



УКРАЇНА

(19) UA

(11) 53949

(13) A

(51) 7 H04L29/14

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІОПИС
ДО ДЕКЛАРАЦІЙНОГО ПАТЕНТУ
НА ВІНАХІДВИДАЄТЬСЯ ПІД
ВІДПОВІДАЛЬНІСТЬ
ВЛАСНИКА
ПАТЕНТУ

(54) СПОСІБ НЕДЕТЕРМІНОВАНОГО КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ БЛОКІВ ДАНИХ

1

2

(21) 2002032372

(22) 26 03 2002

(24) 17 02 2003

(72) Долгов Віктор Іванович, Супрунук Сергій Володимирович, Лисицька Ірина Вікторівна

(73) ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

(57) Спосіб недетермінованого криптографічного перетворення блоків даних, що полягає у формуванні ключа шифрування у вигляді сукупності підключів, розбивці блока даних на підблоки і почерговому перетворенні підблоків на основі керованих підстановок, який відрізняється тим, що таблицю підстановок подають у вигляді латинського прямо-

кутника, розмірність якого визначається підблоком, що шифрують, а саме перетворення на основі керованої підстановки виконують по черзі в двох напрямках, причому в одному напрямку використовують підстановки-рядки, а в іншому напрямку підстановки-стовпці латинського прямокутника, при цьому номер кожної чергової конкретної підстановки задають попереднім зашифрованим підблоком, а між перетвореннями в кожному з напрямків вводять операцію додавання підблоків даних із ключем, що вибирають параметрично в залежності від значення останнього зашифрованого підблока, що передуює потоковій операції керованої підстановки

Винахід відноситься до галузі обчислювальної техніки, а саме до способів і пристроїв криптографічного перетворення даних

Відомий недетермінований спосіб шифрування блоків даних, патент № 2108752 РФ, МПК 6 H04L9/00 Опубл. 10.03.98 Бюл. № 7 Спосіб включає формування ключа шифрування у вигляді сукупності підключів, генерування машинного коду програми шифрування, розбивку блоку даних на підблоки і почергове перетворення підблоків, що відрізняються від відомих способів тим, що додатково формують двійковий вектор, а на i -тий підблок B_i , де $i = 1, 2, 3, \dots, N \geq 2$ - число підблоків, накладають i -тий підключ, де $i = 1, 2, 3, \dots, k \geq 8$ число підключів, при цьому значенню сформованого двійкового вектора присвоюють, значення i підключа. Сам двійковий вектор формують за структурою j -того підблока B_j , $j = 1, 2, 3, \dots, N$, причому $j \neq i$, і номера підключа, накладеного на підблок на попередньому кроці накладення

У даному способі шифрування використовуються попередня генерація машинного коду програми, унаслідок чого даний спосіб вимагає значних попередніх обчислень. У ряді випадків, де потрібно шифрування невеликих блоків даних на різних ключах, даний спосіб застосувати неможливо.

Найбільш близькими по сукупності суттєвих

ознак до способу, що заявляється, є шифр на основі керованих підстановок, (див. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография СПб. Изд. «Лань», 2000 с. 136 - 142) Шифрування виконують таким чином. Вхідний блок 64 біт розбивають на 8 підблоків $b_0, b_1, b_2, \dots, b_7$ розміром 8 біт кожний. Після цього формують двійковий вектор v , що має значення 5 молодших двійкових розрядів підблока b_0 : $v \leftarrow b_0 \bmod 2^5$. Потім над блоком b_1 і підключем k_1 виконують операцію порозрядного підсумовування за модулем 2 і вихідне значення результату цієї операції присвоюють блоку b_1 : $b_1 \leftarrow b_1 \oplus k_1$. Потім відповідно до таблиці підстановок з номером v виконують операцію підстановки над блоком b_1 : $b_1 \leftarrow Sv(b_1)$. За значенням b_1 формують двійковий вектор v : $v \leftarrow v \oplus (b_1 \bmod 2^5)$, при цьому нове значення двійкового вектора залежить від попереднього значення. Після цього виконують операцію підстановки над підблоком b_2 : $b_2 \leftarrow Sv(b_2)$. Аналогічно виконують перетворення підблоків b_3, b_4, b_5, b_6, b_7 . На останньому кроці кожного циклу шифрування виконують перестановку блоків у зворотному напрямку.

У даному алгоритмі для вибору однієї з підстановок використовується 5 з 8 біт підблока, що значно погіршує показники лавинного ефекту. Операція формування двійкового вектора v сповільнює швидкість алгоритму, додатково усклад-

(13) A

(11) 53949

(19) UA

нюючи його криптографічний аналіз

В основу винаходу поставлена мета створення недетермінованого способу криптографічного перетворення блоків даних, у якому нова послідовність дій дозволяла б забезпечити високі показники лавинного ефекту, стійкості, простоти і швидкості перетворення

Такий технічний результат може бути досягнутий тим, що в недетермінованому способі криптографічного перетворення блоків даних, що полягає у формуванні ключа шифрування у вигляді сукупності підключів, розбивці блоку даних на підблоки і поточковому перетворенні підблоків на основі керованих підстановок, згідно винаходу, таблицю підстановок подають у виді латинського прямокутника, розмірність якого визначають підблоком, що шифрується, а дійсне перетворення на основі керованої підстановки виконують по черзі в двох напрямках, при цьому в одному напрямку використовують підстановки-рядки, а в іншому напрямку підстановки-стовпці латинського прямокутника, при цьому номер кожної чергової конкретної підстановки задають попереднім зашифрованим підблоком, а між перетвореннями в кожному з напрямків вводять операцію додавання підблоків даних із ключем, що вибирається параметрично в залежності від значення останнього шифрованого підблоку, що передусє поточній операції керованої підстановки

Заявлений спосіб дозволяє поглибити показники лавинного ефекту за кількістю циклів в 5 - 6 разів. Невизначеність криптоаналітика на кожному циклі перетворення збільшується з 2^{35} до 2^{64} . Крім того, в алгоритмі використовується не 32 а 512 підстановок, що приводить до збільшення стійкості алгоритму. Криптографічна стійкість нового алгоритму шифрування виявляється набагато вище. За рахунок зменшення кількості циклів можливо одержати вигаш у швидкості шифрування. Спосіб дозволяє збільшити швидкість перетворення більш ніж у два рази, при збереженні тієї ж стійкості. В способі використовуються усього три різних операції, такі як керована підстановка, параметричний вибір підключів, додавання ключа до перетвореного блоку, що говорить про простоту способу, який має перевагу перед складними і запутаними. Його легше реалізувати і налагодити. Крім того, що більш важливо, він прозорий для аналізу і більш зрозумілий. Поданий спосіб дозволяє зменшити коефіцієнт стиску шифрованих після першого циклу перетворення даних у 2 - 3 рази, при збільшенні швидкості перетворень. Це досягнуто не тільки завдяки збільшенню кількості підстановок, але і завдяки тому що вони обов'язково повинні утворювати латинський прямокутник (квадрат), що неможливо у попередній структурі алгоритму. Більш того, операція параметричного вибору підключів забезпечує додаткову неоднозначність у ключовому просторі. Завдяки поточковому використанню операцій керованої підстановки і параметричного вибору підключів в способі досягається необхідна стійкість, швидкість і простота перетворень

На фіг 1 зображено обчислювальний пристрій, фіг 2 - операція керованої підстановки, де як підстановки використовуються рядки латинського

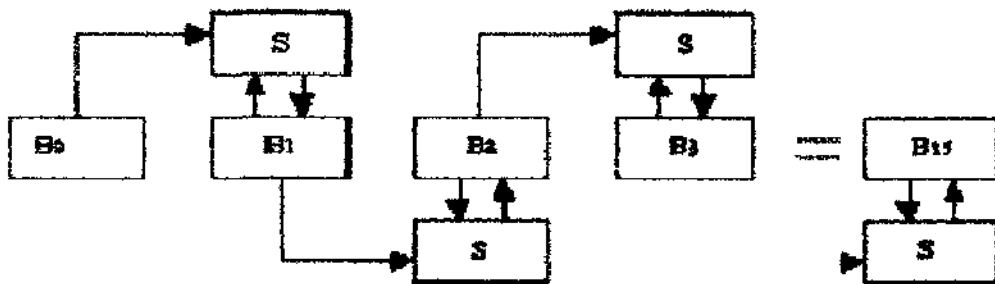
прямокутника, фіг 3 - ключова операція, де ключ обирається в залежності від останнього підблоку даних, фіг 4 - операція керованої підстановки, де як підстановки використовуються стовпці латинського прямокутника, фіг 5 ключова операція, де ключ обирається в залежності від першого підблоку даних

Запропонований спосіб може бути реалізований за допомогою обчислювального пристрою, представленого блок-схемою на фіг 1, де пристрій введення пароля користувача 1, блок формування ключа шифрування 2, генератор матриці значень з властивостями латинського прямокутника 3, шина передачі пароля користувача 4 до блока 2, шина передачі сформованих підключів 5, шина передачі значень сформованих елементів латинського прямокутника 6, пристрій шифрування 7, у якому знаходиться блок пам'яті сформованих підключів 8, блок пам'яті елементів латинського прямокутника 9, операційний блок пристрою шифрування 10, шина передачі ключів 11, адресні шини 12 і 13, шина передачі елементів латинського прямокутника 14, шина виходу шифрованого тексту 15, шина введення вхідних даних 16

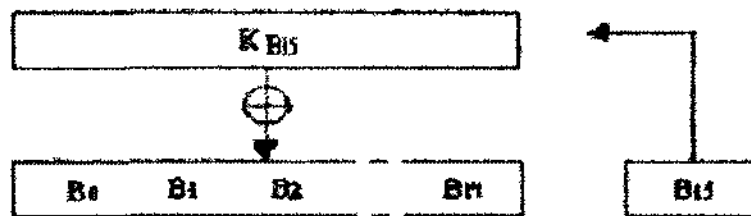
Використовуючи блок 1, вводять секретний ключ розміром, наприклад, 128 біт, значення якого по шині 4 передають до блоку 2. У блоці 2 формують розгорнутий ключ шифрування шляхом циклічного зсуву наявного шифрключа на n розрядів уліво, де $n = 0, 1, 2, \dots, 255$. Кожен сформований підключ передають по шині 5 у блок пам'яті 8. У блоці 3 відбувається одноразово для всього алгоритму генерування матриці значень, у стовпцях якої відсутні збіги, а в рядках немає повторень. Матриця значень, має назву латинський прямокутник. Отримані значення передаються по шині 6 до блоку пам'яті 9, де зберігаються. Після цього пристрій шифрування 7 готовий до криптографічних перетворень. Вхідну інформацію B , розміром наприклад 128 біт, подають на шину 16 і вона поступає у операційний блок 10, де розміщується у вигляді сукупності підблоків B_0, B_1, \dots, B_m , де $m = 15$, по 8 біт у кожному, причому підблоки записуються по фіксованих адресах. Перетворення на основі керованих підстановок, де як підстановки використовуються рядки латинського прямокутника зображено на фіг 2. Перші два підблока B_0, B_1 попадають на шину адресації 13, тим самим задають вибір одного з можливих значень S_{B_0, B_1} латинського прямокутника у блоку пам'яті 9. Обране значення, S_{B_0, B_1} через шину 14 поступає до блоку 10 і присвоюється підблоку $B_0, B_1 \leftarrow S(B_0, B_1)$. Далі наступні два блоки B_0, B_1 попадають на шину адресації 13, тим самим задають вибір одного з можливих значень, S_{B_0, B_1} латинського прямокутника у блоку пам'яті 9. Обране значення S_{B_0, B_1} через шину 14 поступає до блоку 10 і присвоюється підблоку $B_2, B_2 \leftarrow S(B_0, B_1)$. Аналогічно виконується перетворення підблоків B_3, B_4, \dots, B_{15} . $B_n \leftarrow S(B_{n-1}, B_n)$, де $n = 3, \dots, 15$. Чергове ключове перетворення зображено на фіг 3, у якому підблок B_{15} попадає на шину адресації 11 і тим самим задає один з можливих підключів K у блоці 8. Обраний підключ $K_{B_{15}}$ через шину 11 поступає у блок 10, де підсумовується з підблоками B_0, B_1, \dots, B_{14} . $B \leftarrow B \oplus K_{B_{15}}$. Наступне перетворення на основі керованих під-

становок, де як підстановки використовуються стовпці латинського прямокутника, зображено на фіг 5. Останні два підблоки B_{15} , B_{14} попадають на шину адресації 13, тим самим задають вибір одного з можливих значень $S_{B_{15}B_{14}}$ латинського прямокутника у блоці пам'яті 9. Обране значення через шину 14 поступає у блок 10 і присвоюється підблоку B_{14} . $B_{14} \leftarrow S(B_{15}, B_{14})$. Аналогічно виконується перетворення підблоки B_{13} , B_{12} , ..., B_0 , $B_n \leftarrow S(B_{n+1},$

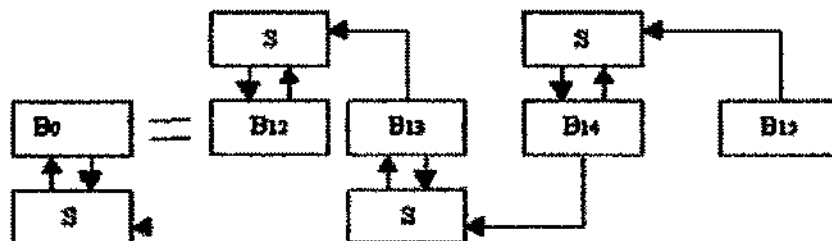
$B_n)$, де $n = 13, 12, 11, \dots, 0$. Чергове ключове перетворення зображено на фіг 3, у якому підблок B_0 попадає на шину адресації 12 і тим самим задає один з можливих підключів K у блоці 8. Обраний підключ K_{B_0} , поступає на шину 11 у блок 10, де підсумовується з підблоками $B_1, B_2, B_3, \dots, B_{15}$. $B \leftarrow \oplus K_{B_{15}}$



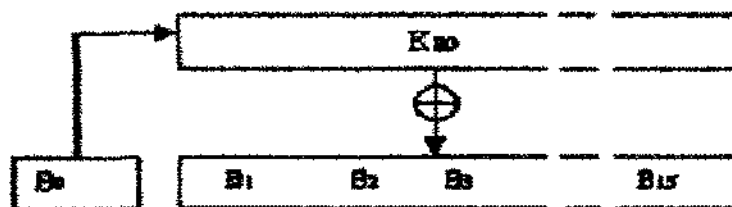
Фиг. 1



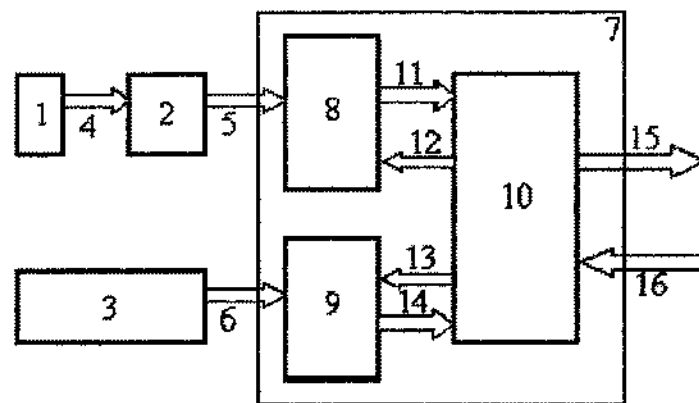
Фиг. 2



Фиг. 3



Фиг. 4



Фиг. 5