



УКРАЇНА

(19) UA (11) 42220 (13) U
(51) МПК (2009)
G09C 1/00МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІОПИС
ДО ПАТЕНТУ
НА КОРИСНУ МОДЕЛЬвидається під
відповідальність
власника
патенту

(54) СПОСІБ ПАРАЛЕЛЬНОГО КЛЮЧОВОГО ХЕШУВАННЯ ТЕОРЕТИЧНО ДОВЕДЕНОЇ СТІЙКОСТІ

1

(21) u200900908

(22) 06.02.2009

(24) 25.06.2009

(46) 25.06.2009, Бюл.№ 12, 2009 р.

(72) ЛУЖЕЦЬКИЙ ВОЛОДИМИР АНДРІЙОВИЧ,
БАРИШЕВ ЮРІЙ ВОЛОДИМИРОВИЧ, ДМИТРИ-
ШИН ОЛЕКСАНДР ВАСИЛЬОВИЧ(73) ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ
УНІВЕРСИТЕТ(57) Спосіб паралельного ключового хешування теоретично доведеної стійкості, який полягає в тому, що інформаційні дані M подають у вигляді послідовності $M = \{m_1, m_2, \dots, m_t\}$, а хешування інформаційних даних виконують за допомогою пристрою піднесення до степеня за модулем інформаційних даних M за ітеративним правилом піднесення до степеня за модулем великого простого числа, яке здійснюють для результату додавання за допомогою третього пристрою додавання значень блоків даних, адреси яких паралельно

2

обчислюють як результат додавання секретного числа a і значення лічильника i ($i=1,2,\dots,t$) за допомогою першого пристрою додавання та додавання секретного числа b і значення лічильника i за допомогою другого пристрою додавання, ключові дані доповнюють секретними числами a та b , який відрізняється тим, що ключові дані K представляють у вигляді послідовності $K = \{k_1, k_2, \dots, k_w, a, b\}$, а суму елементів інформаційної послідовності $m_{i-a} + m_{i-b}$ розбивають на w частин, кожен u -ту ($u=1,2,\dots,w$) частину підносять до степеня, який отримують шляхом додавання за допомогою $(u+3)$ -го пристрою додавання елемента ключової послідовності k_u та суми результатів піднесення до степеня, отриманих на попередньому кроці, за модулем простого числа p_u , піднесення до степеня за модулем кожної u -тої частини суми елементів інформаційної послідовності $m_{i-a} + m_{i-b}$ виконують паралельно.

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, м. кл. G09C 1/00, бюл. №11 2006 р.], який полягає в тому, що інформаційні дані M подають у вигляді послідовності $M = \{m_1, m_2, \dots, m_t\}$, ключові дані K подають у вигляді великого секретного числа k та особистого ключа k' , а хешування інформаційних даних M виконують за допомогою пристрою множення елементів m_i ($i = 1, 2, \dots, t$)

інформаційної послідовності M та елементів ключової послідовності K за ітеративним правилом піднесення до степеня значення блока даних, в 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, ключові дані використовують як степінь ступеня в ітераційному правилі хешу-

вання, а задача зламу ключа хешування зводиться до обчислення дискретного логарифма в полі простого числа.

Недоліком аналогу є недостатня стійкість хешування, оскільки для зламу способу хешування даних необхідне лише знаходження значення ключа, яке зводиться до знаходження значення першого елемента інформаційної послідовності m_1 .

Найбільш близьким до способу, що пропонується є спосіб ключового хешування теоретично доведеної стійкості [Патент України №36582, м. кл. G09C 1/00, бюл. №20 2008 р.], який полягає в тому, що інформаційні дані M подають у вигляді послідовності $M = \{m_1, m_2, \dots, m_t\}$, ключові дані K подають у вигляді великого секретного числа k та особистого ключа k' , а хешування інформаційних даних виконують за допомогою пристрою піднесення до степеня за модулем елементів m_i ($i = 1, 2, \dots, t$) інформаційної послідовності M та елементів ключової послідовності K за ітеративним правилом піднесення до степеня значення елемента інформаційної послідовності за модулем великого

(13) U

(11) 42220

(19) UA

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 доповнюють секретними числами a та b , а ітеративне правило піднесення до степеня за модулем великого простого числа p здійснюють для результату додавання значень блоків даних, надалі елементів інформаційної послідовності, адреси яких паралельно обчислюють як результат додавання секретного числа a і значення лічильника K за допомогою першого пристрою додавання та додавання секретного числа b і значення лічильника i за допомогою другого пристрою додавання.

Недоліком найближчого аналога є недостатня швидкість хешування, в зв'язку з тим, що для обробки i -го елемента інформаційної послідовності необхідно попередньо обчислити хеш-значення для всіх попередніх $i-1$ елементів інформаційної послідовності, а отже необхідно t ітерацій піднесення до степеня для обробки всіх елементів інформаційної послідовності m_i .

В основу корисної моделі поставлена задача створити спосіб паралельного ключового хешування теоретично доведеної стійкості, який дозволить забезпечити підвищену швидкість обчислення за рахунок паралельної обробки елементів інформаційної послідовності.

Поставлена задача вирішується за рахунок того, що інформаційні дані M подають у вигляді послідовності $M = \{m_1, m_2, \dots, m_t\}$, а хешування інформаційних даних виконують за допомогою пристрою піднесення до степеня за модулем інформаційних даних M за ітеративним правилом піднесення до степеня за модулем великого простого числа, яке здійснюють для результату додавання за допомогою третього пристрою додавання значень блоків даних, адреси яких паралельно обчислюють як результат додавання секретного числа a і значення лічильника i за допомогою другого пристрою додавання, ключові дані доповнюють секретними числами a та A , причому ключові дані K представляють у вигляді послідовності $K = \{k_1, k_2, \dots, k_w, a, b\}$, а суми елементів інформаційної послідовності $m_{i-a} + m_{i-b}$ розбивають на w частин, кожну u -ту ($u = 1, 2, \dots, w$) частину підносять до степеня, який отримують шляхом додавання за допомогою $(u + 3)$ -го пристрою додавання елемента ключової послідовності k_u та суми результатів піднесення до степеня, отриманих на попередньому кроці, за модулем простого числа p_u , піднесення до степеня за модулем кожної u -тої частини суми елементів інформаційної послідовності $m_{i-a} + m_{i-b}$ виконують паралельно.

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

Пристрій містить лічильник 1, вихід якого з'єднано з першим входом першого пристрою додавання 2 та першим входом другого пристрою додавання 3, вихід регістра зберігання секретного числа a 4 з'єднано з другим входом першого пристрою додавання 2, вихід регістра зберігання сек-

ретного числа b 5 з'єднано з другим входом другого пристрою додавання 3, вихід першого пристрою додавання 2 з'єднано з першим входом першого блока комутації 6, а вихід другого пристрою додавання 3 з'єднано з другим входом першого блока комутації 6. Вихід першого блока комутації 6 є входом оперативного запам'ятовуючого пристрою 7, вихід якого є входом другого блока комутації 8. Перший вихід другого блока комутації 8 є першим входом третього пристрою додавання 9, другий вихід другого блока комутації 8 з'єднано з входом блока затримки 10, вихід якого є другим входом третього пристрою додавання 9, u -ий вихід якого з'єднано з першим входом u -го пристрою піднесення до степеня за модулем 11_u , вихід якого є u -им входом $(u + 4)$ -го пристрою додавання 12 та u -им виходом всього пристрою. Вихід $(u + 4)$ -го пристрою додавання 12 є другим входом $(u + 3)$ -го пристрою додавання 14 $_u$. Вихід регістра зберігання елемента ключової послідовності k_u 13 $_u$ з'єднано з першим входом $(u + 3)$ -го пристрою додавання 14 $_u$, вихід якого з'єднано з другим входом u -го пристрою піднесення до степеня за модулем 11_u . Вихід регістра зберігання значення модуля p_u 15 $_u$ є третім входом u -го пристрою піднесення до степеня за модулем 11_u .

Здійснення способу паралельного ключового хешування теоретично доведеної стійкості виконують на пристрої таким чином.

В регістр зберігання секретного числа a 4 заносять значення параметра a , в регістр зберігання секретного числа b 5 заносять значення параметра b , в регістр зберігання елемента ключової послідовності k_u 13 $_u$ заносять значення параметра k_u , в регістр зберігання значення модуля p_u 15 $_u$ заносять значення параметра p_u , встановлюють в початкове положення лічильник 1 згідно початкової адреси оперативного запам'ятовуючого пристрою 7, в який заносять інформаційні дані M , які подають у вигляді послідовності $M = \{m_1, m_2, \dots, m_t\}$. Значення виходу $(w + 4)$ -го пристрою додавання 12 встановлюють рівним нулю. Починають ітеративний процес. З лічильника 1 отримують попередню адресу i -го елемента інформаційної послідовності в оперативного запам'ятовуючого пристрою 7, яку надсилають до першого пристрою додавання 2 та другого пристрою додавання 2 отримують адресу $(i - a)$ -го елемента інформаційної послідовності, яку надсилають за допомогою першого блока комутації 6 до оперативного запам'ятовуючого пристрою 7, разом із значенням отриманої адреси $(i - b)$ -го елемента інформаційної послідовності з виходу другого пристрою додавання 3, яку надсилають за допомогою першого блока комутації 6. На виході оперативного запам'ятовуючого пристрою 7, отримують значення $(i-a)$ -го елемента інформаційної послідовності m_{i-a} , який надсилають до блока затримки 10 за допомогою другого блока комутації 8, значення $(i-b)$ -го елемента інформаційної послідовності m_{i-b} з виходу оперативного запам'ятовуючого пристрою 7, надсилають до третього пристрою додавання 9 за допомогою другого блока комутації 8, де його додають до значення з виходу блока затримки 10. Додають за допомогою $(u + 3)$ -го пристрою додавання 14 $_u$ частину ключа k_u , що зберігається в ре-

гістрі зберігання елемента ключової послідовності k_u , 13_u та значення виходу $(w + 4)$ -го пристрою додавання 12. u -ту частину результату додавання $(i-a)$ -го та $(i-b)$ -го елементів інформаційної послідовності $(m_{i-a} + m_{i-b})_u$ надсилають на вхід m -го пристрою піднесення до степеня за модулем 11_u , де згідно вхідних значень з $(u+3)$ -го пристрою додавання 14_u виконують піднесення до степеня за модулем p_u , отриманим з виходу регістра збері-

гання значення модуля p_u , 15_u . Результат h_{iu} , отриманий в u -му пристрої піднесення до степеня за модулем 11_u , надсилають на u -ий вхід $(w + 4)$ -го пристрою додавання 12, за допомогою якого визначають суму h^*_{i-1} всіх частин i -го хеш-значення h_{iu} , та на u -ий вихід всього пристрою. Результуючим хеш-значенням H буде результат конкатенації всіх h_{iu} .

