УКРАЇНА

(19) UA (11) 64925 (13) U

(51) МПК (2011.01)
G09C 1/00

ДЕРЖАВНА СЛУЖБА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ УКРАЇНИ

ОПИС
ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

видається під відповідальність власника патенту

(54) СПОСІБ КЛЮЧОВОГО ХЕШУВАННЯ ТЕОРЕТИЧНО ДОВЕДЕНОЇ СТІЙКОСТІ НА ОСНОВІ ЕЛІПТИЧНИХ КРИВИХ

(21) u201104428
(22) 11.04.2011
(24) 25.11.2011
(46) 25.11.2011, Бюл.№ 22, 2011 р.
(72) ЛУЖЕЦЬКИЙ ВОЛОДИМИР АНДРІЙОВИЧ, БАРИШЕВ ЮРІЙ ВОЛОДИМИРОВИЧ, ЧЕРНЯХОВИЧ КОСТЯНТИН ВІТАЛІЙОВИЧ, ОЛЕКСЮК АНЕЛІЯ ОЛЕКСІЇВНА
(73) ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
(57) Спосіб ключового хешування теоретично доведеної стійкості на основі еліптичних кривих, який полягає в тому, що інформаційні дані M подають у вигляді послідовності $M=\{m_1, m_2,...,m_\ell\}$, задача зламу ключа хешування зводиться до обчислення дискретного логарифма в полі простого числа, який **відрізняється** тим, що хешування здійснюється шляхом множення точки еліптичної кривої на скаляр, який отримують шляхом додавання значення блока даних $m_\ell\left(i=\overline{1,\ell}\right)$, персонального ключа k* та проміжного хеш-значення, отриманого на попередній ітерації h_{i-1}, множення точки еліптичної кривої на скаляр відбувається шляхом додавання набору наперед обчислених точок $2^{(j-1)}P$ $\left(j=\overline{1,n}\right.$, де n - розрядність вихідного хеш-значення), ключові дані представлені персональним ключем k*.

Корисна модель належить 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., МПК 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, в подальшому пристрою піднесення до степеня за модулем, 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, в подальшому як початкове заповнення h_0, а задача зламу ключа хешування зводиться до обчислення дискретного логарифма в полі простого числа.

Недоліком цього способу 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 полі простого числа.

Найбільш близьким до способу, що пропонується є спосіб ключового хешування теоретично доведеної стійкості [Патент України № 50818 від 25.06.2010 р., МПК G 09 C 1/00, бюл. № 12 2010 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, 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 k використовують як початкове заповнення h_0, задача зламу ключа хешування зводиться до обчислення дискретного логари-

(19) UA (11) 64925 (13) U

фма в простому полі, підносять велике число g, яке є примітивним коренем за модулем p, степінь, до якого виконують піднесення, є результатом додавання значення елемента інформаційної послідовності т* та результату хешування попереднього елемента інформаційної послідовності.

Недоліком прототипу є недостатня швидкість хешування, внаслідок того, що для реалізації піднесення до степеня розрядності n необхідно виконати $O(2^n)$ операцій множення за ітеративним алгоритмом.

В основу корисної моделі поставлена задача створити спосіб ключового хешування теоретично доведеної стійкості на основі еліптичних кривих, який дозволить забезпечити підвищення швидкості хешування шляхом передобчислень значень точок еліптичної кривої $2^{j-1}P \ (j = \overline{1,n}$, де n - розрядність вихідного хеш-значення).

Поставлена задача вирішується за рахунок того, що в способі ключового хешування теоретично доведеної стійкості на основі еліптичних кривих інформаційні дані M подають у вигляді послідовності $M= \{m_1, m_2,\ldots, m_\ell\}$, задача зламу ключа хешування зводиться до обчислення дискретного логарифма в полі простого числа, причому хешування здійснюється шляхом множення точки еліптичної кривої на скаляр, який отримують шляхом додавання значення блока даних персонального ключа та проміжного хеш-значення, отриманого на попередній ітерації, множення точки еліптичної кривої на скаляр відбувається шляхом додавання набору наперед обчислених точок $2^{(j-1)}P \ (j = \overline{1,n}$, де n - розрядність вихідного хеш-значення), ключові дані представлені персональним ключем.

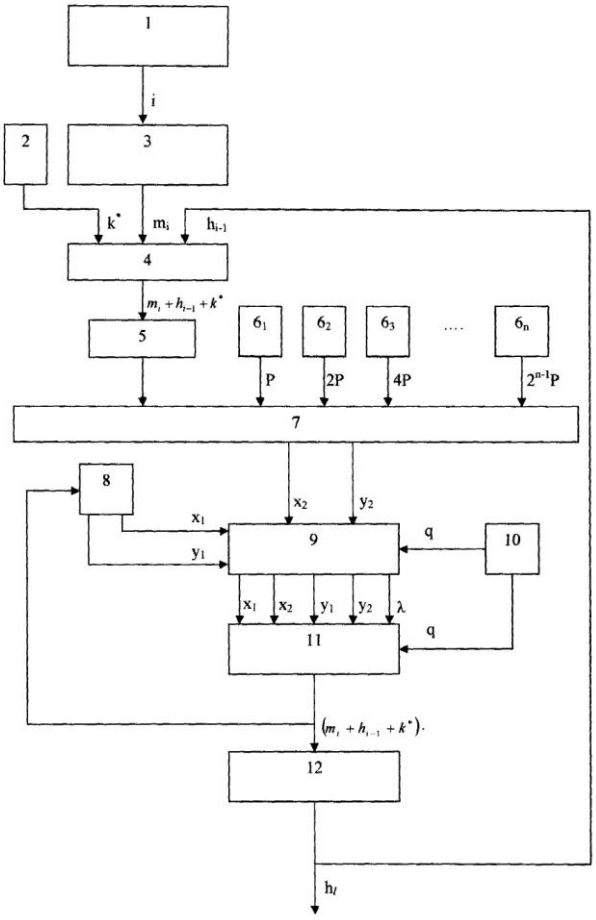
На кресленні наведена схема пристрою, що реалізує спосіб ключового хешування теоретично доведеної стійкості на основі еліптичних кривих.

Пристрій містить лічильник 1, вихід якого з'єднано з входом оперативно запам'ятовуючого пристрою 3, вихід якого з'єднано з входом блока додавання 4. Другий вхід блока додавання 4 є виходом блока збереження персонального ключа k* 2. Вихід блока додавання 4 є входом блока керування 5, вихід якого є (n+1)-м входом комутатора 7. 1-м входом комутатора є вихід блока збереження точки еліптичної кривої $2^{j-1}P$ 6_i. Перший вихід блока комутатора 7 з'єднано з першим входом блока обчислення λ 9, другий вихід блока комутатора 7 з'єднано з другим входом блока обчислення λ 9, третім входом блока обчислення λ 9 є перший вихід блока збереження точки еліптичної кривої P* 8, четвертим входом блока обчислення λ 9 є другий вихід блока збереження точки еліптичної кривої P* 8, п'ятим входом блока обчислення λ 9 є перший вихід блока збереження модуля q 10. Перший, другий, третій, четвертий, п'ятий виходи блока обчислення A, 9 є першим, другим, третім, четвертим, п'ятим входами блока додавання точок еліптичної кривої 11 відповідно. Шостим входом блока додавання точок еліптичної кривої 11 є другий вихід блока збереження модуля q 10. Вихід блока додавання точок еліптичної кривої 11 є входом блока збереження точки еліптичної кривої P* 8 та входом блока перетворення 12. Вихід блока перетворення 12 є третім входом блока додавання 4 та виходом всього пристрою.

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

Лічильник 1 встановлюють відповідно початкової адреси оперативно запам'ятовуючого пристрою 3. В блок збереження персонального ключа k* 2 заносять значення персонального ключа k*. В блок збереження точки еліптичної кривої $2^{j-1}P$ 6_j заносять координати точки еліптичної кривої $2^{j-1}P$. В блок збереження точки еліптичної кривої P* 8 заносять значення координат нульової точки еліптичної кривої. В блок збереження модуля q 10 заносять значення модуля q. В оперативно запам'ятовуючий пристрій 3 заносять інформаційні дані M, які подають у вигляді послідовності $M= \{m_1, m_2,\ldots, m_\ell\}$. Починають ітеративний процес. З лічильника 1 отримують адресу i-го елемента інформаційної послідовності, яку надсилають до оперативно запам'ятовуючого пристрою 3, де на виході отримують значення i-го елемента інформаційної послідовності m_i, яке надсилають до блока додавання 4. За допомогою блока додавання 4 отримують значення суми $m_i + h_{i-1} + k^*$ шляхом додавання значення елемента інформаційної послідовності m_i, значення (i-1)-го проміжного хеш-значення h_{i-1}, яке надходить з виходу блока перетворення 12, та значення персонального ключа k*, яке отримують з виходу блока збереження персонального ключа k* 2. Значення суми $m_i+h_{i-1}+k^*$ подають на вхід блока керування 5, де визначають послідовність керуючих сигналів для комутатора 7 для обчислення $(m_i+h_{i-1}+k^*) \cdot P$, кожен з яких послідовно надсилають на (n+1) -й вхід комутатора 7. Починають процедуру додавання точки еліптичної кривої. За допомогою комутатора 7 відповідно до керуючого сигналу подають на перший вихід значення координати x, а на другий вихід - значення координати y, які отримують з j-го входу комутатора 7. З блока збереження точки еліптичної кривої P* 8 на перший вихід подають координату x даної точки, а на другий - координату y. Перший вихід блока збереження точки еліптичної кривої P* 8 є третім входом блока обчислення λ 9, а другий вихід блока збереження точки еліптичної кривої P* 8 є четвертим входом блока обчислення λ 9. На п'ятий вхід блока обчислення λ 9 подають значення модуля q, який отримують з першого виходу блока збереження модуля q 10. Значення x1, y1, x2, y2, та λ, які отримують з першого, другого, третього, четвертого, та п'ятого виходів блока обчислення λ 9 відповідно, подають на перший, другий, третій, четвертий та п'ятий входи блока додавання точок еліптичної кривої 11 відповідно. На шостий вхід блока додавання точок еліптичної кривої 11 подають значення модуля q, який отримують з другого виходу блока збереження модуля q 10. Значення, яке отримують на виході блока додавання точок еліптичної кривої 11 подають на вхід блока перетворення 12 та на вхід блока збереження точки еліптичної кривої P* 8. Завершують процедуру

додавання точки еліптичної кривої. Надсилають наступний керуючий сигнал з блока керування 5 до комутатора 7 та повторюють процедуру додавання точки еліптичної кривої доти, доки точка еліптичної кривої $(m_i+h_{i-1}+k^*)\cdot P$ не буде обчислена. За допомогою блока перетворення 12 координати точки еліптичної кривої $(m_i+h_{i-1}+k^*)\cdot P$ перетворюють у проміжне хеш-значення h_i. Результат, який отримують на виході блока перетворення 12, подають на третій вхід блока додавання 4. Починають наступну ітерацію. На ℓ-ій ітерації на виході блока перетворення 12 отримують вихідне значення результату хешування.



Комп'ютерна верстка А. Крижанівський Підписне Тираж 23 прим.

Державна служба інтелектуальної власності України, вул. Урицького, 45, м. Київ, МСП, 03680, Україна

ДП "Український інститут промислової власності", вул. Глазунова, 1, м. Київ – 42, 01601