УКРАЇНА

(19) UA (11) 37465 (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) u200808805
(22) 04.07.2008
(24) 25.11.2008
(46) 25.11.2008, Бюл.№ 22, 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 $M=\{m_1, m_2, ..., m_t\}$, 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, який **відрізняється** тим, що ключові дані доповнюють секретним числом α та секретним простим числом q, а ітеративне правило піднесення до степеня за модулем здійснюють для результату додавання значення блока даних m_i та значення блока даних, номер якого відрізняється від і на число, яке обчислюють за допомогою пристрою множення як результат піднесення до степеня α значення блока даних m_i за модулем q.

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

$$g_X(m)=\sum_{i=1}^{t} m_i x_1 \bmod p,$$

що реалізує відображення вигляду: $MMH=\left\{g_X : Z_p^t \to Z_p \mid M \in Z_p^t\right\}$, де $g_X(m)$ - хеш-код; Z_p^t - кільце цілих чисел за модулем 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 15.11.2006р., М. кл. G09C1/00, бюл. №11 2006р.], 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.

Недоліком прототипу є недостатня стійкість хешування, оскільки для зламу необхідно лише

(19) UA (11) 37465 (13) U

знаходження ключа, яке зводиться до знаходження m_1 блоку даних.

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 операцій.

Поставлена задача вирішується за рахунок того, що в способі ключового хешування теоретично доведеної стійкості, 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 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 секретним числом a та секретним простим числом q, 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 q.

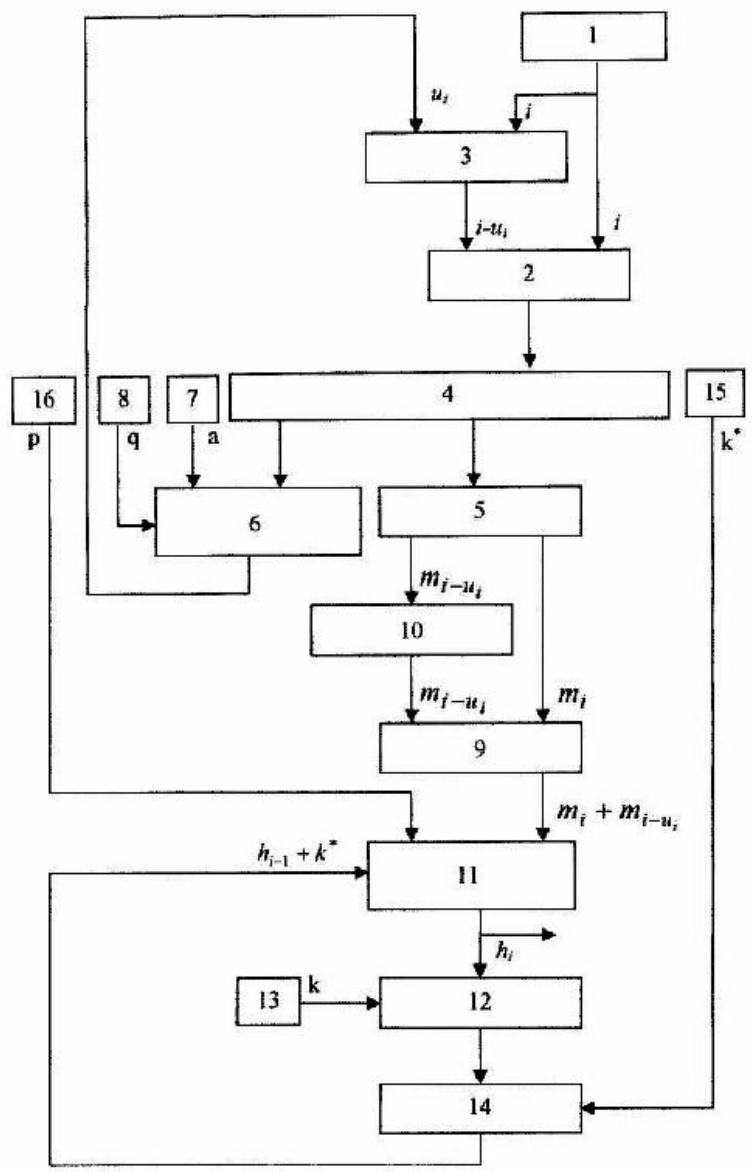
Технічний результат, який може буде отриманий при здійсненні корисної моделі, полягає в підвищенні складності задачі зламу ключа хешування без збільшення розрядності хеш-функції.

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 блока комутації 2 та першим входом першого блока 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 блока піднесення до степеня за модулем 6. Другий вхід першого блока піднесення до степеня за модулем 6 з'єднано з виходом регістра 7, третій вхід першого блока піднесення до степеня за модулем 6 є виходом регістра 8. Вихід першого блока піднесення до степеня за модулем 6 є другим входом першого блока додавання 3. Перший вихід другого блока комутації 5 є першим входом другого блока додавання 9, другий вихід другого блока комутації 5 з'єднано з входом блока затримки 10, вихід якого є другим входом другого блока додавання 9. Вихід другого блока додавання 9 з'єднано з першим входом другого блока піднесення до степеня за модулем 11, вихід якого є першим входом третього блока комутації 12 та виходом пристрою. Вихід регістра 13 є другим входом третього блока комутації 12, вихід якого з'єднано з першим входом третього блока додавання 14. Вихід регістра 15 з'єднано з другим входом третього блока додавання 14, вихід якого з'єднано з другим входом другого блока піднесення до степеня за модулем 11. Вихід регістра 16 є третім входом другого блока піднесення до степеня за модулем 11.

Спосіб ключового хешування теоретично доведеної стійкості виконується на пристрої таким чином.

В регістр 7 заносять значення параметра a, в регістр 8 заносять значення параметра q, 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 К та встановлюють в початкове положення лічильник 1 згідно початкової адреси оперативно запам'ятовуючого пристрою 4, в який заносять інформаційні дані М, які подають у вигляді послідовності $M=\{m_1, m_2, ..., m_t\}$. З лічильника 1 отримують адресу і-го інформаційного блоку даних, яку надсилають за допомогою першого блока комутації 2 до оперативно запам'ятовуючого пристрою 4, де на виході отримують значення і-то інформаційного блоку даних m_i, який надсилають до блока затримки через другий блок комутації 5 та до першого блока піднесення до степеня за модулем 6 та виконують піднесення інформаційного блоку даних m_i до степеня, значення якого надходить з регістра 7, за модулем, отриманим з регістра 8. Значення з виходу першого блока піднесення до степеня за модулем 6 надсилають на перший блок додавання 3, де розраховують зсув адреси блоку даних, що через перший блок комутації 2 надсилають в оперативно запам'ятовуючий пристрій 4. Значення з оперативно запам'ятовуючого пристрою 4 надсилають до другого блока додавання 9 через другий блок комутації 5, де його додають до значення з виходу блока затримки 10. Результат додавання з виходу другого блока додавання 9 надсилають до другого блока піднесення до степеня за модулем 11, де згідно вхідних значень з третього блока додавання 14 виконують піднесення до степеня за модулем, отриманим з регістра 16. Отриманий результат через третій блок комутації 12 надсилають до третього блока додавання 14, де до нього додають значення k* з виходу регістра 15. На першій ітерації на третій блок додавання 14 надходить значення к з виходу регістра 13 через третій блок комутації 12. На t-й ітерації на виході другого блока піднесення до степеня за модулем 11 формується вихідне значення результату хешування.



Фіг.

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