УКРАЇНА

(19) UA (11) 36582 (13) U

(51) МПК (2006)
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 КЛЮЧОВОГО ХЕШУВАННЯ ТЕОРЕТИЧНО ДОВЕДЕНОЇ СТІЙКОСТІ

(21) u200808802
(22) 04.07.2008
(24) 27.10.2008
(46) 27.10.2008, Бюл.№ 20, 2008 р.
(72) ЛУЖЕЦЬКИЙ ВОЛОДИМИР АНДРІЙОВИЧ, UA, БАРИШЕВ ЮРІЙ ВОЛОДИМИРОВИЧ, UA, ДМИТРИШИН ОЛЕКСАНДР ВАСИЛЬОВИЧ, UA
(73) ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ, UA
(57) Спосіб ключового хешування теоретично доведеної стійкості, який полягає в тому, що інформаційні дані М подають у вигляді послідовності М = $\{m_1, m_2,...,m_t\}$, ключові дані К подають у вигляді великого секретного числа k та особистого ключа k*, а хешування інформаційних даних виконують за допомогою пристрою множення елементів m_t інформаційної послідовності М та елементів ключової послідовності К за ітеративним правилом піднесення до степеня значення блока даних за модулем великого простого числа р, степінь, до якого здійснюють піднесення, отримують шляхом додавання особистого ключа k* та результату попередньої ітерації хешування за допомогою пристрою додавання, який **відрізняється** тим, що ключові дані доповнюють секретними числами а та b, а ітеративне правило піднесення до степеня за модулем великого простого числа р здійснюють для результату додавання значень блоків даних, адреси яких паралельно обчислюють як результат додавання секретного числа а і значення лічильника і за допомогою першого пристрою додавання та додавання секретного числа b і значення лічильника і за допомогою другого пристрою додавання.

1 2

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 хешування даних [Halevi S., Krawczyk H. MMH: Software Message Authentication in the Gbit/second Rates // J. of Computing, Vol.16. - No.2. - P.133-140.] ґрунтується на тому, що інформаційні дані подають у вигляді послідовності блоків $M=\{m_1,m_2,...,m_t\}$, ключові дані подають у вигляді послідовності блоків $X=\{x_1,x_2,...,x_t\}$, а хешування інформаційних даних виконують за допомогою пристроїв множення по ітераційному правилу:

$$g_X(m) = \sum_{i=1}^{t} m_i x_i \bmod p,$$

що реалізує відображення вигляду:

$$MMH = \left\{ g_X : Z_p^t \to Z_p \middle| M \in Z_p^t \right\},$$

де $g_X(m)$ - хеш-код; Z_p^t - кільце цілих чисел по модулю р, р - просте число.

Недоліками цього способу є залежність обчислювальної стійкості хешування від властивостей та періоду генератора випадкових послідовностей, за допомогою якого формують ключову послідовність $X=\{x_1, x_2,..., x_t\}$ та неспроможність теоретичного доведення обчислювальної стійкості ключового хешування.

Найбільш близьким до способу, що пропонується є спосіб ключового хешування теоретично доведеної стійкості [Патент України №18693 від 15.11.2006 р., М. кл. G09C1/00, бюл. №11 2006 р.], 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 числа k та особистого ключа k*, а хешування інформаційних даних виконують за допомогою пристрою множення елементів m_i інформаційної послідовності М та елементів ключової послідовності К за ітеративним правилом піднесення до степеня значення блока даних за модулем великого простого числа р, степінь, до якого здійснюють піднесення, отримують шляхом додавання особистого ключа k* та результату попередньої ітерації хешування за допомогою пристрою додавання, ключові дані використовують як степінь ступеня в ітераційному правилі хешування, а задача зламу ключа хешування зводиться до обчислення дискретного логарифма в простому полі.

(19) UA (11) 36582 (13) U

Недоліком прототипу є недостатня стійкість хешування, оскільки для зламу способу хешування даних необхідне лише знаходження значення ключа, яке зводиться до знаходження значення першого блоку даних m_1.

В основу корисної моделі поставлена задача створити спосіб ключового хешування теоретично доведеної стійкості, який дозволить забезпечити підвищену обчислювальну стійкість хешування інформації за рахунок ускладнення задачі зламу ключа хешування шляхом введення додаткових арифметичних операцій.

Поставлена задача вирішується за рахунок того, що в способі ключового хешування теоретично доведеної стійкості 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, причому 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, 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; за допомогою другого пристрою додавання.

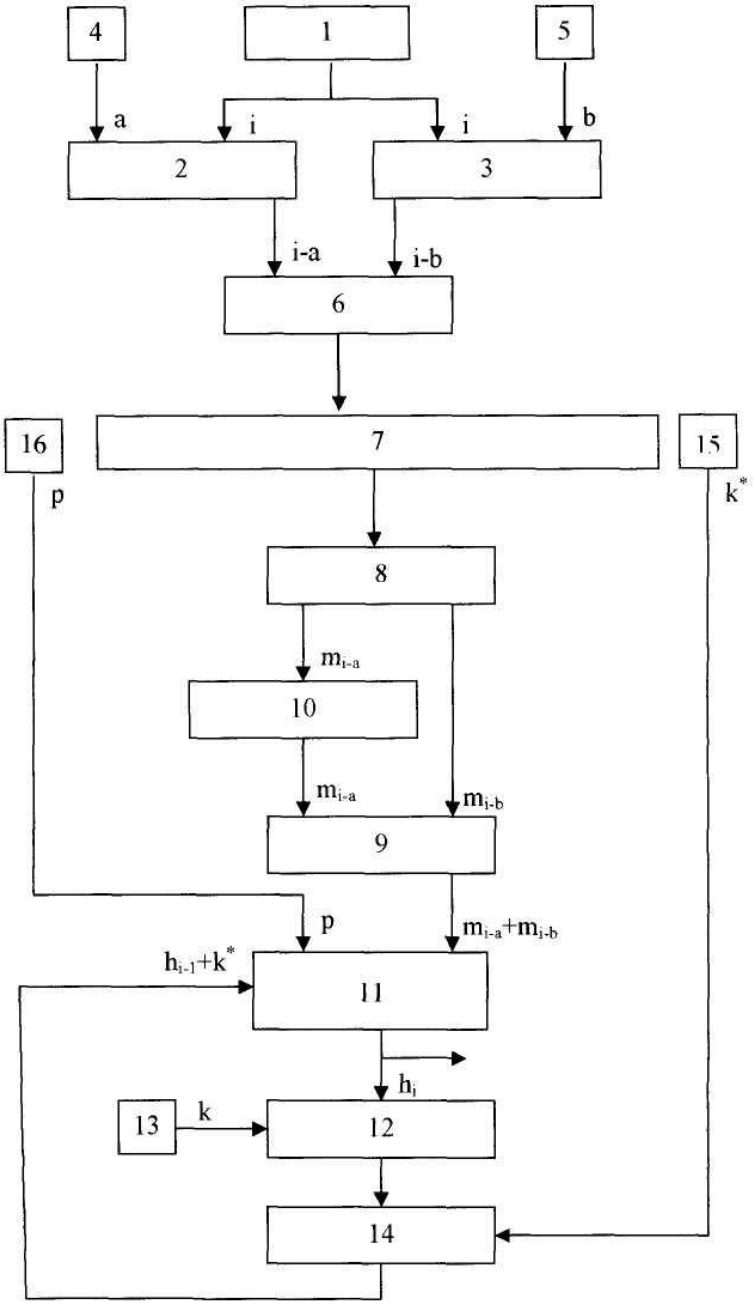
Технічний результат, який може буде отриманий при здійсненні корисної моделі, полягає в підвищенні складності задачі зламу ключа хешування без збільшення розрядності хеш-функції.

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

Пристрій містить лічильник 1, вихід якого з'єднано з першим входом першого пристрою додавання 2 та першим входом другого пристрою додавання 3, вихід регістра 4 з'єднано з другим входом першого пристрою додавання 2, вихід регістра 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. Вихід третього пристрою додавання 9 з'єднано з першим входом пристрою піднесення до степеня за модулем 11, вихід якого є першим входом третього блоку комутації 12 та виходом пристрою. Вихід регістра 13 є другим входом третього блока комутації 12, вихід якого з'єднано з першим входом четвертого пристрою додавання 14. Вихід регістра 15 з'єднано з другим входом четвертого пристрою додавання 14, вихід якого з'єднано з другим входом пристрою піднесення до степеня за модулем 11. Вихід регістра 16 є третім входом пристрою піднесення до степеня за модулем 11.

Здійснення способу ключового хешування теоретично доведеної стійкості виконують на пристрої таким чином.

В регістр 4 заносять значення параметра a, в регістр 5 заносять значення параметра b, в регістр 13 заносять значення параметра k, в регістр 15 заносять значення параметра k*, в регістр 16 заносять значення параметра p, в які надсилають відповідні частини ключової інформації K та 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 $M=\{m_1,m_2,..,m_t\}$. З лічильника 1 отримують попередню адресу i-го інформаційного блока даних 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 інформаційного блока даних, яку надсилають за допомогою першого блока комутації 6 до оперативно запам'ятовуючого пристрою 7, разом із значенням отриманої адреси (i-b)-го інформаційного блока даних 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 інформаційного блока даних m_{i-a}, який надсилають до блока затримки 10 за допомогою другого блока комутації 8, значення (i-b)-ого інформаційного блока даних 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. Результат додавання з виходу пристрою додавання 9 надсилають на вхід пристрою піднесення до степеня за модулем 11, де згідно вхідних значень з четвертого пристрою додавання 14 виконують піднесення до степеня за модулем p, отриманим з виходу регістра 16. Результат, отриманий у пристрої піднесення до степеня за модулем 11, за допомогою третього блока комутації 12 надсилають до четвертого пристрою додавання 14, де до нього додають значення k* з виходу регістра 15. На першій ітерації на четвертий пристрій додавання 4 надходить значення k з виходу регістра 13 за допомогою третього блока комутації 12. На t-ій ітерації на виході пристрою піднесення до степеня за модулем 11 отримують вихідне значення результату хешування.



Комп'ютерна верстка В. Мацело 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