УКРАЇНА

(19) UA (11) 43511 (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) u200900930
(22) 06.02.2009
(24) 25.08.2009
(46) 25.08.2009, Бюл.№ 16, 2009 р.
(72) ЛУЖЕЦЬКИЙ ВОЛОДИМИР АНДРІЙОВИЧ, БАРИШЕВ ЮРІЙ ВОЛОДИМИРОВИЧ, ДМИТРИШИН ОЛЕКСАНДР ВАСИЛЬОВИЧ
(73) ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
(57) Спосіб паралельного ключового хешування теоретично доведеної стійкості, який полягає в тому, що інформаційні дані M подають у вигляді послідовності $M = \{m_1, m_2, ..., m_t\}$, ключові дані K подають у вигляді великого секретного ключа k, секретного числа α 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 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 як результат піднесення до степеня a значення елемента інформаційної послідовності m_i за модулем q, який **відрізняється** тим, що 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, на пристроях піднесення 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.

1

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

Відомий спосіб хешування даних спосіб ключового хешування теоретично доведеної стійкості [Патент України № 18693 від 15.11.2006 р., М. кл. G 09 C 1/00, бюл. №11 2006 р.], 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 m_1 інформаційної послідовності M 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 аналогу є недостатня стійкість хешування, оскільки для зламу способу хешування

2

даних необхідне лише знаходження значення ключа, яке зводиться до знаходження значення першого елементу інформаційної послідовності m_1.

Найбільш близьким за сукупністю ознак є спосіб ключового хешування теоретично доведеної стійкості [Патент України №37465 від 25.11.2008 р., М. кл. G 09 C 1/00, бюл. № 22 2008 р.], 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, в подальшому великий секретний ключ, та особистого ключа k*, а хешування інформаційних даних виконують за допомогою пристрою множення, надалі пристрій піднесення до степеня за модулем, елементів m_i (i = 1, 2, ..., t) інформаційної послідовності M та елементів ключової послідовності K за ітеративним правилом піднесення до степеня значення блока даних, в подальшому елементів інформаційної послідовності, за модулем великого простого числа p, степінь, до якого здійснюють піднесення, отримують шляхом додавання особистого ключа k* та результату попере-

(19) UA (11) 43511 (13) U

дньої 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, надалі для результату додавання s, 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, як результат піднесення до степеня a значення елемента інформаційної послідовності m_i за модулем q.

В описаному найближчому аналогу не досягається висока швидкодія за рахунок того, що для обробки i-го елементу інформаційної послідовності необхідно попередньо обчислити хеш-значення для всіх попередніх i-1 елементів інформаційної послідовності, а отже, необхідно виконати 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, в якому за рахунок паралельної обробки елементів інформаційної послідовності досягається можливість підвищення швидкості обчислення хеш-значення інформаційних даних.

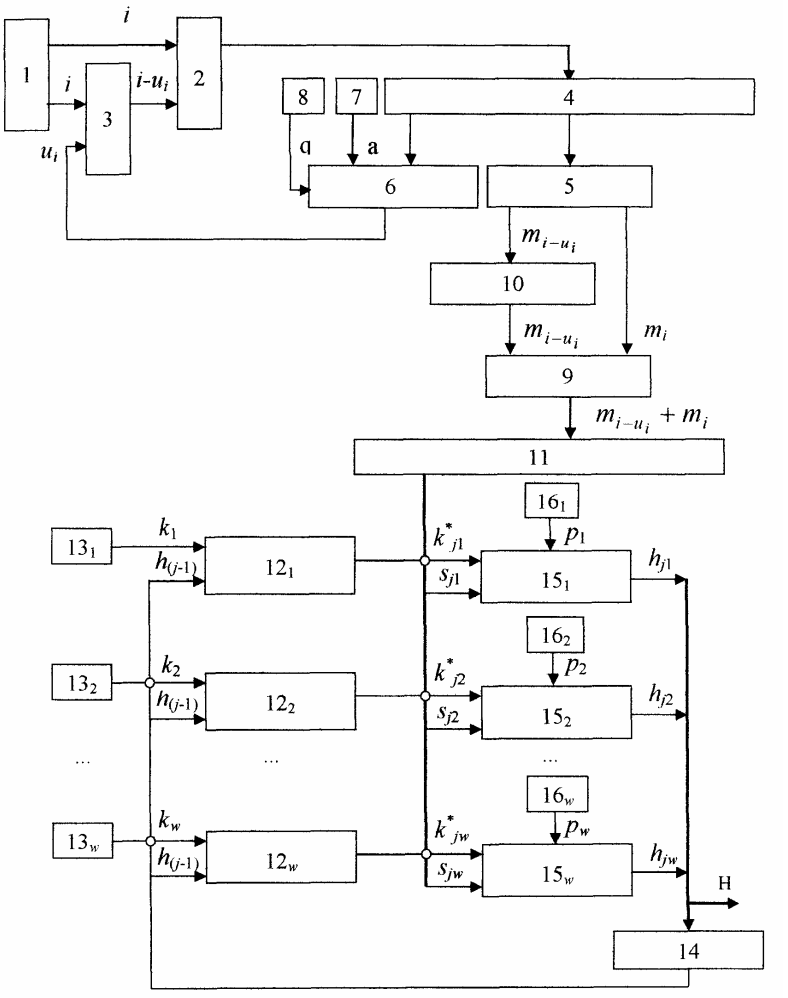
Поставлена задача вирішується за рахунок того, що інформаційні дані M подають у вигляді послідовності $M=\{m_1, m_2,..., m_t\}$, ключові дані K подають у вигляді великого секретного ключа k, секретного числа a і секретного простого числа q, а хешування інформаційних даних виконують за допомогою пристрою 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 s 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 як результат піднесення 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 s розбивають на w частин, кожну з яких s_j (j=1, 2, ..., w) паралельно підносять до степеня, на пристроях піднесення 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.

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 2 та першим входом першого пристрою додавання 3. вихід якого з'єднано з другим входом першого блока комутації 2. Вихід першого блока комутації 2 є входом оперативно запам'ятовуючого пристрою 4. перший вихід якого є входом другого блока комутації 5, а другий вихід з'єднано з першим входом першого пристрою піднесення до степеня за модулем 6. Другий вхід першого пристрою піднесення до степеня за модулем 6 з'єднано з виходом регістра 7, третій вхід першого пристрою піднесення до степеня за модулем 6 є виходом регістра 8. Вихід першого пристрою піднесення до степеня за модулем 6 є другим входом першого пристрою додавання 3. Перший вихід другого блока комутації 5 є першим входом другого пристрою додавання 9, другий вихід другого блока комутації 5 з'єднано з входом блока затримки 10, вихід якого є другим входом другого пристрою додавання 9. Вихід другого пристрою додавання 9 з'єднано з входом блока зберігання даних 11, j-й вихід якого з'єднано з першими входом (j+1)-го пристрою піднесення за модулем 15_j, вихід якого є j-м входом третього пристрою додавання 14. Вихід третього пристрою додавання 14 є першим входом j-го пристрою додавання 12_j, другим входом 7-го пристрою додавання 12, є вихід j-го регістра 13j, вихід j-го пристрою додавання 12_j є другим входом (j+1)-го пристрою піднесення за модулем 15_j, третім входом (j+1)-го пристрою піднесення за модулем 15_j є вихід j-го регістра 16_j. Виходи пристроїв піднесення до степеня 15_1, 15_2, ..., 15_w є виходами пристрою.

Спосіб паралельного ключового хешування теоретично доведеної стійкості виконують на пристрої таким чином. В регістр 7 заносять значення параметра a, в регістр 8 заносять значення параметра q, в j-й регістр 13_j заносять j-те значення великого секретного ключа k, в j-й регістр 16_j надсилають відповідне значення модуля p_j, значення виходу третього пристрою додавання 14 встановлюють рівним нулю і встановлюють в початкове положення лічильник 1, згідно початкової адреси оперативно запам'ятовуючого пристрою 4, в який заносять інформаційні дані M, які подають у вигляді послідовності $M=\{m_1, m_2,..., m_t\}$. З лічильника 1 отримують номер i-го елемента інформаційної послідовності, який надсилають за допомогою першого блока комутації 2 до оперативно запам'ятовуючого пристрою 4, де на виході отримують значення i-го елемента інформаційної послідовності m_i, який надсилають до блока затримки через другий блок комутації 5 і до першого пристрою піднесення до степеня за модулем 6, на якому виконують піднесення елемента інформаційної послідовності m_i, до степеня a, значення якого надходить з регістра 7, за модулем q, отриманим з регістра 8. Значення з виходу першого пристрою піднесення до степеня за модулем 6 надсилають на перший пристрій додавання 3, де розраховують зміщення номера елемента інформаційної послідовності, який через перший блок комутації 2 надсилають в оперативно запам'ятовуючий пристрій 4. Значення з оперативно запам'ятовуючого пристрою 4 надсилають до другого пристрою додавання 9 через другий блок комутації 5, де його додають до значення з вихода блока затримки 10. Результат додавання з виходу другого пристрою додавання 9 надсилають в блок зберігання даних

11, паралельно w пристроїв додавання 12_1, 12_2, …, 12_w додають w складових великого секретного ключа k, які одночасно надходять з регістрів 13_1, 13_2, …, 13_w на відповідні перші входи пристроїв додавання 12_1, 12_2, …, 12_w і результат додавання, який одночасно надходить на відповідні другі входи пристроїв додавання 12_1, 12_2, …, 12_w, з виходу третього пристрою додавання 14, отримані результати k^*_{j1}, …, k^*_{jw} на пристроях додавання 12_1, 12_2, …, 12_w відповідно, одночасно надсилають на відповідні другі входи пристроїв піднесення за модулем 15_1, 15_2, …, 15_w. Одночасно з w виходів блока зберігання даних 11 на відповідні перші входи пристроїв піднесення за модулем 15_1, 15_2, …, 15_w надсилають w частин елемента даних s, де згідно вхідних значень з відповідних пристроїв додавання 12_1, 12_2, …, 12_w виконують піднесення до степеня за модулями p_1, p_2, …, p_w, які отримують з відповідних регістрів 16_1, 16_2, …, 16_w. Отримані результати з виходів пристроїв піднесення за модулем 15_1, 15_2, …, 15_w надсилають на відповідні w входи третього пристрою додавання 14, де всі w результатів додають. На останній ітерації хешування формується вихідне значення хешу H, яке є результатом конкатенації всіх результатів з виходів w блоків піднесення за модулем 15_1, 15_2, …, 15_w.



Комп'ютерна верстка А. Крижанівський 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