкість хешування, в зв'язку з тим, що для обробки і-го елемента 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.

Найбільш близьким за сукупністю ознак до способу, що пропонується, є спосіб паралельного

(19) UA (11) 48681 (13) U

ключового хешування теоретично доведеної стійкості (Патент України №43511 від 25.08.2009р., М. кл. G 09 C 1/00, бюл. №16, 2009р.), який полягає в тому, що інформаційні дані М подають у вигляді послідовності $M = (m_1, m_2, ..., m_t)$, ключові дані К подають у вигляді великого секретного ключа k, секретного числа а і секретного простого числа q, а хешування інформаційних даних виконують за допомогою пристрою піднесення до степеня елементів m_i (i=1,2,...,t) інформаційної послідовності М та елементів ключової послідовності К за ітеративним правилом піднесення до степеня за модулем великого простого числа р результату додавання s значення елемента інформаційної послідовності m_i та значення елемента інформаційної послідовності, номер якого відрізняється від і на число, яке обчислюють за допомогою пристрою піднесення до степеня а значення елемента інформаційної послідовності m_i за модулем q, великий секретний ключ k представляють у вигляді послідовності $k = (k_1, k_2, ..., k_w)$, а результат додавання s розбивають на w частин, кожну з яких s_j (j=1,2, ...,w) паралельно підносять до степеня, який отримують шляхом додавання за допомогою пристрою додавання, елемента ключової послідовності k_j та суми результатів піднесення до степеня, яка підраховується за допомогою пристрою додавання, отриманих на попередньому кроці, за модулем простого числа p_j.

Недоліком найближчого аналогу є недостатня швидкість хешування, пов'язана з необхідністю додавання всіх результатів піднесення до степеня на кожній ітерації, що неможливо зробити за один такт.

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.

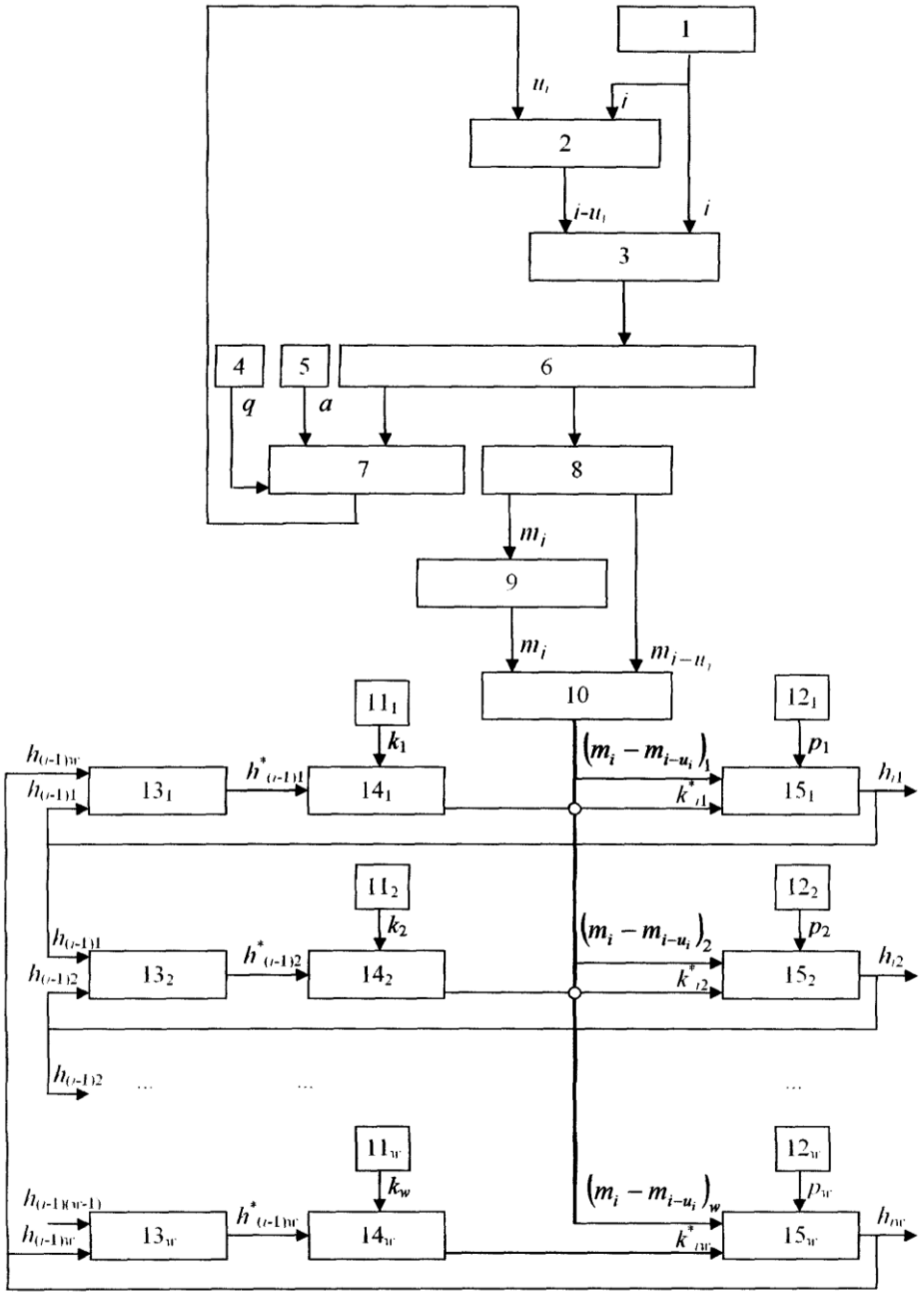
Поставлена задача вирішується за рахунок того, що інформаційні дані М подають у вигляді послідовності $M = (m_1, m_2, ..., m_t)$, ключові дані К подають у вигляді великого секретного ключа k, секретного числа а і секретного простого числа q, а хешування інформаційних даних виконують за допомогою пристрою піднесення до степеня елементів m_i (i=1,2,...,t) інформаційної послідовності М та елементів ключової послідовності К за ітеративним правилом піднесення до степеня за модулем великого простого числа р результату додавання значення елемента інформаційної послідовності m_i та значення елемента інформаційної послідовності, номер якого відрізняється від і на число, яке обчислюють за допомогою пристрою піднесення до степеня за модулем до степеня а значення елемента інформаційної послідовності m_i за модулем q, великий секретний ключ k представляють у вигляді послідовності $k = (k_1, k_2, ..., k_w)$, а результат додавання розбивають на w частин, кожну з яких паралельно підносять до степеня, який отримують шляхом додавання за допомогою пристрою додавання, елемента ключової послідовності k, (j=1,2, ...,w) та суми результатів піднесення до степеня, яка підраховується за допомогою пристрою додавання, отриманих на попередньому кроці, за модулем простого числа p_j, і згідно корисної моделі, степінь, до якого підносять частину суми елементів інформаційної послідовності $m_i + m_{i-u_i}$, отримують шляхом додавання результатів піднесення до степеня, отриманих на попередньому кроці на (j+i)-му та ((j-1)mod w+1)-му блоках піднесення за модулем.

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

Пристрій містить лічильник 1, вихід якого з'єднано з першим входом першого блока комутації 3 та першим входом першого блока додавання 2, вихід якого з'єднано з другим входом першого блока комутації 3. Вихід першого блока комутації 3 є входом оперативно запам'ятовуючого пристрою 6. перший вихід якого є входом другого блока комутації 8, а другий вихід з'єднано з першим входом першого блока піднесення до степеня за модулем 7. Другий вхід першого блока піднесення до степеня за модулем 7 з'єднано з виходом першого регістра 4, третім входом першого блока піднесення до степеня за модулем 7 є вихід другого регістра 5. Вихід першого блока піднесення до степеня за модулем 7 є другим входом першого блока додавання 2. Перший вихід другого блока комутації 8 є першим входом другого блока додавання 10, другий вихід другого блока комутації 8 з'єднано з входом блока затримки 9, вихід якого є другим входом другого блока додавання 10, j-й (j=1,2,...,w) вихід якого з'єднано з першим входом (j+1)-го блока піднесення за модулем 15_j, вихід якого є першим входом (j+2)-го блока додавання 13_j, другим входом ((j+1)mod w+2)-го блока додавання $13_{(j+1) \bmod w}$ та j-м виходом пристрою. Вихід (j+2)-го блока додавання 13_j є першим входом (w+j+2)-го блока додавання 14_j, другим входом якого є вихід (j+2)-го регістра 11_j. Вихід (w+j+2)-го блока додавання 14_j є другим входом (j+1)-го блока піднесення за модулем 15_i, третім входом якого є вихід (w+j+2)-го регістра 12_j.

Спосіб паралельного ключового хешування теоретично доведеної стійкості виконують на пристрої таким чином. В перший регістр 4 заносять значення параметра q в другий регістр 5 заносять значення параметра а, в (j+2)-й регістр 11_j заносять відповідне значення параметра k_j, що виконують шляхом надсилання відповідних частин ключової інформації К. В (w+j+2)-й регістр 12_j надсилають відповідне значення модуля p_j, значення виходу (j+2)-го блока додавання 13_j встановлюють рівним нулю і встановлюють в початкове положення лічильник 1 згідно початкової адреси оперативно запам'ятовуючого пристрою 6, в який заносять інформаційні дані М, які подають у вигляді послідовності $M = (m_1, m_2, ..., m_t)$. Починають ітеративний процес. З лічильника 1 отримують адресу і-го інформаційного блоку даних, яку надсилають за допомогою першого блока комутації 3 до оперативно запам'ятовуючого пристрою 6, де на

виході отримують значення і-го інформаційного блоку даних m_i, який надсилають до блока затримки 9 через другий блок комутації 8 і до першого блока піднесення до степеня за модулем 7, на якому виконують піднесення інформаційного блоку даних m_i до степеня, значення якого надходить з другого регістра 5, за модулем, отриманим з першого регістра 4. Значення з виходу першого блока піднесення до степеня за модулем 7 надсилають на перший блок додавання 2, де розраховують зсув $i\text{-}u_i$ адреси інформаційного блоку даних, що через перший блок комутації 3 надсилають в оперативно запам'ятовуючий пристрій 6. Значення m_{i-u_i} з оперативно запам'ятовуючого пристрою 6 надсилають до другого блока додавання 10 через другий блок комутації 8, де його додають до значення, отриманого з виходу блока затримки 9. Кожну j-ту частину результату додавання $(m_i - m_{i-u_i})_j$ надсилають на вхід (j+1)-го блока піднесення за модулем 15_j. Паралельно на кожному (w+j+2)-го блоці додавання 14_j додають j-ту складову ключа k_j, яку отримують з (j+2)-го регістра 11_j, і значення, отримане з виходу (j+2)-го блока додавання 13_j. За допомогою (j+1)-го блока піднесення за модулем 15_j підносять значення, отримане з другого блока додавання 10 до степеня, отриманого з (w+j+2)-го блока додавання 14_j за модулем p_j, отриманого з виходу (w+j+2)-го регістра 12_j. Отримане значення з (j+1)-го блока піднесення за модулем 15_j надсилають на вхід (j+2)-го блока додавання 13_j, на вхід ((j+1)mod w+2)-го блока додавання $13_{(j+1) \bmod w}$ та на j-ий вихід всього пристрою. За допомогою (j+2)-го блока додавання 13_j визначають суму $h^*_{(i-1)j}$, після чого починають наступну ітерацію. Результуючим хеш-значенням H буде результат конкатенації всіх h_{tj}.



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