УКРАЇНА

(19) UA (11) 50818 (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 КЛЮЧОВОГО ХЕШУВАННЯ ТЕОРЕТИЧНО ДОВЕДЕНОЇ СТІЙКОСТІ

(21) u200913292
(22) 21.12.2009
(24) 25.06.2010
(46) 25.06.2010, Бюл.№ 12, 2010 р.
(72) ЛУЖЕЦЬКИЙ ВОЛОДИМИР АНДРІЙОВИЧ, БАРИШЕВ ЮРІЙ ВОЛОДИМИРОВИЧ, СЕМЕНЕНКО ДАР'Я СЕРГІЇВНА
(73) ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
(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, а хешування інформаційних даних виконують шляхом піднесення до степеня за модулем великого простого числа p за допомогою пристрою піднесення до степеня за модулем, велике секретне число к використовують як початкове заповнення h_0, задача зламу ключа хешування зводиться до обчислення дискретного логарифма в простому полі, який **відрізняється** тим, що підносять велике число g, яке є примітивним коренем за модулем p, степінь, до якого виконують піднесення, є результатом додавання значення елемента інформаційної послідовності m_i та результату хешування попереднього елемента інформаційної послідовності.

1

2

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:

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

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 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. G 09 C 1/00, 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, в подальшому пристрою піднесення до степеня за модулем, 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, ключові дані використовують як степінь ступеня в ітераційному правилі хешування, в подальшому як початкове заповнення h_0, а задача зламу ключа хешування зводиться до обчислення дискретного логарифма в простому полі.

Недоліком прототипу є недостатня теоретична стійкість внаслідок того, що для заданого p не всі m_i дозволяють отримати повну множину вихідних значень (від 0 до p-1), оскільки не всі вони є примітивними коренями за модулем p, що робить можливим для зловмисника злам хеш-значення за допомогою перебору відмінного від повного, а тому задача зламу не зводиться до обчислення дискретного логарифма в простому полі.

(19) UA (11) 50818 (13) U

В основу корисної моделі поставлена задача створити спосіб ключового хешування теоретично доведеної стійкості, який дозволить забезпечити підвищену обчислювальну стійкість хешування інформації за рахунок зведення задачі зламу до обчислення дискретного логарифма в простому полі шляхом введення додаткових операцій.

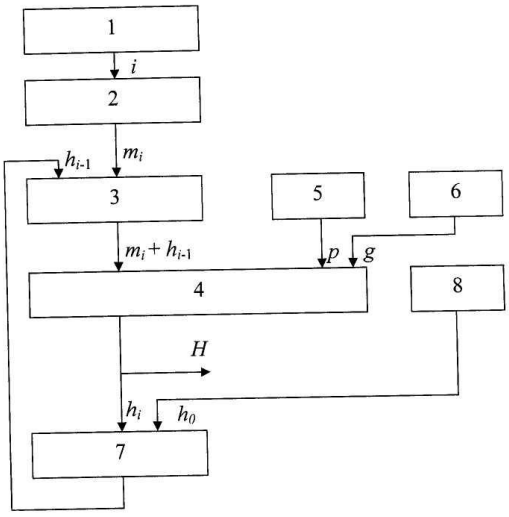
Поставлена задача вирішується за рахунок того, що в способі ключового хешування теоретично доведеної стійкості інформаційні дані M подають у вигляді послідовності $M= \{m_1, m_2,..., m_t\}$, ключові дані K подають у вигляді великого секретного ключа k, а хешування інформаційних даних виконують шляхом піднесення до степеня за модулем великого простого числа p за допомогою пристрою піднесення до степеня за модулем, великий секретний ключ к використовують як початкове заповнення h_0, задача зламу ключа хешування зводиться до обчислення дискретного логарифма в простому полі, причому підносять велике число g, яке є примітивним коренем за модулем p, степінь, до якого виконують піднесення, є результатом додавання значення елемента інформаційної послідовності τ_i та результату хешування попереднього елемента інформаційної послідовності.

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

Пристрій містить лічильник 1, вихід якого з'єднано з входом оперативно запам'ятовуючого пристрою 2, вихід якого з'єднано з першим входом блока додавання 3. Другий вхід блока додавання 3 є виходом блока комутації 7. Вихід блока додавання 3 є входом блока піднесення до степеня за модулем 4. Другий вхід блока піднесення до степеня за модулем 4 з'єднано з виходом першого регістра 5, третій вхід блока піднесення до степеня за модулем 4 з'єднано з виходом другого регістра 6. Вихід блока піднесення до степеня за модулем 4 є першим входом блока комутації 7. Другий вхід блока комутації 7 з'єднано з виходом третього регістра 8.

Спосіб ключового хешування теоретично доведеної стійкості здійснюється таким чином.

В перший регістр 5 заносять значення параметра p, в другий регістр 6 значення параметра g, а в третій регістр 8 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 $M= \{m_1, m_2,..., m_t\}$. На вихід блока комутації 7 надсилають вихідне значення третього регістра 8. Починають ітеративний процес. З лічильника 1 отримують адресу i-го елемента інформаційної послідовності, яку надсилають до оперативно запам'ятовуючого пристрою 2, де на виході отримують значення i-го елемента інформаційної послідовності m_i, яке надсилають до блока додавання 3. За допомогою блока додавання 3 отримують суму значення елемента інформаційної послідовності m_i та (i-1)-го значення хеш-функції h_{i-1}, яке надходить з виходу блока комутації 7. В блоці піднесення до степеня за модулем 4 виконують піднесення значення виходу другого регістру 6 до степеня, який отримують з виходу блока додавання 3, за модулем, який отримують з виходу першого регістра 5. Значення з виходу блока піднесення до степеня за модулем 4 надсилають на вхід блока комутації 7. Починають наступну ітерацію. На t-ій ітерації на виході блока піднесення до степеня за модулем 4 отримують вихідне значення результату хешування.



Комп'ютерна верстка А. Крижанівський 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