УКРАЇНА

(19) UA (11) 48410 (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 БЕЗКЛЮЧОВОГО ХЕШУВАННЯ

(21) u200911723
(22) 16.11.2009
(24) 10.03.2010
(46) 10.03.2010, Бюл.№ 5, 2010 р.
(72) ЛУЖЕЦЬКИЙ ВОЛОДИМИР АНДРІЙОВИЧ, БАРИШЕВ ЮРІЙ ВОЛОДИМИРОВИЧ, РУДИЙ ІВАН ВОЛОДИМИРОВИЧ
(73) ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
(57) Спосіб безключового хешування, який полягає в тому, що інформаційні дані M подають у вигляді послідовності $M=\{m_1, m_2 \ldots m_t\}$, хешування інформаційних даних виконують шляхом піднесення до степеня елементів m_i інформаційної послідовності M за модулем великого простого числа p за допомогою пристрою піднесення до степеня за модулем, який **відрізняється** тим, що степінь, до якого виконують піднесення за модулем, є результатом хешування попереднього елемента інформаційної послідовності h_{i-1}, а початкове заповнення h_0 є відкритим.

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 $M=(m_1,m_2,\ldots,m_t)$, ключові дані подають у вигляді послідовності блоків $X=(x_1,x_2,\ldots,x_t)$, 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: $MMH=\{g_k : Z_p^t \to Z_p \mid M \in Z_p^t\}$, де $g_x(m)$ - хеш-код; Z_p^t - кільце цілих чисел за модулем p; p - просте число.

Недоліками цього способу є неспроможність теоретичного доведення обчислювальної стійкості 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 M подають у вигляді послідовності $M=(m_1,m_2,\ldots,m_t)$, ключові дані K подають у вигляді великого секретного числа k та особистого ключа k^*, а хешування інформаційних даних виконують за допомогою пристрою множення, в подальшому пристрою піднесення до степеня за модулем, 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 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 використовують як степінь ступеня в ітераційному правилі хешування, а задача зламу ключа хешування зводиться до обчислення дискретного логарифма в простому полі.

Недоліком прототипу є надмірна ключова інформація та наявність додаткових операції, які виконують над нею, що не дозволяє ефективно впровадити безключове хешування при автентифікації даних.

В основу корисної моделі поставлена задача створити спосіб безключового хешування, який дозволить забезпечити підвищену швидкість хешування інформації за рахунок безключового об-

(19) UA (11) 48410 (13) U

числення хеш-значення за рахунок введення нових операцій.

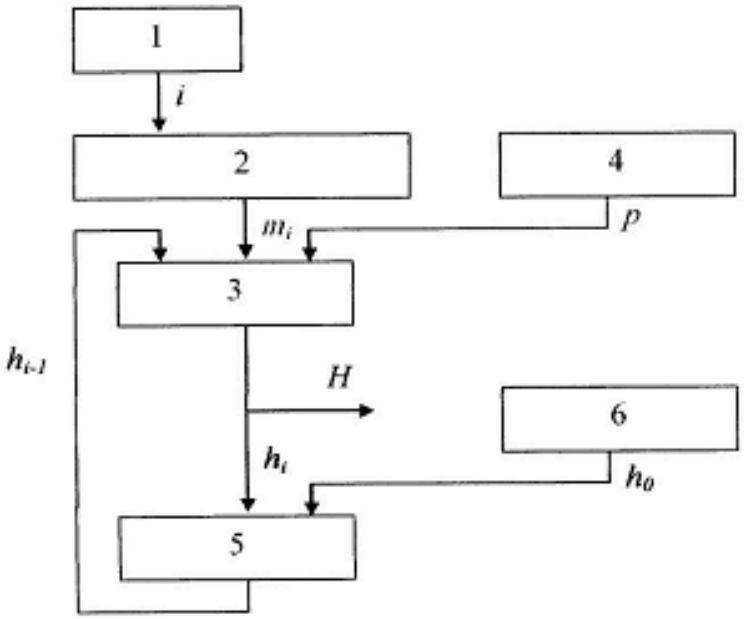
Поставлена задача вирішується за рахунок того, що в способі безключового хешування інформаційні дані M подають у вигляді послідовності $M = (m_1, m_2, \ldots, m_t)$, хешування інформаційних даних виконують шляхом піднесення до степеня елементів m_i інформаційної послідовності M за модулем великого простого числа p за допомогою пристрою піднесення до степеня за модулем, причому степінь, до якого виконують піднесення за модулем, є результатом хешування попереднього елементу інформаційної послідовності h_{i-1}, а початкове заповнення h_0 є відкритим.

На кресленні наведена схема пристрою, що реалізує спосіб безключового хешування.

Пристрій містить лічильник 1, вихід якого з'єднано з входом оперативно запам'ятовуючого пристрою 2, вихід якого з'єднано з першим входом блока піднесення до степеня за модулем 3. Другий вхід блока піднесення до степеня за модулем 3 з'єднано з виходом першого регістра 4, третій вхід блока піднесення до степеня за модулем 3 є виходом блока комутації 5. Вихід блока піднесення до степеня за модулем 3 є першим входом блока комутації 5 та виходом всього пристрою. Другий вхід блока комутації 5 з'єднано з виходом другого регістра 6.

Спосіб безключового хешування здійснюється таким чином.

В перший регістр 4 заносять значення параметра p, а в другий регістр 6 початкове хеш-значення h_0 та встановлюють в початкове положення лічильник 1 згідно початкової адреси оперативно запам'ятовуючого пристрою 2, в який заносять інформаційні дані M, які подають у вигляді послідовності $M = (m_1, m_2, \ldots, m_t)$. На вхід блока комутації 5 надсилають значення другого регістра 6. Починають ітеративний процес. З лічильника 1 отримують адресу і-го елемента інформаційної послідовності, яку надсилають до оперативно запам'ятовуючого пристрою 2, де на виході отримують значення і-го елемента інформаційної послідовності m_i, яке надсилають до блока піднесення до степеня за модулем 3 та виконують піднесення значення елемента інформаційної послідовності m_i до степеня, значення якого надходить з виходу блока комутації 5, за модулем, отриманим з першого регістра 4. Значення з виходу блока піднесення до степеня за модулем 3 надсилають на вхід блока комутації 5. На t-й ітерації на виході блока піднесення до степеня за модулем 3 отримують вихідне значення результату хешування H.



Комп'ютерна верстка Н. Лисенко 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