УКРАЇНА

(19) UA (11) 55699 (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) u201006266
(22) 25.05.2010
(24) 27.12.2010
(46) 27.12.2010, Бюл.№ 24, 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 $M=\{m_1, m_2, ..., m_l\}$, хешування інформаційних даних виконують шляхом піднесення до степеня інформаційних даних M за модулем великого простого числа за допомогою пристрою піднесення до степеня за модулем, яке здійснюють для результату додавання за допомогою третього пристрою додавання значень блоків даних, адреси яких паралельно обчислюють як результат додавання секретного числа a і значення лічильника i (i=1, 2, ..., l) за допомогою першого пристрою додавання та додавання секретного числа b і значення лічильника i за допомогою другого пристрою додавання, ключові дані доповнюють секретними числами a та b, ключові дані K представляють у вигляді послідовності $K=\{k_1, k_2, ..., k_q, a, b\}$, а суму елементів інформаційної послідовності $m_{i-a}+m_{i-b}$ розбивають на q частин, кожну j-ту (j=1, 2, ..., q) частину $(m_{i-a}+m_{i-b})_j$ підносять до степеня за модулем простого числа p_j, степінь, до якого виконують піднесення, отримують шляхом додавання за допомогою (j+3)-го пристрою додавання елемента ключової послідовності k_j та значення результату об'єднання h^*_{i-1} результатів піднесення до степеня за модулем простого числа, отриманих на попередньому кроці, піднесення до степеня за модулем кожної j-ї частини суми елементів інформаційної послідовності $m_{i-a}+m_{i-b}$ виконують паралельно, який **відрізняється** тим, що об'єднання h^*_{i-1} результатів піднесення до степеня за модулем отримують шляхом множення всіх значень h_{i-1j} результатів піднесення до степеня за модулем суми елементів інформаційної послідовності $(m_{i-1-a}+m_{i-1-b})_j$, результуючим хеш-значенням є результат об'єднання h^*_l результатів піднесення до степеня за модулем, отриманий після останньої ітерації.

Корисна модель відноситься до галузі криптографічного захисту інформації і може бути використана в засобах забезпечення цілісності даних у системах обробки та передачі даних.

Відомий спосіб ключового хешування теоретично доведеної стійкості [Патент України №36582 від 27.10.2008р., м.кл. G09C1/00, бюл. №20 2008р.], 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 та особистого ключа k^*, а хешування інформаційних даних виконують за допомогою пристрою піднесення до степеня за модулем елементів m_i інформаційної послідовності M та елементів ключової послідовності K за ітеративним правилом піднесення до степеня значення елемента інформаційної послідовності 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 секретними числами a та b, а ітеративне правило піднесення до степеня за модулем великого простого числа p здійснюють для результату додавання значень блоків даних, надалі елементів інформаційної послідовності, адреси яких паралельно обчислюють як результат додавання секретного числа a і значення лічильника i за допомогою першого пристрою додавання та додавання секретного числа b і значення лічильника i за допомогою другого пристрою додавання.

Недоліком аналогу є недостатня швидкість хешування, в зв'язку з тим, що для обробки i-го елемента інформаційної послідовності необхідно попередньо обчислити хеш-значення для всіх попередніх i-1 елементів інформаційної послідовності, а отже необхідно l ітерацій піднесення до степеня для обробки всіх елементів інформаційної послідовності m_i.

(19) UA (11) 55699 (13) U

Найбільш близьким до способу, що пропонується, є спосіб паралельного ключового хешування теоретично доведеної стійкості [Патент України №42220 від 25.06.2009р., м.кл. G09C1/00, бюл. №12 2009р.], який полягає в тому, що інформаційні дані M подають у вигляді послідовності $M=\{m_1, m_2, ..., m_l\}$, а хешування інформаційних даних виконують за допомогою пристрою піднесення до степеня за модулем інформаційних даних M за ітеративним правилом піднесення до степеня за модулем великого простого числа, яке здійснюють для результату додавання за допомогою третього пристрою додавання значень блоків даних, адреси яких паралельно обчислюють як результат додавання секретного числа a і значення лічильника i (i=1, 2, ..., l) за допомогою першого пристрою додавання та додавання секретного числа b і значення лічильника i за допомогою другого пристрою додавання, ключові дані доповнюють секретними числами a та b, ключові дані K представляють у вигляді послідовності $K=\{k_1, k_2,..., k_q, a, b\}$, а суму елементів інформаційної послідовності $m_{i-a} + m_{i-b}$ розбивають на q частин, кожну j-ту (j=1, 2, ..., q) частину підносять до степеня, який отримують шляхом додавання за допомогою (j+3)-го пристрою додавання елемента ключової послідовності k_j та суми результатів піднесення до степеня, отриманих на попередньому кроці, за модулем простого числа p_j, піднесення до степеня за модулем кожної j-тої частини суми елементів інформаційної послідовності $m_{i-a}+m_{i-b}$ виконують паралельно.

Недоліком прототипу є недостатня криптографічна стійкість хешування, пов'язана з тим, що результат хешування отримують шляхом конкатенації результатів піднесення до степеня частин суми елементів інформаційного повідомлення $(m_{i-a}+m_{i-b})_j$, яка дає лінійний приріст складності з ростом кількості блоків піднесення до степеня, а об'єднання проміжних результатів хешування h_{ij} виконують за допомогою лінійної операції додавання.

В основу корисної моделі поставлена задача створити спосіб паралельного ключового хешування, який дозволить забезпечити підвищену криптографічну стійкість хешування інформації за рахунок об'єднання проміжних результатів хешування h_{ij} за допомогою нелінійної операції та використання результату об'єднання як результуючого значення хешування за рахунок введення нових операцій.

Поставлена задача вирішується за рахунок того, що інформаційні дані M подають у вигляді послідовності $M=\{m_1, m_2, ..., m_l\}$, хешування інформаційних даних виконують шляхом піднесення до степеня інформаційних даних M за модулем великого простого числа за допомогою пристрою піднесення до степеня за модулем, яке здійснюють для результату додавання за допомогою третього пристрою додавання значень блоків даних, адреси яких паралельно обчислюють як результат додавання секретного числа a і значення лічильника i (i=1, 2, ..., l) за допомогою першого пристрою додавання та додавання секретного числа b і значення лічильника i за допомогою другого пристрою додавання, ключові дані доповнюють секретними числами a та b, ключові дані K представляють у вигляді послідовності $K=\{k_1, k_2,..., k_q, a, b\}$, а суму елементів інформаційної послідовності $m_{i-a} + m_{i-b}$ розбивають на q частин, кожну j-ту (j=1, 2, ..., q) частину $(m_{i-a}+m_{i-b})_j$ підносять до степеня за модулем простого числа p_j, степінь, до якого виконують піднесення отримують шляхом додавання за допомогою (j+3)-го пристрою додавання елемента ключової послідовності k_j та значення результату об'єднання h^*_{i-1} результатів піднесення до степеня за модулем простого числа, отриманих на попередньому кроці, піднесення до степеня за модулем кожної j-ї частини суми елементів інформаційної послідовності $m_{i-a}+m_{i-b}$ виконують паралельно, причому об'єднання h^*_{i-1} результатів піднесення до степеня отримують шляхом множення всіх значень результатів h_{i-1j} піднесення до степеня частин суми елементів інформаційної послідовності $(m_{i-1-a}+m_{i-1-b})_i$. за модулем p_j, а результуючим хеш-значенням є результат об'єднання h^*_1 результатів піднесення до степеня за модулем, отриманий після останньої ітерації.

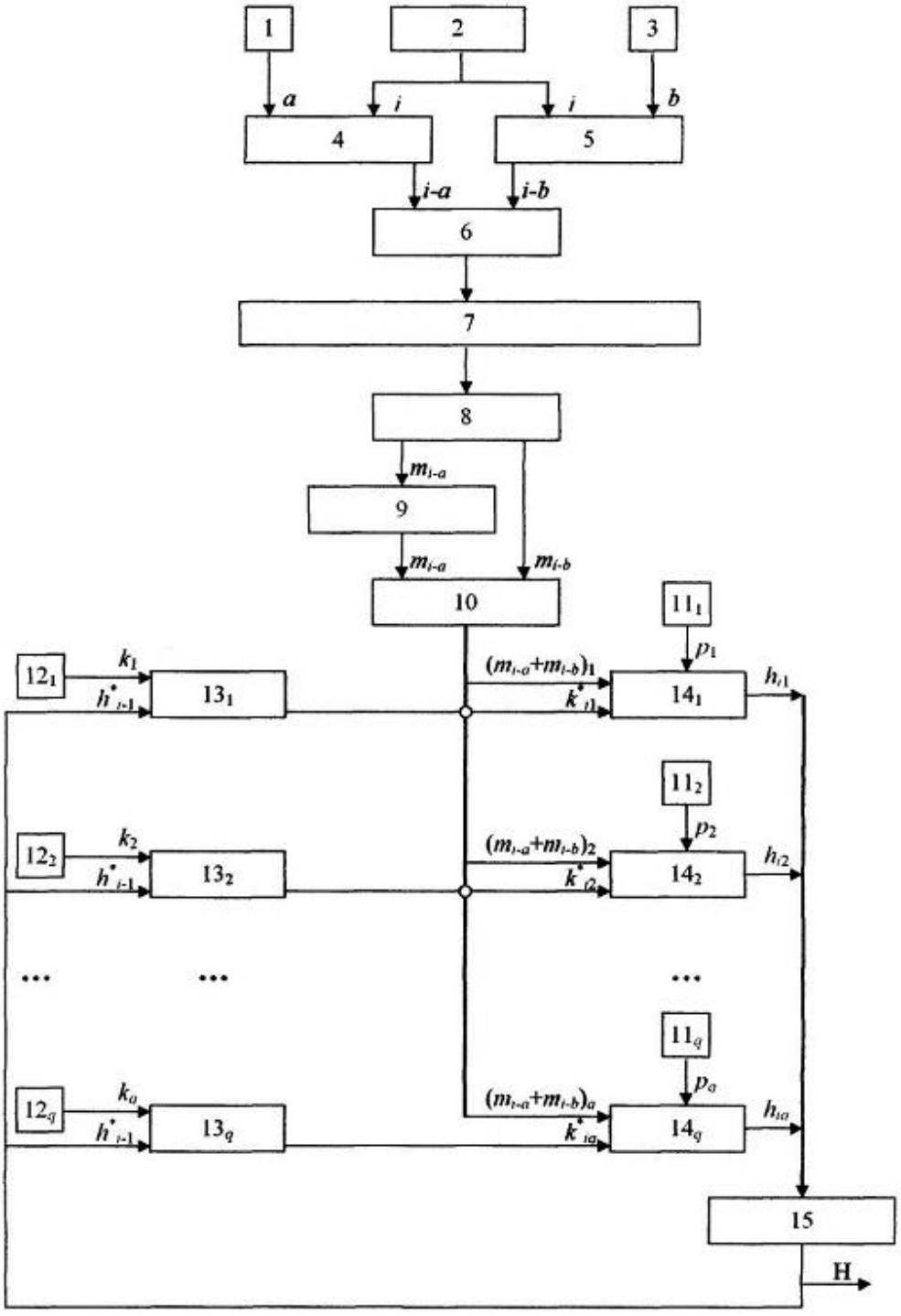
На кресленні наведена схема пристрою, що реалізує спосіб паралельного ключового хешування.

Пристрій містить лічильник 2, вихід якого з'єднано з першим входом першого пристрою додавання 4 та першим входом другого пристрою додавання 5, вихід регістра зберігання секретного числа a 1 з'єднано з другим входом першого пристрою додавання 4, вихід регістра зберігання секретного числа b 3 з'єднано з другим входом другого пристрою додавання 5, вихід першого пристрою додавання 4 з'єднано з першим входом першого блока комутації 6, а вихід другого пристрою додавання 5 з'єднано з другим входом першого блока комутації 6. Вихід першого блока комутації 6 є входом оперативно запам'ятовуючого пристрою 7, вихід якого є входом другого блока комутації 8. Перший вихід другого блока комутації 8 є першим входом третього пристрою додавання 10, другий вихід другого блока комутації 8 з'єднано з входом блока затримки 9, вихід якого є другим входом третього пристрою додавання 10, j-ий вихід якого з'єднано з першим входом j-го пристрою піднесення до степеня за модулем 14_j, вихід якого є j-им входом пристрою множення 15. Вихід пристрою множення 15 є другим входом (j+3)-го пристрою додавання 13_j та виходом всього пристрою. Вихід регістра зберігання елемента ключової послідовності k_j 12_j з'єднано з першим входом (j+3)-го пристрою додавання 13_j, вихід якого з'єднано з другим входом y-го пристрою піднесення до степеня за модулем 14_j. Вихід регістра зберігання значення модуля p_j 11_j є третім входом j-го пристрою піднесення до степеня за модулем 14_j.

Здійснення способу паралельного ключового виконують на пристрої таким чином.

В регістр зберігання секретного числа a 1 заносять значення параметра a, в регістр зберігання секретного числа b 3 заносять значення параметра b, в регістр зберігання елемента ключової послідовності k_j 12_j заносять значення параметра k_j, в регістр зберігання значення модуля p_j 11_j заносять значення модуля p_j, встановлюють в початкове

положення лічильник 2 згідно початкової адреси оперативно запам'ятовуючого пристрою 7, в який заносять інформаційні дані M, які подають у вигляді послідовності $M=\{m_1, m_2, ..., m_l\}$. Значення виходу пристрою множення 15 встановлюють рівним нулю. Починають ітеративний процес. З лічильника 2 отримують адресу i-го елемента інформаційної послідовності в оперативно запам'ятовуючому пристрої 7, яку надсилають до першого пристрою додавання 4 та другого пристрою додавання 5, на виході першого пристрою додавання 4 отримують адресу (i-a)-го елемента інформаційної послідовності, яку надсилають за допомогою першого блока комутації 6 до оперативно запам'ятовуючого пристрою 7. На виході оперативно запам'ятовуючого пристрою 7, отримують значення (i-a)-го елемента інформаційної послідовності m_{i-a}, який надсилають до блока затримки 9 за допомогою другого блока комутації 8. Значення отриманої адреси (i-b)-го елемента інформаційної послідовності з виходу другого пристрою додавання 5 надсилають за допомогою першого блока комутації 6 на вхід оперативно запам'ятовуючого пристрою 7, з виходу якого отримують значення (i-b)-го елемента інформаційної послідовності m_{i-b} та надсилають його до третього пристрою додавання 10 за допомогою другого блока комутації 8, де його додають до значення з виходу блока затримки 9. Одночасно додають за допомогою (j+3)-го пристрою додавання 13_j частину ключа k_j, що зберігається в регістрі зберігання елемента ключової послідовності k_j 12_j, та значення виходу пристрою множення 15 j-ту частину результату додавання (i-a)-го та (i-b)-го елементів інформаційної послідовності $(m_{i-a}+m_{i-b})_j$ надсилають на вхід j-го пристрою піднесення до степеня за модулем 14_j, де згідно вхідних значень з (j+3)-го пристрою додавання 13_j виконують піднесення до степеня за модулем p_j, отриманим з виходу регістра зберігання значення модуля p_j 11_j. Результат h_{ij} отриманий в j-му пристрої піднесення до степеня за модулем 14_j, надсилають на j-ий вхід пристрою множення 15, за допомогою якого визначають результат об'єднання h^*_i всіх результатів піднесення до степеня h_{ij}, який надсилають на вхід (j+3)-го пристрою додавання 13_j та на вихід всього пристрою. Після цього починають наступну ітерацію. Результуючим хеш-значенням H буде результат об'єднання h^*_l, отриманий після завершення l-ої ітерації.



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