УКРАЇНА

(19) UA (11) 53508 (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

(21) u201003900
(22) 06.04.2010
(24) 11.10.2010
(46) 11.10.2010, Бюл.№ 19, 2010 р.
(72) ЛУЖЕЦЬКИЙ ВОЛОДИМИР АНДРІЙОВИЧ, БАРИШЕВ ЮРІЙ ВОЛОДИМИРОВИЧ, СТАХ ОЛЕКСІЙ СЕРГІЙОВИЧ
(73) ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
(57) Спосіб ключового хешування, який полягає в тому, що 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*, секретних чисел a та b, хешування інформаційних даних виконують за допомогою блока піднесення до степеня за модулем елементів m_i, інформаційної послідовності M та елементів ключової послідовності K, підносять суму значень елементів інформаційної послідовності m_i, частину $(m_{i-a}+m_{i-b})$ якої визначають як результат додавання значень елементів інформаційної послідовності, адреси яких обчислюють як результат додавання секретного числа a та значення лічильника і за допомогою другого блока додавання, додавання секретного числа b та значення лічильника і за допомогою третього блока додавання, за модулем великого простого числа p, степінь, до якого здійснюють піднесення, отримують шляхом додавання особистого ключа k* та результату попередньої ітерації хешування за допомогою шостого блока додавання, який **відрізняється** тим, що до значення частини $(m_{i-a}+m_{i-b})$ суми значень елементів інформаційної послідовності m_i додають значення елемента інформаційної послідовності, адресу якого обчислюють як результат додавання числа u_i, яке обчислюють як стан генератора псевдовипадкових чисел, якому передує стан, що дорівнює значенню елемента інформаційної послідовності m_i, та значення лічильника і за допомогою першого блока додавання.

1

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

Відомий 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 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, ключові дані використовують як степінь ступеня в ітераційному правилі хешування, а задача зламу ключа хешування зводиться до обчислення дискретного логарифма в простому полі.

Недоліком цього способу є недостатня стійкість хешування, оскільки для зламу необхідно лише знаходження ключа, яке зводиться до знаходження m_1 елемента інформаційної послідовності.

Найбільш близьким до способу, що пропонується є спосіб ключового хешування [Патент України №36582 від 27.10.2008 р., МПК. G 09 C 1/00, бюл. №20 2008 р.], який полягає в тому, що 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, в подальшому блока 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, в

(19) UA (11) 53508 (13) U

подальшому елемента інформаційної послідовності, 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, в подальшому блока додавання, при чому 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 елементів інформаційної послідовності, адреси яких паралельно обчислюють як результат додавання секретного числа a і значення лічильника i за допомогою першого блока додавання та додавання секретного числа b і значення лічильника i за допомогою другого блока додавання.

Недоліком прототипу є недостатня стійкість хешування, внаслідок того, що задача зламу за допомогою мультиколізій зводиться до розв'язання системи рівнянь, оскільки параметри a і b не змінюються під час хешування.

В основу корисної моделі поставлена задача створити спосіб ключового хешування, який дозволить забезпечити підвищену обчислювальну стійкість хешування інформації за рахунок того, що вводять змінний параметр, що утруднює задачу зламу за допомогою мультиколізій.

Поставлена задача вирішується за рахунок того, що в способі ключового хешування 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*, секретних чисел a та b, хешування інформаційних даних виконують за допомогою блока піднесення до степеня за модулем елементів m_i інформаційної послідовності M та елементів ключової послідовності K, підносять суму значень елементів інформаційної послідовності m_i, частину $(m_{i-a}+m_{i-b})$ якої визначають як результат додавання значень елементів інформаційної послідовності, адреси яких обчислюють як результат додавання секретного числа a та значення лічильника i за допомогою другого блока додавання, додавання секретного числа b та значення лічильника i за допомогою третього блока додавання, за модулем великого простого числа p, степінь, до якого здійснюють піднесення, отримують шляхом додавання особистого ключа k* та результату попередньої ітерації хешування за допомогою шостого блока додавання, причому до значення частини $(m_{i-a}+m_{i-b})$ суми значень елементів інформаційної послідовності m_i додають значення елемента інформаційної послідовності, адресу якого обчислюють як результат додавання числа u_i, яке обчислюють як стан генератора псевдовипадкових чисел, якому передує стан, що дорівнює значенню елемента інформаційної послідовності m_i, та значення лічильника i за допомогою першого блока додавання.

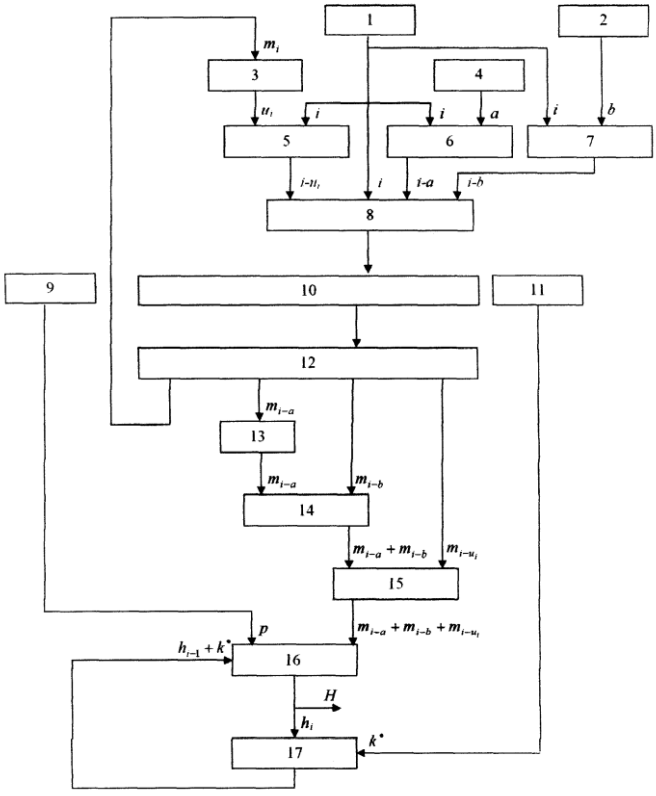
На кресленні наведена схема пристрою, що реалізує спосіб ключового хешування теоретично доведеної стійкості.

Пристрій містить лічильник 1, вихід якого з'єднано з першим входом першого блока додавання 5, першим входом другого блока додавання 6, першим входом третього блока додавання 7 та першим входом першого блока комутації 8. Вихід першого блока додавання 5 з'єднаний з другим входом першого блока комутації 8. Вихід регістра зберігання параметра a 4 є другим входом другого блока додавання 6, вихід якого з'єднано з третім входом першого блока комутації 8. Вихід регістра зберігання параметра b 2 є другим входом третього блока додавання 7, вихід якого з'єднано з четвертим входом першого блока комутації 8. Вихід першого блока комутації 8 є входом оперативно запам'ятовуючого пристрою 10, вихід якого є входом другого блока комутації 12. Перший вихід другого блока комутації 12 з'єднано з входом блока генерації псевдовипадкових чисел 3, вихід якого є другим входом першого блока додавання 5. Другий вихід другого блока комутації 12 є входом блока затримки 13, третій вихід другого блока комутації 12 є входом четвертого блока додавання 14, другим входом якого є вихід з блока затримки 13. Четвертий вихід другого блока комутації 12 є першим входом п'ятого блока додавання 15, другим входом якого є вихід четвертого блока додавання 14. Вихід п'ятого блока додавання 15 є першим входом блока піднесення до степеня за модулем 16. Другим входом блока піднесення до степеня за модулем 16 є вихід регістра зберігання параметра p 9. Вихід блока піднесення до степеня за модулем 16 є першим входом шостого блока додавання 17 та виходом всього пристрою. Другим входом шостого блока додавання 17 є вихід регістра зберігання параметра k* 11. Вихід шостого блока додавання 17 є третім входом блока піднесення до степеня за модулем 16.

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

В регістр зберігання параметра a 4 заносять значення параметра a, в регістр зберігання параметра b 2 заносять значення параметра b, в регістр зберігання параметра k* 11 заносять значення параметра k*, в регістр зберігання параметра p 9 заносять значення параметра p, встановлюють в початкове положення лічильник 1 згідно початкової адреси оперативно запам'ятовуючого пристрою 10, в який заносять інформаційні дані M, що подають у вигляді послідовності $M=\{m_1, m_2,..., m_t\}$, вихідне значення шостого блока додавання 17 встановлюють рівним великому секретному числу k. Починають ітеративний процес. З лічильника 1 отримують адресу r-го елемента інформаційної послідовності m_i, яку надсилають на вхід першого блока додавання 5, на вхід другого блока додавання 6, на вхід третього блока додавання 7 та на вхід першого блока комутації 8, з якого її надсилають до оперативно запам'ятовуючого пристрою 10. Значення елемента інформаційної послідовності m_i, яке отримують з виходу оперативно запам'ятовуючого пристрою 10, надсилають до другого блока комутації 12, з першого виходу якого дані надсилають до блока генерації псевдовипадкових чисел 3, на виході якого отримують псевдовипадкове число u_i, використовуючи значення елемента інформаційної послідовності m_i як по-

чаткове заповнення, що надсилають на вхід першого блока додавання 5. Одночасно на вхід другого блока додавання 6 надсилають значення виходу регістра зберігання параметра a 4 та обчислюють значення адреси (i-o)-го елемента інформаційної послідовності m_{i-a}, яку надсилають до оперативно запам'ятовуючого пристрою 10 через перший блок комутації 8. Значення (i-a)-го елемента інформаційної послідовності m_{i-a}, що отримують з виходу оперативно запам'ятовуючого пристрою 10 надсилають до другого блока комутації 12. З другого виходу другого блока комутації 12 дані надсилають до блока затримки 13, звідки дані поступають до четвертого блока додавання 14. На вхід третього блока додавання 7 надсилають значення виходу регістра зберігання параметра b 1 та обчислюють значення адреси (i-b)-го елемента інформаційної послідовності m_{i-b}, яку надсилають до оперативно запам'ятовуючого пристрою 10 через перший блок комутації 8. Значення елемента інформаційної послідовності m_{i-b}, що отримують з виходу оперативно запам'ятовуючого пристрою 10 надсилають до четвертого блока додавання 14 через другий блок комутації 12. На вхід першого блока додавання 5 надсилають значення виходу блока генерації псевдовипадкових чисел 3 та обчислюють значення адреси $(i-u_i)$-го елемента інформаційної послідовності m_{i-ui}, яку надсилають до оперативно запам'ятовуючого пристрою 10 через перший блок комутації 8. Значення елемента інформаційної послідовності m_{i-ui}, що отримують з виходу оперативно запам'ятовуючого пристрою 10 надсилають до п'ятого блока додавання 15 через другий блок комутації 12, де його додають зі значенням суми (i-a)-го та (i-b)-го елементів інформаційної послідовності $m_{i-a}+m_{i-b}$, що отримують з виходу четвертого блока додавання 14. Значення суми $(m_{i-ui}+m_{i-a}+m_{i-b})$, що отримують на виході п'ятого блока додавання 15, надсилають до блока піднесення до степеня за модулем 16, де його підносять до степеня значення, якого отримують з виходу шостого блока додавання 17, за модулем, значення якого отримують з регістру зберігання параметра p 9. Результат, що отримують на виході блока піднесення до степеня за модулем 16 надсилають на вихід всього пристрою та на вхід шостого блока додавання 17, на виході якого отримують результат його додавання зі значенням особистого ключа k*, що надходить з виходу блока зберігання параметра k* 11. Починають наступну ітерацію. Результат хешування отримують з блока піднесення до степеня за модулем 16 після завершення t-ї ітерації.



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