УКРАЇНА

(19) UA (11) 50841 (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) u200913535
(22) 25.12.2009
(24) 25.06.2010
(46) 25.06.2010, Бюл.№ 12, 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 М подають у вигляді послідовності $M=\{m_1, m_2,...,m_t\}$, хешування інформаційних даних виконують шляхом піднесення до степеня елементів m_i інформаційної послідовності М за модулем великого простого числа р за допомогою пристрою піднесення до степеня за модулем, піднесення до степеня за модулем здійснюють для результату додавання значення елемента інформаційної послідовності m_i та значення елемента інформаційної послідовності, номер якого відрізняється від і на число, яке обчислюють за допомогою пристрою піднесення до степеня за модулем як результат піднесення до степеня а значення елемента інформаційної послідовності m_i за модулем q, 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.

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. G09C1/00, 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 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 пристрого додавання, ключові дані використовують як степінь ступеня в ітераційному правилі хешування, а задача зламу ключа хешування зводиться до обчислення дискретного логарифма в простому полі.

Найбільш близьким до способу, що пропонується є спосіб ключового хешування теоретично доведеної стійкості (Патент України №37465 від 25.11.2008 р., М. кл. G09C1/00, бюл. №22 2008 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, в подальшому пристрою піднесення до степеня за модулем, елементів m_i інформаційної послідовності М та елементів ключової послідовності К за ітеративним правилом піднесення до степеня значення блока даних, в подальшому елемента інформаційної послідовності, 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 доповнюють секретним числом а та секретним простим числом q, а ітеративне правило піднесення до степеня за модулем здійснюють для результату додавання значення елемента інформаційної послідовності m_i та значення елемента інформаційної послідовності, номер якого відрізняється від і на число, яке обчислюють за допомогою пристрою піднесення до степеня за модулем як результат піднесення до степеня а значення елемента інформаційної послідовності m_i, за модулем q.

Недоліками аналогу та прототипу є надмірна ключова інформація та наявність додаткових операції, які виконують над нею, що не дозволяє ефе-

(19) UA (11) 50841 (13) U

ктивно впровадити безключове хешування при автентифікації даних.

В основу корисної моделі поставлена задача створення способу безключового хешування, який за рахунок введення нових операцій дозволить забезпечити підвищену швидкість хешування інформації за рахунок безключового обчислення хеш-значення.

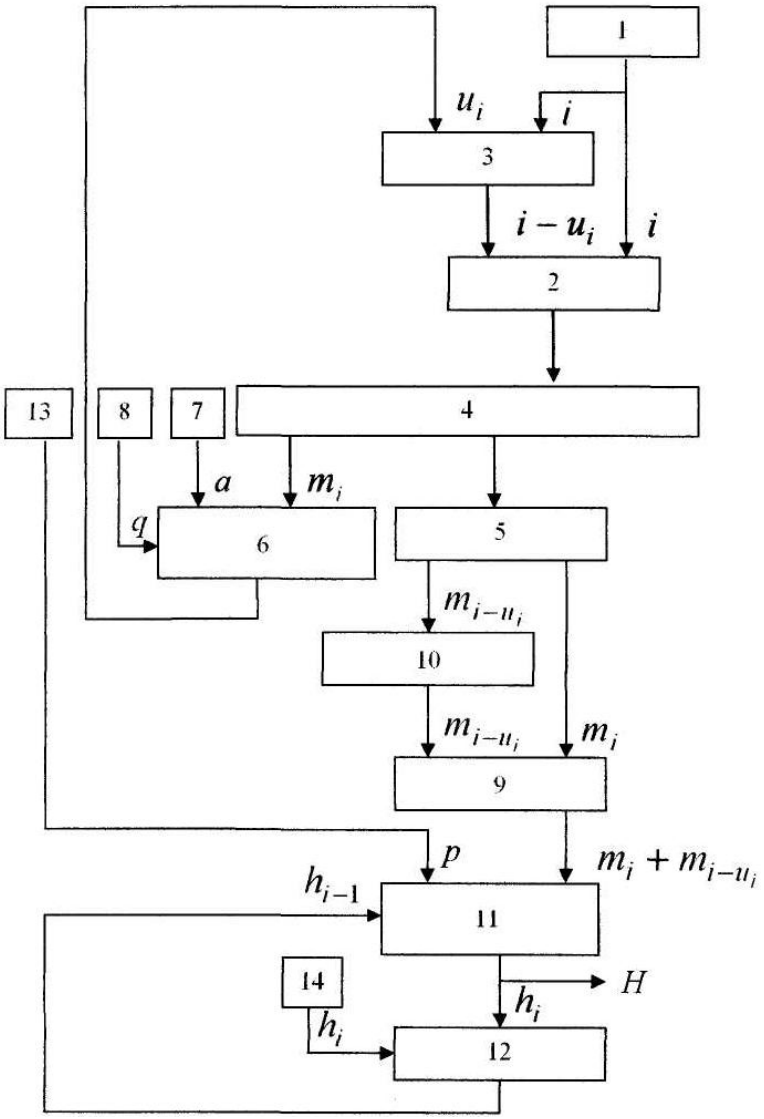
Поставлена задача вирішується за рахунок того, що в способі безключового хешування інформаційні дані M подають у вигляді послідовності $M=\{m_1, m_2,..., m_t\}$, хешування інформаційних даних виконують шляхом піднесення до степеня елементів m_i інформаційної послідовності M за модулем великого простого числа p за допомогою пристрою піднесення до степеня за модулем, піднесення до степеня за модулем здійснюють для результату додавання значення елемента інформаційної послідовності m_i та значення елемента інформаційної послідовності, номер якого відрізняється від і на число, яке обчислюють за допомогою пристрою піднесення до степеня за модулем як результат піднесення до степеня a значення елемента інформаційної послідовності m_i, за модулем q, причому степінь, до якого виконують піднесення за модулем, є результатом хешування попереднього елемента 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 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 першого регістра 7, третій вхід першого блока піднесення до степеня за модулем 6 є виходом другого 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. Вихід четвертого регістра 14 є другим входом третього блока комутації 12. Вихід третього блока комутації 12 є другим входом другого блока піднесення до степеня за модулем 11. Вихід третього регістра 13 є третім входом другого блока піднесення до степеня за модулем 11.

Спосіб безключового хешування виконується на пристрої таким чином.

В перший регістр 7 заносять значення параметра a, в другий регістр 8 заносять значення параметра q, в третій регістр 13 заносять значення параметра p, в четвертий регістр 14 заносять значення параметра h_0 та надсилають його на вхід третього блока комутації 12. Встановлюють в початкове положення лічильник 1 згідно початкової адреси оперативно запам'ятовуючого пристрою 4, в який заносять інформаційні дані M, які подають у вигляді послідовності $M=\{m_1, m_2,...,m_t\}$. Починають ітеративний процес. З лічильника 1 отримують адресу i-то елемента інформаційної послідовності, яку надсилають через перший блок комутації 2 до оперативно запам'ятовуючого пристрою 4, де на виході отримують значення i-го елемента інформаційної послідовності 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 елемента інформаційної послідовності m_i до степеня, значення якого надходить з першого регістра 7, за модулем, отриманим з другого регістра 8. Значення з виходу першого блока піднесення до степеня за модулем 6 надсилають на перший блок додавання 3, де розраховують зсув адреси елемента інформаційної послідовності, 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 виконують піднесення до степеня, що надходить з виходу третього блока комутації 12, за модулем, отриманим з третього регістра 13. Отримане значення надсилають на вхід третього блока комутації 12. Починають наступну ітерацію. На t-й ітерації на виході другого блока піднесення до степеня за модулем 11 формується вихідне значення результату хешування H.



Комп'ютерна верстка В. Мацело 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