УКРАЇНА

(19) UA (11) 54814 (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) u201006158
(22) 21.05.2010
(24) 25.11.2010
(46) 25.11.2010, Бюл.№ 22, 2010 р.
(72) ЛУЖЕЦЬКИЙ ВОЛОДИМИР АНДРІЙОВИЧ, БАРИШЕВ ЮРІЙ ВОЛОДИМИРОВИЧ
(73) ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
(57) Спосіб безключового хешування, який полягає в тому, що інформаційні дані M подають у вигляді послідовності $M=\{m_1, m_2,..., m_\ell\}$, хешування інформаційних даних виконують шляхом піднесення до степеня елементів $\boldsymbol{m}_\ell$ інформаційної послідовності M за модулем великого простого числа $\boldsymbol{p}$ за допомогою блока піднесення до степеня за модулем, степінь, до якого виконують піднесення за модулем, є результатом хешування попереднього елемента інформаційної послідовності $\boldsymbol{h_{i-1}}$, початкове заповнення $\boldsymbol{h_0}$ є відкритим, який **відрізняється** тим, що підносять до степеня за модулем великого простого числа $\boldsymbol{p}$ результат додавання значень елементів інформаційної послідовності, адреси яких паралельно обчислюють як результат додавання константи $\boldsymbol{a}$ і значення лічильника $\boldsymbol{i}$ за допомогою першого блока додавання за модулем та додавання константи $\boldsymbol{b}$ і значення лічильника $\boldsymbol{i}$ за допомогою другого блока додавання за модулем.

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 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 $M=\{m_1,m_2,..., m_\ell\}$, 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 надмірна ключова інформація та наявність додаткових операції, які виконують над нею, що не дозволяє ефективно впровадити безключове хешування при автентифікації даних.

Найбільш близьким до способу, що пропонується є спосіб безключового хешування (Патент України №48410 від 10.03.2010 р., М. кл. G 09 C 1/00, бюл. №5 2010 р.), який полягає в тому, що інформаційні дані M подають у вигляді послідовності $M= \{m_1, m_2,..., m_\ell\}$, хешування інформаційних даних виконують шляхом піднесення до степеня значення елементів m_i інформаційної послідовності M за модулем великого простого числа p за допомогою пристрою піднесення до степеня за модулем, в подальшому блока піднесення до степеня за модулем, степінь, до якого виконують піднесення за модулем, є результатом хешування попереднього елементу інформаційної послідовності h_{i-1}, а початкове заповнення h_0 є відкритим.

Недоліками прототипу є недостатня стійкість хешування, оскільки кожен елемент інформаційної послідовності m_i приймає участь в ітеративному перетворенні лише один раз, відповідно даний блок безпосередньо впливає лише на один проміжний результат хешування, що полегшує пошук колізій для зловмисника.

(19) UA (11) 54814 (13) U

В основу корисної моделі поставлена задача створення способу безключового хешування, який за рахунок введення нових операцій дозволить забезпечити підвищену стійкість хешування інформації за рахунок безпосереднього впливу кожного елемента інформаційної послідовності на два проміжні результати хешування.

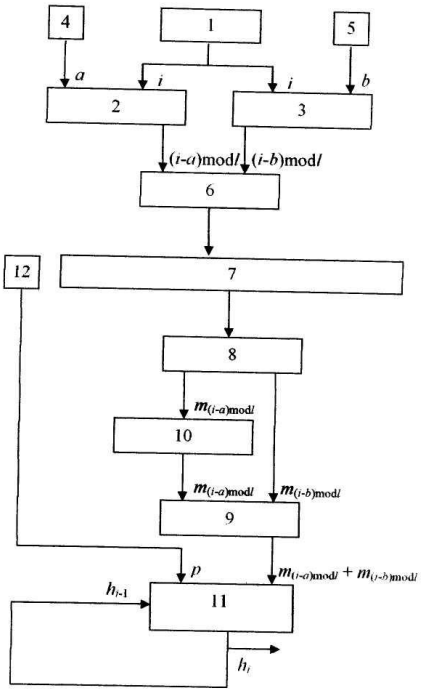
Поставлена задача вирішується за рахунок того, що в способі безключового хешування інформаційні дані M подають у вигляді послідовності M = $\{m_1, m_2, ..., m_\ell\}$, хешування інформаційних даних виконують шляхом піднесення до степеня елементів інформаційної послідовності M за модулем великого простого числа p за допомогою блока піднесення до степеня за модулем, степінь, до якого виконують піднесення за модулем, є результатом хешування попереднього елемента інформаційної послідовності h_{i-1}, початкове заповнення h_0 є відкритим, причому підносять до степеня за модулем великого простого числа p результат додавання значень елементів інформаційної послідовності, адреси яких паралельно обчислюють як результат додавання константи a і значення лічильника і за допомогою першого блока додавання за модулем та додавання константи b і значення лічильника і за допомогою другого блока додавання за модулем.

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

Пристрій містить лічильник 1, вихід якого з'єднано з першим входом першого блока додавання за модулем 2 та першим входом другого блока додавання за модулем 3, вихід регістра зберігання константи a 4 з'єднано з другим входом першого блока додавання за модулем 2, вихід регістра зберігання константи b 5 з'єднано з другим входом другого блока додавання за модулем 3, вихід першого блока додавання за модулем 2 з'єднано з першим входом першого блока комутації 6, а вихід другого блока додавання за модулем 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 блока додавання за модулем 9, другий вихід другого блока комутації 8 з'єднано з входом блока затримки 10, вихід якого є другим входом третього блока додавання за модулем 9. Вихід третього блока додавання за модулем 9 з'єднано з першим входом блока піднесення до степеня за модулем 11, вихід якого є його другим входом та виходом всього пристрою. Вихід регістра зберігання модуля p 12 є третім входом блока піднесення до степеня за модулем.

Спосіб безключового хешування здійснюється таким чином.

В регістр зберігання константи a 4 заносять значення константи a, в регістр зберігання константи b 5 заносять значення константи Ь, в регістр зберігання модуля p 12 заносять значення модуля p, встановлюють у початкове положення лічильник 1 згідно початкової адреси оперативно запам'ятовуючого пристрою 7, в який заносять інформаційні дані M, які подають у вигляді послідовності M=$\{m_1, m_2, ..., m_\ell\}$, вихід блока піднесення до степеня за модулем встановлюють рівним значенню початкового заповнення h_0. Починають ітеративний процес. З лічильника 1 отримують адресу i-го елемента інформаційної послідовності в оперативно запам'ятовуючому пристрої 7, яку надсилають до першого блока додавання за модулем 2 та другого блока додавання за модулем 3, на виході першого блока додавання за модулем 2 отримують адресу $(i-a) \bmod \ell$-го елемента інформаційної послідовності, яку надсилають за допомогою першого блока комутації 6 до оперативно запам'ятовуючого пристрою 7, одночасно значення отриманої адреси $(i-b) \bmod \ell$-го елемента інформаційної послідовності з виходу другого блока додавання за модулем 3 надсилають на вхід першого блока комутації 6. На виході оперативно запам'ятовуючого пристрою 7, отримують значення $(i-a) \bmod \ell$-го елемента інформаційної послідовності $m_{(i-a) \bmod \ell}$ який надсилають до блока затримки 10 за допомогою другого блока комутації 8, одночасно на вхід оперативно запам'ятовуючого пристрою надсилають адресу $(i-b) \bmod \ell$-го елемента інформаційної послідовності з виходу першого блока комутації 6. Значення $(i-b) \bmod \ell$-го елемента інформаційної послідовності $m_{(i-b) \bmod \ell}$ з виходу оперативно запам'ятовуючого пристрою 7, надсилають до третього блока додавання за модулем 9 за допомогою другого блока комутації 8, де його додають до значення з виходу блока затримки 10. Результат додавання $(m_{(i-a) \bmod \ell} + m_{(i-b) \bmod \ell})$ з виходу третього блока додавання за модулем 9 надсилають на вхід блока піднесення до степеня за модулем 11, де згідно вхідних значень з регістра зберігання модуля/» 12 та виходу блока піднесення до степеня 11 виконують піднесення результату додавання $(m_{(i-a) \bmod \ell} + m_{(i-b) \bmod \ell})$ до степеня h_{i-1} за модулем p. Результат, отриманий у блоці піднесення до степеня за модулем 11, надсилають на вхід його вхід та на вихід всього пристрою. На ℓ-ій ітерації на виході блока піднесення до степеня за модулем 11 отримують вихідне значення результату хешування h_ℓ.



Комп'ютерна верстка І.Скворцова 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