УКРАЇНА

(19) UA (11) 96826 (13) C2

(51) МПК
H04L 9/06 (2006.01)

ДЕРЖАВНА СЛУЖБА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ УКРАЇНИ

ОПИС
ДО ПАТЕНТУ НА ВИНАХІД

(54) СПОСІБ СИМЕТРИЧНОГО ШИФРУВАННЯ ДАНИХ

(21) a201001987
(22) 23.02.2010
(24) 12.12.2011
(46) 12.12.2011, Бюл.№ 23, 2011 р.
(72) БРИТІК ВОЛОДИМИР ІВАНОВИЧ, КОБЗЄВ ВОЛОДИМИР ГРИГОРОВИЧ, МАРКОВА ЛЮБОВ ІВАНІВНА, ПУТЯТІН ЄВГЕНІЙ ПЕТРОВИЧ, СТРУКОВ ЄВГЕНІЙ ВОЛОДИМИРОВИЧ
(73) ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ
(56) UA 50199 A; 15.10.2002; 4 сторінки
RU 2359415 C2; 20.06.2009; 31 сторінка
KR 20080112082; 24.12.2008; 33 сторінки
ГОСТ 28147-89, Системы обработки информации. Защита криптографическая, Москва, 1989, 28 страниц
UA 42531 A; 15.10.2001; 4 сторінки
RU 2140709 C1; 27.10.1999; 10 сторінок
RU 2106752 C1; 10.03.1998; 7 сторінок
WO 9845975 A2; 15.10.1998; 51 сторінка
US 5926549 A; 20.07.1999; 7 сторінок
JP 2006320014 A; 24.11.2006; 30 сторінок
(57) Спосіб симетричного шифрування даних, який полягає в тому, що шифрування здійснюється за допомогою блокового шифру із 256-бітовим ключем і 32 циклами перетворення, що оперує 64-бітними блоками і використовує мережу Фейстеля, який **відрізняється** тим, що формування ключів і підключів виконується за допомогою трьох детермінованих складових, які є випадковими щодо інформації, яка передається, при цьому ключ формується в три етапи - передача інформації про зображення, передача інформації про локальні фрагменти на зображенні, передача інформації про значення фільтра, що дозволяє сформувати значення ключа W шляхом конкатенації координат x_{L_i} і y_{L_j}, отриманих у результаті згортки точок локального фрагмента з маскою, що визначається особливістю цього фрагмента за формулою:

$$\max_{S_{L_i}} g_{i,j} = \max_{S_{L_i}} \left\{ \sum_{p=-P/2}^{+P/2} \sum_{q=-Q/2}^{+Q/2} m_{p,q} \cdot B\left(x_{i+p}, y_{j+q}\right) \bmod 256 \right\},$$

де S_{L_i} - вибраний багатокутник,

$g_{i,j}$ - значення згортки відносно якого будуть зафіксовані значення i, j - x_{L_i} і y_{L_j} відповідно,

P, Q - кількість рядків і стовпців матриці дійсних значень фільтра,

$m_{p,q}$ - значення цього фільтра з координатами $p \in P$, $q \in Q$,

$B(x_i, y_j)$ - значення інтенсивності в точці x_i, y_l - $i \in M, j \in N$ на вибраному зображенні,

яка є випадкова щодо інформації, яка передається, і постійна щодо процесу зашифрування-розшифрування і яка є складовою ключа.

Винахід належить до області забезпечення захисту інформації, переданої по мережах зв'язку, зокрема забезпечення захисту переданої інформації в системах цифрового радіозв'язку, супутниковому зв'язку, а саме до криптографічних способів захисту інформації з використанням симетричного ключа.

Відомий спосіб шифрування даних, система відкритого ключа RSA (PKCS #1 v2.1: RSA Cryptography Standard RSA Laboratories June 14, 2002) - в основу якої покладена складність розкладання великого числа на прості множники, де обчислюються добутки двох досить великих простих чисел p і q, n=p*q; n - модуль, на основі якого обчислюються відкриті й закриті ключі: (n; e) - відкритий (public) ключ і закриті (n; d) - приватний (private) ключ. Алгоритм обчислення полягає у виборі числа e (e - відкритий (public) показник), що задовольняє умові 1<e<(p-1)*(q-1) і не має спільних дільників, крім 1 (взаємно простої) із числом (p-1)*(q-1). Потім обчислюється число d (d - приватний (private) показник) таким чином, що (e*d-1) ділиться націло на (p-1)*(q-1). Дільники (фактори) p і q можна або знищити, або зберегти разом із часткою (private) ключа. Для зашифрування повідомлення його наводять у вигляді числа m, яке повинно бути менше модуля n алгоритму. Шифротекст C отримується з числа m за наступним правилом:

$c=m^B \pmod n$.

(19) UA (11) 96826 (13) C2

Розшифрування повідомлення проводиться за наступною формулою:

$m=c^d(\mathrm{mod}\ n)$.

Недоліками цього способу є низька швидкість шифрування, необхідність вибору ключів довжиною не менше 1024-2048 бітів, що значно зменшує швидкість роботи алгоритму, складність забезпечення регулярної заміни ключа для дотримання необхідного рівня безпеки, необхідність вибору двох великих простих чисел, що є досить громіздкою задачею, та також можливість атаки по передбачуваному відкритому тексту.

Найбільш близьким за сукупністю ознак до запропонованого є спосіб шифрування даних, що реалізується криптосистемою (ДЕРЖСТАНДАРТ 28147-89) - блоковий шифр із 256-бітовим ключем і 32 циклами перетворення, що оперує 64-бітними блоками. Основа алгоритму шифру - Мережа Фейстеля. Базовим режимом шифрування є режим простої заміни, а також визначені більш складні режими гамування, гамування зі зворотним зв'язком і режим імітовставки. Для зашифрування в цьому режимі відкритий текст спочатку розбивається на дві половини (молодші біти - A, старші біти - B). На i-ому циклі використовується підключ K_i:

$A_{i+1}=B_i \oplus f(A_i, K_i)$ ($\oplus$ - двійкове «або, що виключає»),

$B_{i+1}=A_i$

Для генерації підключів вихідний 256-бітний ключ розбивається на вісім 32-бітних блоків: $K_1...K_8$..... Ключі $K_9...K_{24}$ є циклічним повторенням ключів $K_1...K_8$ (нумеруються від молодших бітів до старшого). Ключі $K_{25}...K_{32}$ є ключами $K_1...K_8$, які ідуть у зворотному порядку. Після виконання усіх 32 кроків алгоритму, блоки A_{33} і B_{33} склеюються: старшим бітом стає A_{33}, а молодшим - B_{33}. Це є результат роботи алгоритму. Розшифрування виконується так само, як і зашифровування, але інвертується порядок підключів K_i. Функція $f(A_i, K_i)$ обчислюється в такий спосіб: A_i і K_i складаються по модулю 2^{32}. Результат розбивається на вісім 4-бітових підпослідовностей, кожна з яких надходить на вхід свого вузла таблиці замін (у порядку зростання старшинства бітів), названого S-Блоком. Загальна кількість S-Блоків - вісім, тобто стільки ж, скільки й підпослідовностей. Кожний S-Блок являє собою перестановку чисел від 0 до 15. Перша 4-бітна підпослідовність попадає на вхід першого S-Блока, друга - на вхід другого й т.д. Якщо S-Блок виглядає так: 1, 15, 13, 0, 5, 7, 10, 4, 9, 2, 3, 14, 6, 11, 8, 12 і на вході S-Блока 0, то на виході буде 1, якщо 5, то на виході буде 7 і т.д. Виходи всіх восьми S-Блоків поєднуються в 32-бітне слово, потім усе слово циклічно зрушується вліво (до старших розрядів) на 11 бітів. Всі вісім S-Блоків можуть бути різними. Фактично, вони можуть бути додатковим ключовим матеріалом, але частіше є параметром схеми, загальним для певної групи користувачів. Недоліками є складність передачі ключа, неможливість визначити криптостійкість, не знаючи заздалегідь таблиць замін; а також несумісність різних таблиць замін від різних виробників приводить до неможливості реалізації цього способу.

В основу винаходу поставлена задача опосередкованої передачі великого кодового числа по засекречених каналах без можливості їх ідентифікування. Такий технічний результат досягається тим, що спосіб симетричного шифрування даних, який полягає в тому, що шифрування здійснюється за допомогою блокового шифру із 256-бітовим ключем і 32 циклами перетворення, що оперує 64-бітними блоками і використовує мережу Фейстеля, відповідно до винаходу, формування ключів і підключів виконується за допомогою трьох детермінованих складових, які є випадковими щодо інформації, при цьому ключ формується в три етапи - передача інформації що до зображення, передача інформації про локальні фрагменти на зображенні, передача інформації про значення фільтра, що дозволяє сформувати значення ключа W шляхом конкатенації координат x_{L_i}, і y_{L_j}, отриманих у результаті згортки точок локального фрагмента з маскою, що визначається деякою особливістю цього фрагмента за формулою

$$\max_{S_{L_i}} g_{i,j} = \max_{S_{L_i}} \left\{ \sum_{p=-P/2}^{+P/2} \sum_{q=-Q/2}^{+Q/2} m_{p,q} \cdot B\left(x_{i+p}, y_{j+q}\right) \mathrm{mod} 256 \right\},$$

яка є випадкова щодо інформації, яка передається і постійна щодо процесу зашифрування-розшифрування і яка є складовою ключа.

Запропонований спосіб симетричного кодування здійснюється таким чином, що припускає наявність одного або декількох ідентичних криптографічних ключів і відрізняється тим, що ключі не вибираються безпосередньо, а генеруються випадковим чином за допомогою виконання операції згортки вибраних локальних фрагментів L одного із множини K зображень на спеціальному або вибраному за якою-небудь ознакою сайтові, розміром M*N, наведеного у вигляді двовимірного масиву дійсних чисел $B[x_i,y_j]$ - значення інтенсивності (яскравості для напівтонового зображення) або компонента вектора інтенсивності для мультиспектрального зображення), де x_i, y_j - номера рядків і стовпців, відповідно, (i=1,..., M; j=1,..., N), а M - кількість рядків, N - кількість стовпців; локальні фрагменти L визначаються шляхом задання їхніх геометричних особливостей - координат точок вершин багатокутників S або центрів і радіусів кіл S, необов'язково покриваючи все зображення, й однієї або декількох масок - цифрових фільтрів із множини F, що являють собою матрицю дійсних значень фільтру розміром PxQ, (зазвичай P=Q, наприклад, розміром 3x3, 5x5,...)

M=

$m_{-1,-1}$	$m_{-1,0}$	$m_{-1,1}$
$m_{0,-1}$	$m_{0,0}$	$m_{0,1}$
$m_{1,-1}$	$m_{1,0}$	$m_{1,1}$

значення якої можуть бути як закритими, так і відкритими параметрами формування криптографічного ключа, отриманого шляхом конкатенації координат x_{L_i} і y_{L_j}, отриманих у результаті згортки точок локального фрагменту з маскою й визначальною деякою особливістю цього фрагменту за формулою

$$\max_{S_{L_i}} g_{i,j} = \max_{S_{L_i}} \left\{ \sum_{p=-P/2}^{+P/2} \sum_{q=-Q/2}^{+Q/2} m_{p,q} \cdot B(x_{i+p}, y_{j+q}) \bmod 256 \right\},$$

де S_{L_i} - вибраний багатокутник, $g_{i,j}$ - значення згортки відносно якого будуть зафіксовані значення i,j - x_{L_i} і y_{L_j} відповідно, P, Q - кількість рядків і стовпців матриці дійсних значень фільтра, де $m_{p,q}$ значення цього фільтра з координатами $p \in P$, $q \in Q$, $B(x_i,y_j)$ - значення інтенсивності в точці x_i, y_j - $i \in M$, $j \in N$ на вибраному зображенні. Алгоритм криптографічного перетворення передбачає режими роботи, аналогічні аналогу. У всіх режимах використовується ключ W необхідної довжини (256 біт), який представляється у вигляді восьми 32-розрядних чисел (x_{L_i} , y_{L_j}).

$$W = (x_{L_{i1}}, y_{L_{j1}})(x_{L_{i2}}, y_{L_{j2}})(x_{L_{i3}}, y_{L_{j3}})..(x_{L_{i7}}, y_{L_{j7}})(x_{L_{i8}}, y_{L_{j8}}).$$

Користувач довільним чином вибирає деяке зображення, довільного розміру, наприклад NxM, із множини К. Імовірність визначення цього зображення криптоаналітиком становить: $P_3=1/F$. На вибраному зображенні користувач задає множину L довільних S - вугільних фігур, що покривають зображення, які є початковими даними для формування коду шифрування. Криптоаналітик може розпізнати координати однієї вибраної точки з імовірністю 1/(NxM). А імовірність розпізнавання криптоаналітиком всіх точок становить:

$$P_2 = \left[\frac{1}{N \times M} \right]^{L \times 5}.$$

З довільного числа фільтрів (масок) F, вибирається один. Загальне число яких залежить від розмірів (PxQ) і може скласти 511^{PxQ} за умови, що кожне значення фільтра лежить у діапазоні - 255≤m≤255. Імовірність визначення вибраного фільтра криптоаналітиком, за умови, що йому відомий набір фільтрів F, становить:

$P_3=1/F$.

За допомогою вибраного фільтра на заданій множині L довільних S-вугільних фігур, що покривають зображення, виділяємо характерні точки, отримані у результаті згортки точок локального фрагмента з маскою. Очевидно, що використовуючи тверду нерівність при пошуку ця точка єдина. Ці L точок мають 2L координат (L координат x і L координат y). Формування коду складається в конкатенації отриманих координат x і y. Кількість всіх можливих варіантів конкатенації становить (2xL)!, а імовірність розпізнавання криптоаналітиком:

$P_4=1/(2xL)!$

Загальна ймовірність розкриття представленого коду криптоаналітиком становить:

$$P_0 = \frac{1}{K} \times \left[\frac{1}{N \times M} \right]^{L \times 5} \times \frac{1}{\Gamma} \times \frac{1}{(2 \times L)!} = \frac{1}{K} \times \left[\frac{1}{N \times M} \right]^{L \times 5} \times \frac{1}{511^{P \times Q}} \times \frac{1}{(2 \times L)!}.$$

Пропонований спосіб вирішує наступні проблеми: цифровий підпис забезпечується передачею зворотного повідомлення, закодованого зміненим кодом; генерація ключів об'єднує у собі простоту запам'ятовування й використовує генератор «натурального» випадкового процесу; нагромадження ключів у вигляді їхніх складових, що виключає можливість його зчитування; розподіл ключів - прямий обмін ключами між користувачами інформаційної системи, що дозволяють виконати ідентифікацію.

Комп'ютерна верстка А. Крулевський 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