УКРАЇНА

(19) UA (11) 57342 (13) U

(51) МПК (2011.01)
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) u201008801
(22) 15.07.2010
(24) 25.02.2011
(46) 25.02.2011, Бюл.№ 4, 2011 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 $M=\{m_1,m_2,\ldots,m_l\}$, ключові дані K подають у вигляді послідовності $k=\{k_1,k_2,\ldots,k_q\}$, хешування інформаційних даних виконують за допомогою пристрою піднесення до степеня за модулем шляхом піднесення до степеня суми $(m_i+m_{i-u_i})$ $(i-1,2,\ldots,l)$ елементів інформаційної послідовності M за модулем великого простого числа p, число u_i обчислюють як псевдовипадкове число, що залежить від значення елемента інформаційної послідовності m_i, суму $(m_i+m_{i-u_i})$ елементів інформаційної послідовності розбивають на q частин, кожну частину суми $(m_i+m_{i-u_i})_j$ паралельно підносять до степеня, який отримують шляхом додавання, за допомогою пристрою додавання, елемента ключової послідовності k_j та результату об'єднання h^*_{i-1} результатів піднесення до степеня, отриманих після попередньої ітерації, за модулем простого числа p_j за допомогою j-го пристрою піднесення до степеня за модулем, 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 частини суми елементів інформаційної послідовності $(m_{i-1}+m_{i-1-u_i})_j$, а результуючим хеш-значенням є результат об'єднання h^*_l результатів піднесення до степеня за модулем, отриманий після останньої ітерації.

Корисна модель належить 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 25.11.2008 р., м. кл. G 09 C 1/00, бюл. № 22, 2008 р.], який полягає в тому, що інформаційні дані M подають у вигляді послідовності $M=\{m_1,m_2,\ldots,m_l\}$, 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 b, 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 b.

Недоліком аналогу є недостатня швидкість

(19) UA (11) 57342 (13) U

хешування, в зв'язку з тим, що для обробки і-го елемента інформаційної послідовності необхідно попередньо обчислити хеш - значення для всіх попередніх $i-1$ елементів інформаційної послідовності, а отже необхідно l ітерацій операції піднесення до степеня над елементами інформаційної послідовності повної розрядності для їх хешування.

Найбільш близьким за сукупністю ознак є спосіб паралельного ключового хешування теоретично доведеної стійкості [Патент України № 43511 від 25.08.2009 р., м. кл. G 09 C 1/00, бюл. № 16, 2009 р.], який полягає в тому, що інформаційні дані M подають у вигляді послідовності $M=\{m_1,m_2,\ldots,m_l\}$, ключові дані K подають у вигляді великого секретного ключа k, секретного числа a і секретного простого числа b, а хешування інформаційних даних виконують за допомогою пристрою піднесення до степеня, в подальшому пристрою піднесення до степеня за модулем, елементів m_i $(i=1,2,\ldots,l)$ 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 b, великий секретний ключ k представляють у вигляді послідовності $k=\{k_1,k_2,\ldots,k_q\}$, а результат додавання s розбивають на q частин, кожну з яких s_j $(j=1,2,\ldots,q)$ 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.

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 $(m_i+m_{i-u_i})_j$, яка дає лінійний приріст складності з ростом кількості проміжних результатів хешування, отриманих на пристроях піднесення до степеня за модулем, 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 $M=\{m_1,m_2,\ldots,m_l\}$, ключові дані K подають у вигляді послідовності $k=\{k_1,k_2,\ldots,k_q\}$, хешування інформаційних даних виконують за допомогою пристрою піднесення до степеня за модулем шляхом піднесення до степеня суми $(m_i+m_{i-u_i})$ $(i=1,2,\ldots,l)$ елементів інформаційної послідовності M за модулем великого простого числа p, число u_i обчислюють як псевдовипадкове число, що залежить від значення елемента інформаційної послідовності m_i, суму $(m_i+m_{i-u_i})$ елементів інформаційної послідовності розбивають на q частин, кожну частину суми $(m_i+m_{i-u_i})_j$ паралельно підносять до степеня, який отримують шляхом додавання, за допомогою пристрою додавання, елемента ключової послідовності k_j та результату об'єднання h^*_{i-1} результатів піднесення до степеня, отриманих після попередньої ітерації, за модулем простого числа p_j за допомогою j-го пристрою піднесення до степеня за модулем, 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 частини суми елементів інформаційної послідовності $(m_{i-1}+m_{i-1-u_i})_j$, а результуючим хеш - значенням є результат об'єднання h^*_l результатів піднесення до степеня за модулем, отриманий після останньої ітерації.

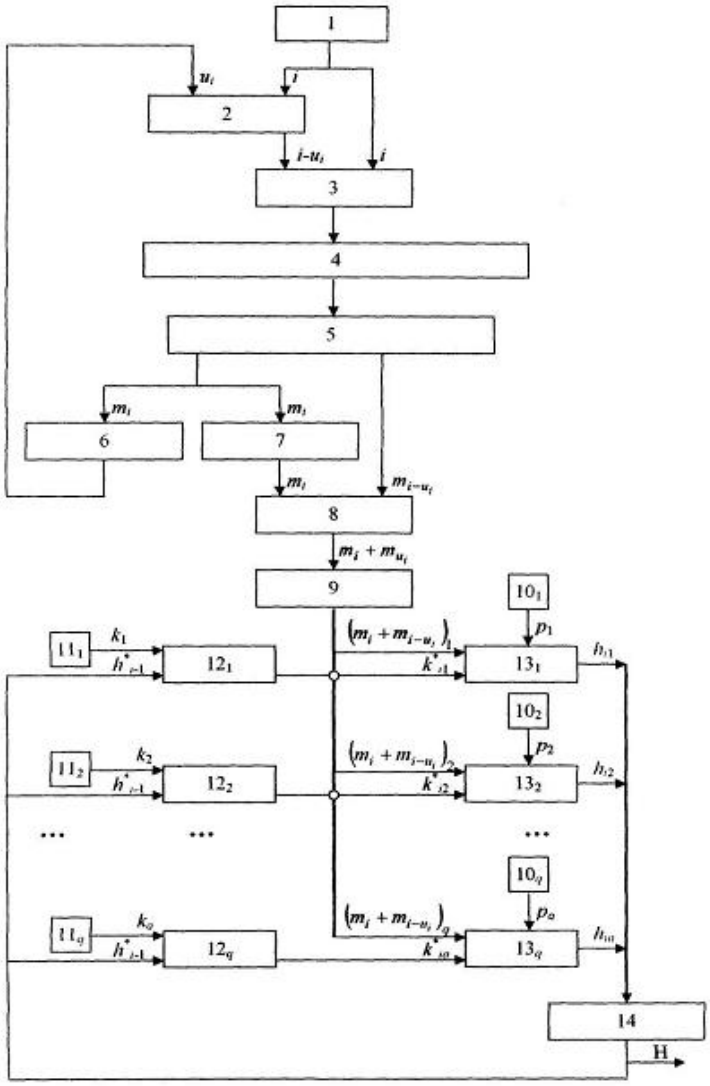
На кресленні наведена схема пристрою, що реалізує спосіб паралельного ключового хешування.

Пристрій містить лічильник 1, вихід якого з'єднано з першим входом першого блока комутації 3 та першим входом першого пристрою додавання 2, вихід якого з'єднано з другим входом першого блока комутації 3. Вихід першого блока комутації 3 є входом оперативно запам'ятовуючого пристрою 4, вихід якого є входом другого блока комутації 5. Перший вихід другого блока комутації 5 з'єднано з входом блока генерації псевдовипадкових чисел 6 та входом блока затримки 7. Вихід блока генерації псевдовипадкових чисел 6 є другим входом першого пристрою додавання 3. Другий вихід другого блока комутації 5 є першим входом другого пристрою додавання 8, другим входом якого є вихід блока затримки 7. Вихід другого пристрою додавання 8 з'єднано з входом блока розділення даних 9, j-й вихід якого з'єднано з першими входом j-го пристрою піднесення до степеня за модулем 13_j, вихід якого є j-м входом пристрою множення 14.

Вихід пристрою множення 14 є виходом всього пристрою та першим входом $(j+2)$-го пристрою додавання 12_j. Другим входом $(j+2)$-го пристрою додавання 12_j є вихід блока зберігання елемента ключової послідовності k_j 11_j. Вихід $(j+2)$-го пристрою додавання 12_j є другим входом j-го пристрою піднесення до степеня за модулем 13_j. Третім входом j-го пристрою піднесення до степеня за модулем 13_j є вихід блока зберігання модуля p_j 10_j.

Спосіб паралельного ключового хешування виконують на пристрої таким чином.

У блок зберігання елемента ключової послідовності k_j 11_j заносять значення елемента ключової послідовності k_j, у блока зберігання модуля p_j 10_j надсилають значення модуля p_j, значення виходу блока множення 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 $M=\{m_1,m_2,\ldots,m_l\}$. Починають ітеративний процес. З лічильника 1 отримують адресу і-то елемента інформаційного повідомлення, яку надсилають на вхід першого блока додавання 2 та до першого блока комутації 3 за допомогою якого його надсилають далі до оперативно запам'ятовуючого пристрою 4, де на виході отримують значення і-го елемента інформаційного повідомлення m_i, яке надсилають за допомогою другого блока комутації 5 на вхід блока генерації псевдовипадкових чисел 6 та на блок затримки 7. З виходу блока генерації псевдовипадкових чисел отримують значення псевдовипадкового числа u_i, яке надсилають на вхід першого блока додавання 2, де його віднімають від адреси і-го елемента інформаційної послідовності. Отриману адресу $(i-u_i)$-го елемента інформаційної послідовності надсилають за допомогою першого блока комутації 3 до оперативно запам'ятовуючого пристрою 4. Значення $(i-u_i)$-го елемента інформаційної послідовності m_{i-u_i} з виходу оперативно запам'ятовуючого пристрою 4 надсилають за допомогою другого блока комутації 5 до другого пристрою додавання 8, де його додають із значенням, що надходить з виходу блока затримки 7. Отриману суму $m_i+m_{i-u_i}$ з виходу другого блока додавання надсилають до блока розділення даних 9, де її розділяють на q частин. Кожну j-ту частину суми $(m_i+m_{i-u_i})_j$ надсилають на вхід j-го пристрою піднесення до степеня за модулем 13_j. Одночасно за допомогою $(j+2)$-го пристрою додавання 12_j додають значення з виходу пристрою множення 14 та блока зберігання елемента ключової послідовності k_j 11_j. Отриманий результат надсилають до j-го пристрою піднесення до степеня за модулем 13_j, де його використовують як показник степеня для піднесення до степеня j-ої частини суми $(m_i+m_{i-u_i})_j$ за модулем p_j, значення якого отримують з виходу блока зберігання модуля p_j 10_j. Результат h_{ij}, отриманий в j-му пристрої піднесення до степеня за модулем 13_j, надсилають на j-ий вхід пристрою множення 14, за допомогою якого визначають результат об'єднання h_l^* всіх результатів піднесення до степеня h_{ij}, який надсилають на вхід $(j+2)$-го пристрою додавання 12_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 Л. Купенко Підписне Тираж 23 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