УКРАЇНА

(19) UA (11) 48267 (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) u200909858
(22) 28.09.2009
(24) 10.03.2010
(46) 10.03.2010, Бюл.№ 5, 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 $M=\{m_1, m_2, ..., m_t\}$, 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 α і значення лічильника i (i=1, 2, ..., t) за допомогою першого пристрою додавання та додавання секретного числа b і значення лічильника i за допомогою другого пристрою додавання, ключові дані доповнюють секретними числами α та b, ключові дані K представляють у вигляді послідовності $K=\{k_l, k_2, ..., k_w, \alpha, b\}$, а суму елементів інформаційної послідовності $m_{i-a}+m_{i-b}$ розбивають на w частин, кожну u-ту (u=1, 2, ..., w) частину підносять до степеня, який отримують шляхом 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 u-тої частини суми елементів інформаційної послідовності $m_{i-a}+m_{i-b}$ виконують паралельно, який **відрізняється** тим, що степінь, до якого підносять частину суми елементів інформаційної послідовності $m_{i-a}+m_{i-b}$, отримують шляхом додавання результатів піднесення до степеня, отриманих на попередньому кроці на u-му та (u-1)mod w-му блоках піднесення за модулем.

1

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, м. кл. G09C 1/00, бюл. №20 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 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 t ітерацій піднесення до степеня для обробки всіх елементів інформаційної послідовності m_i.

Найбільш близьким до способу, що пропонується, є спосіб паралельного ключового хешування теоретично доведеної стійкості (патент України №4220, м. кл. G09C 1/00, бюл. №12, 2009р.), який полягає в тому, що інформаційні дані M подають у вигляді послідовності $M=\{m_1, m_2, ..., m_t\}$, а хешування інформаційних даних виконують за допомогою пристрою піднесення до степеня за модулем інформаційних даних M за ітеративним правилом

(19) UA (11) 48267 (13) U

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 і за допомогою першого пристрою додавання та додавання секретного числа b і значення лічильника і за допомогою другого пристрою додавання, ключові дані доповнюють секретними числами a та b, причому ключові дані K представляють у вигляді послідовності $K=\{k_1, k_2, ..., k_w, a, b\}$, а суму елементів інформаційної послідовності $m_{i-a}+m_{i-b}$ розбивають на w частин, кожну u-ту (u=1, 2, ..., w) частину підносять до степеня, який отримують шляхом додавання за допомогою (u+3)-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 u-тої частини суми елементів інформаційної послідовності $m_{i-a}+m_{i-b}$ виконують паралельно.

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.

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

Поставлена задача вирішується за рахунок того, що в способі паралельного ключового хешування інформаційні дані M подають у вигляді послідовності $M=\{m_1, m_2, ..., m_t\}$, 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, ..., t) за допомогою першого пристрою додавання та додавання секретного числа b і значення лічильника і за допомогою другого пристрою додавання, ключові дані доповнюють секретними числами a та b, ключові дані K представляють у вигляді послідовності $K=\{k_1, k_2,..., k_w, a, b\}$, а суму елементів інформаційної послідовності $m_{i-a}+m_{i-b}$ розбивають на w частин, кожну u-ту (u=1, 2, ..., w) частину підносять до степеня, який отримують шляхом 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 u-тої частини суми елементів інформаційної послідовності $m_{i-a}+m_{i-b}$ виконують паралельно, причому степінь, до якого підносять частину суми елементів інформаційної послідовності $m_{i-a}+m_{i-b}$, отримують шляхом додавання результатів піднесення до степеня, отриманих на попередньому кроці на u-му та (u-1)mod w-му блоках піднесення за модулем.

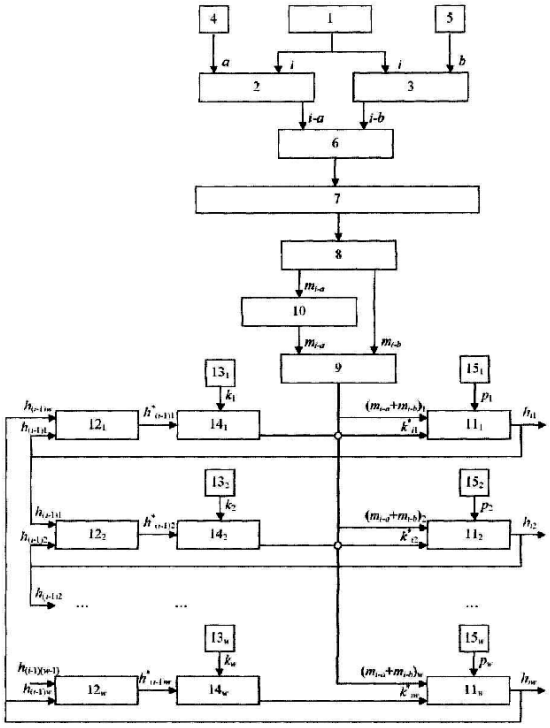
На кресленні приведена схема пристрою, що реалізує спосіб паралельного ключового хешування.

Пристрій містить лічильник 1, вихід якого з'єднано з першим входом першого пристрою додавання 2 та першим входом другого пристрою додавання 3, вихід регістра зберігання секретного числа a 4 з'єднано з другим входом першого пристрою додавання 2, вихід регістра зберігання секретного числа b 5 з'єднано з другим входом другого пристрою додавання 3, вихід першого пристрою додавання 2 з'єднано з першим входом першого блока комутації 6, а вихід другого пристрою додавання 3 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 9, другий вихід другого блока комутації 8 з'єднано з входом блока затримки 10, вихід якого є другим входом третього пристрою додавання 9, u-ий вихід якого з'єднано з першим входом u-го пристрою піднесення до степеня за модулем 11_u, вихід якого є першим входом (u+3)-го пристрою додавання 12_u, другим входом ((u+1)mod w+3)-го пристрою додавання $12_{(u+1)\bmod w}$ та u-им виходом всього пристрою. Вихід (w+3)-го пристрою додавання 12_u є другим входом (w+u+3)-го пристрою додавання 14_u. Вихід регістра зберігання елемента ключової послідовності k_u 13_u з'єднано з першим входом (w+u+3)-го пристрою додавання 14_u, вихід якого з'єднано з другим входом u-го пристрою піднесення до степеня за модулем 11_u. Вихід регістра зберігання значення модуля p_u 15_u є третім входом u-го пристрою піднесення до степеня за модулем 11_u.

Здійснення способу паралельного ключового хешування виконують на пристрої таким чином.

В регістр зберігання секретного числа a 4 заносять значення параметра a, в регістр зберігання секретного числа b 5 заносять значення параметра b, в регістр зберігання елемента ключової послідовності k_u 13_u заносять значення параметра k_u, в регістр зберігання значення модуля p_u 15_u заносять значення параметра p_u, встановлюють в початкове положення лічильник 1 згідно початкової адреси оперативно запам'ятовуючого пристрою 7, в який заносять інформаційні дані M, які подають у вигляді послідовності $M=\{m_1, m_2, ..., m_t\}$. Значення виходу (u+3)-го пристрою додавання 12_u встановлюють рівним нулю. Починають ітеративний процес. З лічильника 1 отримують попередню адресу i-го елемента інформаційної послідовності в оперативно запам'ятовуючому пристрої 7, яку надсилають до першого пристрою додавання 2 та другого пристрою додавання 3, на виході першого пристрою додавання 2 отримують адресу (i-a)-го елемента інформаційної послідовності, яку надсилають за допомогою першого блока комутації 6 до оперативно запам'ятовуючого пристрою 7, разом із значенням отриманої адреси (i-b)-го елемента інформаційної послідовності з виходу другого пристрою додавання 3, яку надсилають за допомогою першого блока комутації 6. На виході оперативно

запам'ятовуючого пристрою 7, отримують значення (i-a)-го елемента інформаційної послідовності m_{i-a}, який надсилають до блока затримки 10 за допомогою другого блока комутації 8, значення (i-b)-го елемента інформаційної послідовності m_{i-b} з виходу оперативно запам'ятовуючого пристрою 7, надсилають до третього пристрою додавання 9 за допомогою другого блока комутації 8, де його додають до значення з виходу блока затримки 10. Додають за допомогою (w+u+3)-го пристрою додавання 14_u частину ключа k_u, що зберігається в регістрі зберігання елемента ключової послідовності k_u 13_u, та значення виходу (u+3)-го пристрою додавання 12_u. u-ту частину результату додавання (i-a)-го та (i-b)-го елементів інформаційної послідовності $(m_{i-a}+m_{i-b})_u$ надсилають на вхід u-го пристрою піднесення до степеня за модулем 11_u, де згідно вхідних значень з (w+u+3)-го пристрою додавання 14_u виконують піднесення до степеня за модулем p_u, отриманим з виходу регістра зберігання значення модуля p_u 15_u. Результат h_{iu}, отриманий в u-му пристрої піднесення до степеня за модулем 11_u, надсилають на перший вхід (w+3)-го пристрою додавання 12_u, на другий вхід ((u+1)mod w+3)-го пристрою додавання $12_{(u+1)\bmod w}$ та на u-ий вихід всього пристрою. За допомогою (w+3)-го пристрою додавання 12_u визначають суму $h^*_{(i-1)u}$ та надсилають на вхід (w+u+3)-го пристрою додавання 14_u. Результуючим хеш-значенням H буде результат конкатенації всіх h_{tu}.



Фіг.

Комп'ютерна верстка Л. Купенко 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