(19) UA (11) 51 836 (13) C2

(51)МПК 7 H 04L 9/00 A

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ

ГОСУДАРСТВЕННЫЙ ДЕПАРТАМЕНТ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ УКРАИНЫ

(21), (22) Заявка: 2000095323, 19.06.1998

(24) Дата начала действия патента: 16.12.2002

(30) Приоритет: 24.02.1998 RU 98103646
20.03.1998 RU 98104851
22.04.1998 RU 98107784

(46) Дата публикации: 15.12.2002

(86) Заявка PCT:
PCT/RU98/00181, 19980619

(72) Изобретатель:
Молдовян Николай Андреевич, RU,
Молдовян Александр Андреевич, RU,
Савлуков Николай Викторович, RU

(73) Патентовладелец:
ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО "МОСКОВСКАЯ ГОРОДСКАЯ ТЕЛЕФОННАЯ СЕТЬ", RU,
Молдовян Николай Андреевич, RU,
Молдовян Александр Андреевич, RU,
Савлуков Николай Викторович, RU

(54) СПОСОБ БЛОЧНОГО КОДИРОВАНИЯ ЦИФРОВЫХ ДАННЫХ

(57) Реферат:

Настоящее изобретение относится к области электросвязи и вычислительной техники. Предлагаемый способ блочного кодирования цифровых данных заключается в том, что формируют ключ кодирования в виде набора подключей, разделяют блок данных на $N \geq 2$ подблоков и осуществляют поочередное преобразование подблоков, выполняя операции преобразования над подблоками и подключами. К отличительным особенностям предлагаемого способа относятся следующие: 1) перед выполнением операции преобразования над i-ми подблоком и подключом выполняют операцию преобразования, которая зависит от j-го подблока, где $j \neq i$; 2) в качестве операции преобразования, которая зависит от j-го подблока, используют операцию перестановки битов подключа, который зависит от j-го подблока; 3) в качестве операции преобразования, которая зависит от j-го подблока, используют операцию циклического сдвига битов подключа, который зависит от j-го подблока; 4) в качестве операции преобразования, которая зависит от j-го подблока, используют операцию подстановки, которая выполняется над подключом в зависимости от j-го подблока.

Официальный бюлетень "Промышленная собственность". Книга 1 "Изобретения, полезные модели, топографии интегральных микросхем", 2002, N 12, 15.12.2002. Государственный департамент интеллектуальной собственности Министерства образования и науки Украины.

UA 51836 C2

UA 51836 C2

(19) UA (11) 51 836 (13) C2

(51) Int. Cl.[7] H 04L 9/00 A

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

STATE DEPARTMENT OF INTELLECTUAL PROPERTY

(12) DESCRIPTION OF PATENT OF UKRAINE FOR INVENTION

(21), (22) Application: 2000095323, 19.06.1998

(24) Effective date for property rights: 16.12.2002

(30) Priority: 24.02.1998 RU 98103646
20.03.1998 RU 98104851
22.04.1998 RU 98107784

(46) Publication date: 15.12.2002

(86) PCT application:
PCT/RU98/00181, 19980619

(72) Inventor:
Moldovian Mykola Andriiovych, RU,
Molovian Oleksandr Andriiovych, RU,
Savlukov Mykola Viktorovych, RU

(73) Proprietor:
OPEN JOINT STOCK COMPANY "MOSCOW MUNICIPAL TELEPHONE NETWORK", RU,
Moldovian Mykola Andriiovych, RU,
Molovian Oleksandr Andriiovych, RU,
Savlukov Mykola Viktorovych, RU

(54) METHOD FOR BLOCK CODING OF DIGITAL DATA

(57) Abstract:

The present invention relates to the communications and computing. The proposed method for block coding of digital data consists in forming a coding key as a set of subkeys, dividing the data block into $N \geq 2$ subblocks, and accomplishing alternating conversion of the blocks by performing conversion operation over the subblocks and subkeys. The proposed method differs in the following features: 1) before performing a conversion operation over the ith subblock and subkey, the conversion operation is performed that depends on the jth subblock, where $j \neq l$; 2) as the conversion operation that depends on the jth subblock, the operation of bit exchange for the key that depends on the jth subblock is used; 3) as the conversion operation that depends on the jth subblock, the operation of bit cyclic shift for the subkey that depends on the jth subblock is used; 4) as the conversion operation that depends on the jth subblock, the operation of substitution is used that is performed over the subkey in dependence on the jth subblock.

Official bulletin "Industrial property". Book 1 "Inventions, utility models, topographies of integrated circuits", 2002, N 12, 15.12.2002. State Department of Intellectual Property of the Ministry of Education and Science of Ukraine.

UA 51836 C2

UA 51836 C2

(19) UA (11) 51 836 (13) C2

(51)МПК 7 H 04L 9/00 A

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

(12) ОПИС ВИНАХОДУ ДО ПАТЕНТУ УКРАЇНИ

(21), (22) Дані стосовно заявки:
2000095323, 19.06.1998

(24) Дата набуття чинності: 16.12.2002

(30) Дані стосовно пріоритету відповідно до Паризької конвенції : 24.02.1998 RU 98103646
20.03.1998 RU 98104851
22.04.1998 RU 98107784

(46) Публікація відомостей про видачу патенту (деклараційного патенту): 15.12.2002

(86) Номер та дата подання міжнародної заявки відповідно до договору PCT:
PCT/RU98/00181, 19980619

(72) Винахідник(и):
Молдовян Алєксандр Андрєєвіч, RU,
Молдовян Ніколай Андрєєвіч, RU,
Савлуков Ніколай Вікторовіч, RU

(73) Власник(и):
ОТКРИТОЄ АКЦІОНЄРНОЄ ОБЩЄСТВО "МОСКОВСКАЯ ГОРОДСКАЯ ТЄЛЄФОННАЯ СЄТЬ", RU,
Молдовян Алєксандр Андрєєвіч, RU,
Молдовян Ніколай Андрєєвіч, RU,
Савлуков Ніколай Вікторовіч, RU

(54) СПОСІБ БЛОЧНОГО ШИФРУВАННЯ ДИСКРЕТНИХ ДАНИХ

(57) Реферат:

Винахід відноситься до галузі електрозв'язку і обчислювальної техніки, а саме, до галузі криптографічних способів та пристроїв для шифрування цифрових даних. Спосіб включає формування ключа шифрування у вигляді сукупності підключів, розбиття блоку даних на $N \geq 2$ підблоків і почергове перетворення підблоків шляхом виконання двомісної операції над підблоком і підключем. Новим у способі, який заявляється, є те, що перед виконанням двомісної операції над і-тим підблоком і підключем над підключем виконують операцію перетворення, яка залежить від j-того підблоку, де $j \neq i$. Новим є також те, що як операцію перетворення, що залежить від j-того підблоку, використовують операцію перестановки бітів підключа, що залежить від j-того підблоку. Крім того, новим є те, що як операцію перетворення, що залежить від j-того підблоку, використовують операцію циклічного зсуву бітів підключа, що залежить від j-того підблоку. Також новим є те, що як операцію перетворення, що залежить від j-того підблоку, використовують операцію підстановки, яка виконується над підключем в залежності від j-того підблоку.

UA 51836 C2

UA 51836 C2

Опис винаходу

Винахід відноситься до галузі електрозв'язку і обчислювальної техніки, а саме, до галузі криптографічних способів та пристроїв для шифрування повідомлень (інформації).

В описі способу, що заявляється, використовуються такі терміни:

секретний ключ - це комбінація бітів, яка відома тільки законному користувачу;

ключ шифрування - це комбінація бітів, яка використовується під час шифрування інформаційних сигналів даних; ключ шифрування є змінним елементом шифру і використовується для перетворення конкретного повідомлення або конкретної сукупності повідомлень; ключ шифрування формується за детермінованими процедурами за секретним ключем; в ряді шифрів як ключ шифрування використовується безпосередньо секретний ключ;

шифр - це сукупність елементарних кроків перетворення вхідних даних з використанням шифрключа; шифр може бути реалізований у вигляді програми для комп'ютера або у вигляді окремого електронного пристрою;

підключ - це частина ключа шифрування, яка використовується під час окремих елементарних кроків шифрування;

шифрування - це процес, який реалізує деякий спосіб перетворення даних з використанням шифрключа, який переводить дані в криптограму, яка являє собою псевдовипадкову послідовність знаків, отримання інформації з якої без знання ключа шифрування є практично неможливим;

дешифрування - це процес, зворотний процедурі шифрування; дешифрування забезпечує відбудову інформації за криптограмою за умови знання ключа шифрування; криптостійкість - це міра надійності захисту зашифрованої інформації і являє собою трудомісткість, що вимірюється кількістю елементарних операцій, які необхідно виконати для відновлення інформації за криптограмою за умови знання алгоритму перетворення, але без знання ключа шифрування.

Відомі способи блочного шифрування даних, див., наприклад, шифр RC5 [R. Rivest, The RC5 Encryption Algorithm, Fast Software Encryption, Second International Workshop Proceedings (Leuven, Belgium, December 14-16, 1994), Lecture Notes in Computer Science, v. 1008, Springer-Verlag, 1995, pp. 86-96]. У відомому способі шифрування блоків даних виконують шляхом формування ключа шифрування у вигляді сукупності підключів, розбиття блоку даних, який перетворюється, на підблоки і зміни їх по черзі за допомогою операції циклічного зсуву, операції підсумовування за модулем 2, які виконуються над двома підблоками, і операції підсумовування за модулем 232, які виконуються над підблоком і підключем. При цьому підключі використовуються за фіксованим розкладом, тобто на цьому кроці виконання бінарної операції між підблоком і підключем значення підключа не залежить від вхідного блоку даних. Цей спосіб блочного шифрування забезпечує високу швидкість шифрування під час реалізації у вигляді програми для комп'ютера.

Однак цьому способу не притаманна достатня стійкість до диференційного і лінійного криптоаналізу [Kalinski B.S., Yin Y.L. On Differential and Linear Cryptanalysis of the RC5 Encryption Algorithm, Advances in Cryptology-CRYPTO'95 Proceedings, Springer-Verlag, 1995, pp. 171-184], що пов'язане з тим, що в цьому способі на заданих кроках шифрування використовуються фіксовані підключі для всіх можливих вхідних блоків.

Найбільш близьким за своєю технічною суттю до способу блочного шифрування є спосіб, який описаний в стандарті США DES [National Bureau of Standards. Data Encryption Standard. Federal Information Processing Standards Publication 46. January 1977]. Цей спосіб шифрування включає формування ключа шифрування у вигляді сукупності 48-бітових підключів, розбиття вхідного блоку дискретних даних на два 32-бітових підблоки L і R і почергове перетворення підблоків під керуванням секретного ключа. Всього виконується 16 раундів перетворення 32-бітового підблоку даних. Кожний раунд перетворення підблоку здійснюється шляхом виконання таких процедур: (1) розширення підблоку R до 48 бітів повторенням деяких бітів цього підблоку: $R \rightarrow R'$, (2) здійснення операції підсумовування за модулем 2 над підблоком і підключем, (3) розбиття підблоку R' на вісім 6-бітових підблоків, (4) виконання операції підстановки над кожним 6-бітовим підблоком шляхом заміни 6-бітових підблоків на 4-бітові підблоки за відомими таблицями підстановки, (5) об'єднання восьми 4-бітових підблоки в 32-бітовий підблок R, (6) здійснення операції перестановки бітів підблоку R за детермінованим законом, (7) здійснення операції підсумовування за модулем 2 підблоку R з підблоком L. Кожний раунд завершується перестановкою підблоків R і L. Під час виконання поточного раунда шифрування використовується фіксований підключ для всіх можливих вхідних блоків даних. Підключі, які використовуються під час перетворення підблоків, формуються під керуванням 56-бітового секретного ключа. Цьому способу блочного шифрування інформації властива висока швидкість перетворень під час реалізації у вигляді спеціалізованих електронних схем.

Однак цей спосіб має недоліки, а саме, в нього низька швидкість шифрування під час програмної реалізації. Крім того, цей спосіб використовує короткий 56-бітовий секретний ключ, що дозволяє на потужних сучасних комп'ютерах розкрити секретний ключ методом підбору можливих значень ключа. Це потребує виконання декількох процедур шифрування, які використовують різні секретні ключі, що робить затрудненим отримання високої швидкості шифрування навіть у разі апаратної реалізації.

В основу винаходу покладене завдання розробити спосіб блочного шифрування дискретних даних, в якому перетворення підблоків даних здійснювалося б таким чином, щоб забезпечувалося зменшення кількості операцій перетворення, які припадають на один біт вхідних даних, одночасно із забезпеченням високої криптостійкості, завдяки чому підвищується швидкість шифрування.

Поставлене завдання вирішується тим, що в способі блочного шифрування дискретних даних, який включає

UA 51836 C2

UA 51836 C2

формування ключа шифрування у вигляді сукупності підключів, розбиття блоку даних на N $\geq$2 підблоків і почергове перетворення підблоків шляхом виконання двомісної операції над підблоком і підключем, новим згідно з винаходом є те, що перед виконанням двомісної операції над і-тим підблоком і підключем над підключем виконують операцію перетворення, що залежить від j-ого підблоку, де j$\neq$1.

Завдяки такому вирішенню структура підключів, які використовуються на завданому кроці шифрування, залежить від даних, які перетворюються, і таким чином на цьому кроці перетворення для різних вхідних блоків використовуються різні модифіковані значення підключів, завдяки чому забезпечується висока стійкість до диференційного криптоаналізу водночас і зменшенням кількості раундів шифрування, що і забезпечує підвищення швидкості криптографічного перетворення.

Новим також є те, що як операцію перетворення, що залежить від j-ого підблоку, використовують операцію перестановки бітів підключа, що залежить від j-ого підблоку.

Завдяки такому вирішенню забезпечується підвищення швидкості шифрування під час реалізації способу, який заявляється, у вигляді електронних пристроїв шифрування.

Новим є також те, що як операцію перетворення, що залежить від j-ого підблоку, використовують операцію циклічного зсуву бітів підключа залежну від j-ого підблоку.

Завдяки такому рішенню забезпечується підвищення швидкості шифрування під час реалізації способу, який заявляється, у вигляді програм шифрування для комп'ютера.

Крім того, новим є те, що як операцію перетворення, що залежить від j-ого підблоку, використовують операцію підстановки, яка виконується над підключем в залежності від j-ого підблоку.

Завдяки такому вирішенню забезпечується додаткове підвищення криптостійкості шифрування водночас із забезпеченням високої швидкості шифрування в разі реалізації способу, який заявляється, у вигляді програм шифрування для комп'ютера.

Нижче суть винаходу, який заявляється, більш докладно роз'яснюється прикладами його здійснення з посиланням на креслення, що додаються.

На фіг.1 наведена узагальнена схема шифрування згідно із способом, який заявляється.

На фіг.2 наведена блок-схема елементарного керованого перемикача, який є базовим елементом блоку керованих перестановок. При u=1 вхідні біти не переставляються, тобто сигнали на виході співпадають з сигналами на вході. При u=0 вхідні біти переставляються.

На фіг.3 наведена таблиця вхідних і вихідних сигналів елементарного керованого перемикача при високому потенціалі керуючого сигналу.

На фіг.4 наведена таблиця вхідних і вихідних сигналів елементарного керованого перемикача при низькому потенціалі керуючого сигналу.

На фіг.5 схематично наведена структура блоку керованих перестановок, який складається з сукупності однотипних блоків - елементарних перемикачів, яка реалізує 2^{79} різних перестановок вхідних бітів в залежності від значення 79-бітового керуючого коду.

На фіг.6 наведена схема спрощеного блоку керованих перестановок.

Винахід пояснюється узагальненою схемою криптографічного перетворення блоків даних на основі способу, що заявляється, яка представлена фіг.1, де: P - блок керованої операції, яка виконується над підключем; A і B - n -бітові підблоки, які перетворюються; K_{2r}, K_{2r-1} - m-бітові підключі (в загальному випадку m$\neq$n); Q(2r), Q(2r-1) - g-бітові додаткові підключі; знак "$\oplus$" позначає операцію порозрядного підсумовування за модулем два; знак "$\otimes$" - операцію підсумовування за модулем 2". Жирні безперервні (суцільні) лінії позначають шину передачі n-бітових сигналів, тонкі пунктирні лінії -передачу одного керуючого біта. Жирні пунктирні лінії - шину передачі n керуючих сигналів, в якості яких використовуються біти перетворюваних підблоків. Жирні пунктирні лінії позначають також шину передачі h бітів додаткових підключів Q(2r) і Q(2r-1), які служать для модифікування операції залежної від перетворюваного підблоку. В окремих випадках додаткові підключі можуть не використовуватися.

Фіг.1 показує один (r-тий) раунд шифрування. В залежності від конкретного вигляду керованої операції, яка використовується, і потрібної швидкості перетворень можуть бути задано від 6 до 10 і більше раундів. Один раунд перетворень полягає в виконанні такої послідовності процедур:

(1) перетворення підключа K_{2r} в залежності від значень підблоку A і від значень додаткового підключа Q(2r), в результаті чого на виході блоку P_1 виробляється перетворене значення підключа $P_{A,Q(2r)}(K_{2r})$;

(2) перетворення підблоку B шляхом виконання операції порозрядного підсумовування за модулем 2 над значенням $P_{A,Q(2r)}(K_{2r})$ 1 підблоком B: B: =B$\oplus$ $P_{A,Q(2r)}(K_{2r})$, де знак ":=" позначає операцію присвоювання;

(3) перетворення підблоку A шляхом виконання операції підсумовування за модулем 2^n над підблоком A і підблоком B: A:=A $\otimes$ B;

(4) перетворення підключа K_{2r-1} в залежності від значення підблоку B і від значення додаткового підключа Q(2r-1), в результаті чого на виході блоку P_2 виробляється значення $P_{A,Q(2r-1)}(K_{2r-1})$;

(5) перетворення підблоку A:

A:-A$\oplus P_{A,Q(2r-1)}(K_{2r-1})$;

(6) перетворення підблоку B:

B:=B $\otimes$ A.

В залежності від конкретного варіанту реалізації способу блочного шифрування дискретної інформації, який пропонується, одна й та ж пара m-бітових підключів K_2 і K_1 (додаткових g-бітових підключів Q(2) і Q(1)) може використовуватись під час виконання кожного раунду шифрування. Можливий варіант, коли в кожному раунді

UA 51836 C2

UA 51836 C2

використовуються незалежні підключі K_{2r}, K_{2r-1} (незалежні додаткові підключі Q(2r) і Q(2r-1)). Наприклад, при кількості раундів r=3 в першому раунді використовуються підключі K_2 і KI (Q(2) і Q(1)), у другому раунді - підключі K_4 і K_3 (Q(4) і Q(3)), в третьому раунді - підключі K_6 і K_5 (Q(6) і Q(5)). Підключі K_{2r}, K_{2r-1} і додаткові підключі Q(2r), Q(2r-1) можуть формуватися за спеціальними процедурами залежно від секретного ключа. Можливий варіант, в якому підключі K_{2r}, K_{2r-1} і додаткові підключі Q(2r), Q(2r-1) формуються шляхом генерації за законом ймовірності..

Можливість технічної реалізації способу, що заявляється, пояснюється далі конкретними прикладами його здійснення.

Приклад 1.

В цьому прикладі пояснюється шифрування 64-бітових блоків даних з використанням керованих перестановок як операції, яка виконується над підключем в залежності від одного з перетворюваних блоків. Ключ шифрування формується у вигляді 16 підключів $K_1,K_2,K_3,.....K_{16}$, кожен із яких має довжину 32 біти. Додаткові підключі не використовуються. Вхідний блок даних розбивається на два 32-бітових підблоки A і B. Шифрування вхідного блоку описується таким алгоримом:

1. Установити лічильник кількості раундів:

r:=1.

2. Перетворити підблок B відповідно до виразу:

$B:=B\oplus P_A(K_{2r})$,

де $P_A(K_{2r})$ позначає операцію перестановки бітів підключа K_{2r}, яка виконується залежно від значення підблоку A.

3. Перетворити підблок A відповідно до виразу:

$A:=A \otimes B$.

4. Перетворити підблок A відповідно до виразу:

$A:=A\oplus P_B(K_{2r-1})$,

де $Pв(K_{2r-1})$ позначає операцію перестановки бітів підключа K_{2r-1}, яка виконується залежно від значення підблоку B.

5. Перетворити підблок B відповіді о до виразу:

$B:-B \otimes A$.

6. Якщо $r\neq 8$, то приростити лічильник r:=r+1 і перейти до кроку 2, в противному разі СТОП.

Цей алгоритм зорієнтований на реалізацію у вигляді електронних схем. Операції перестановки бітів підключа, що залежать від одного з підблоків, які перетворюються, можуть бути виконані за допомогою блоку керованих перестановок, реалізованого на основі використання сукупності елементарних перемикачів, які виконують операцію перестановки двох бітів.

Фіг.2 пояснює роботу елементарного перемикача, де u - керуючий сигнал, a і b - вхідні сигнали даних, c і d - вихідні сигнаги даних.

Таблиці на фіг.3 і 4 показують залежність вихідних сигналів від вхідних і керуючих сигналів. Із наведених таблиць видно, що коли u=1, лінія a комутується з лінією c, а лінія b - з лінією d. Коли u=0, лінія a комутується з лінією d, а лінія b – з лінією d. Таким чином, під час одиничного керуючого сигналу перестановка двох вхідних бітів не здійснюється, а під час нульового керуючого сигналу вхідні біти переставляються.

На фіг.5 показана можлива реалізація блоку керованих перестановок, яка використовує сукупність елементарних перемикачів S. Цей приклад відповідає блоку P із 32-бітовим інформаційним входом і 79-бітовим керуючим входом. Як інформаційні сигнали використовуються біти поточного перетворюваного підключа. Як керуючі сигнали використовуються 32 біти одного з підблоків і 47 бітів одного з додаткових підключів.

Кількість різних варіантів операції перестановки дорівнює кількості можливих кодових комбінацій на вході керування і дорівнює 2^{79} для блока P із структурою, показаною на фіг.2. Цей блок керованих перестановок реалізує унікальну перестановку вхідних бінарних розрядів для кожного можливого значення кодової комбінації на керуючому вході, кількість яких дорівнює 2^{79}. Зовнішні інформаційні входи блоку керованих перестановок позначені i1,i2,...,i32, зовнішні виходи позначені c1,c2,...,c32, керуючі входи позначені c1,c2,...,c79. Елементарні перемикачі S з'єднані таким чином, що вони утворюють матрицю, яка складається з 31 рядка. В першому рядку з'єднані 31 елементарний перемикач S, у другому рядку - 30, в третьому - 29 і т.д. В кожному наступному рядку кількість елементарних перемикачів зменшується на 1. В крайньому нижньому 31 -ому рядку з'єднаний 1 елементарний перемикач.

Рядок з номером $j\neq 31$ має 33-j входів, 33-j виходів і 32-j керуючих входи. Останній (крайній правий) вихід j-ого рядка є зовнішнім виходом блоку керованих перестановок, решта 32-j виходи j-рядка з'єднані з відповідними входами (j+1)-ого рядка. Останній 31-й рядок має два виходи і обидва з них є зовнішніми виходами блоку керованих перестановок. Не більше, ніж на один керований вхід кожного рядка подається одиничний (u=1) керуючий сигнал. Для забезпечення цієї вимоги служать бінарно-тридцятидвохрядш дешифратори $F_1,F_2,...,P_{15}$ і бінарно-шістнадцятирядний дешифратор F_{16}. Дешифратори $F_1,F_2,...,F_{15}$ мають п'ять зовнішніх керуючих входів, на які подається довільний 5-бітовий бінарний код, і 32 виходи. Ці дешифратори виробляють тільки на одному виході одиничний сигнал. На 31 виході, які залишаються, встановлюється нульовий сигнал. Дешифратор F_{16} має 4 входи, на які подається довільний 4-бітовий бінарний код, і 16 виходів, з яких тільки на одному встановлюється одиничний сигнал. Для всіх дешифраторів $F_1,F_2,...,F_{15}$ і F_{16} кожне вхідне значення бінарного коду задає лише один можливий номер виходу, на якому встановлюється одиничний сигнал (u=1).

UA 51836 C2

UA 51836 C2

Частина виходів дешифратора F_h, де $h \le 15$, з'єднані з керуючими входами рядка з номером h (32-h виходів), а частина виходів - з керуючими входами (32-h) - го рядка (h виходів). Таким чином, в кожному рядку тільки на одному елементарному перемикачу встановлюється керуючий сигнал (u=1). Вхід рядка, приєднаний до правого входу елементарного перемикача, на який поданий одиничний керуючий сигнал, комутується з зовнішнім виходом блоку керованих перестановок, що відповідає цьому рядку. Якщо одиничний керуючий сигнал поданий на крайній лівий елементарний перемикач, то з зовнішнім виходом блоку керованих перестановок (блок P) комутується крайній лівий вхід рядка. Перший рядок комутує один із зовнішніх входів i1,i2, i32 блоку P з зовнішнім виходом o1, а решта 31 зовнішній вхід - з входами другого рядка. Другий рядок комутує один із решти 31 зовнішнього входу з зовнішнім виходом o2, а решта 30 зовнішніх входів - з входами 3-тього рядка і т.д. Така структура блоку P реалізує унікальну перестановку вхідних бітів для кожного значення бінарного кода, який поданий на 79-бітовий керуючий вхід блоку P.

Можливий такий варіант використання блоку керуючих перестановок P з 32-бітовим інформаційним входом і 79-бітовим керуючим входом. Як керуючі сигнали, які подаються на 79-бітовий керуючий вхід блоку керуючих перестановок P, можуть використовуватися 32 біти підблоку A і 47 бітів додаткового 47-бітового підключа Q(2r). В цьому випадку в залежності від 47-бітового додаткового підключа формується одна з 2^{47} різних модифікацій операції перестановки бітів, залежної від значення вхідного блоку. При цьому кожна модифікація цієї операції включає 2^{32} різних операцій перестановки бітів підключа K_{2r}, причому вибір конкретної операції перестановки визначається значенням підблоку A. Вибір модифікації не є визначеним заздалегідь, оскільки він визначається додатковим підключем Q(2r), який є безпосередньо елементом секретного ключа або залежать від секретного ключа. Це додатково підвищує стійкість криптографічного перетворення. Якщо в пристрої шифрування використовуються два блоки P, які мають структуру, показану на фіг.2, то кількість можливих комбінацій модифікацій операції перестановок, які встановлюються на блоках P залежно від додаткових 47-бітових підключів, може бути задано до $(2^{47})^2=2^{94}$ під час використання секретного ключа довжиною 94 біта.

Завдяки простій структурі блоків P, сучасна технологія виготовлення інтегральних схем дозволяє легко виготовити криптографічні мікропроцесори, які мають керовані блоки перестановок із розміром входу 32 і 64 біти і які забезпечують швидкість шифрування до 1Гбіт/с і вище.

На фіг.6, де тонкі суцільні лінії позначають передачу одного біта підключа, показана можлива реалізація блоку керованих перестановок, яка використовує сукупність елементарних перемикачів S. Цей приклад блоку керованих перестановок відповідає блоку керованих перестановок з 8-бітовим входом для інформаційних сигналів (бітів підключа) і 8-бітовим входом для керуючих сигналів (бітів підблоку даних, які позначені пунктирними лініями аналогічно позначенню на фіг.1). Аналогічно може бути побудований довільний блок керованих перестановок, наприклад такий, який має 64-бітовий вхід для інформаційних сигналів і 128-бітовий вхід для керуючих сигналів. При використанні блоку керованих перестановок з 32-бітовим інформаційним входом кількість різних перестановок дорівнює 2^{32}. Це означає, що під час шифрування двох різних блоків даних ймовірність повторення деякої перестановки на заданому кроці дорівнює 2^{-32}, а повторення перестановок на z заданих кроках дорівнює 2^{-32z}. Таким чином, набір модифікованих значень підключів, які використовуються для перетворення кожного вхідного повідомлення, практично є унікальним, що забезпечує високу криптостійкість шифрування.

Використовуючи спрощену структуру блоку керованих перестановок, яка схематично представлена на фіг.6, легко здійснити виготовлення криптографічних мікропроцесорів, які мають блоки керованих перестановок із розміром входу до 128 бітів. Використання операції керованих перестановок над 128-бітовими підключами дозволяє отримати більш високу криптостійкість шифрування. Блок керованих перестановок являє собою комбінаційну електричну схему, що забезпечує високу швидкість виконання керованих перестановок.

Приклад 2.

Цей приклад пояснює використання операції циклічного зсуву, яка залежить від перетворюваних підблоків і виконується над підключами. Ключ шифрування формується у вигляді 16 підключів $K_1, K_2, K_3, ..., K_{32}$, кожен із яких має довжину 32 біти. Вхідний 64-бітовий блок даних розбивається на два 32-бітових підблоки A і B. Шифрування вхідного блоку описується таким алгоритмом:

1. Установити лічильник кількості раундів: r=1.

2. Перетворити підблок B відповідно до виразу: B:=B $\oplus$ (K2r<<<A), де K2r<<<A позначає операцію циклічного зсуву вліво на A бітів, яка виконується над підключем K_{2r}.

3. Перетворити підблок A відповідно до виразу:

A:=A $\otimes$ B, де "$\otimes$" - операція підсумовування за модулем 2^{32}.

4. Перетворити підблок A відповідно до виразу:

A:=A $\oplus$ ($K_{2r-1<<<}$B), де $K_{2r-1<<<}$B позначає операцію циклічного зсуву вліво на B бітів, яка виконується над підключем K_{2r-1}.

5. Перетворити підблок B відповідно до виразу:

B:=B $\otimes$ A.

6. Якщо r≠16, то приростити лічильник r:=r+1 і перейти до кроку 2, в противному разі СТОП.

Схема одного раунда перетворень пояснюється на фіг.1. Блоки P_1 і P_2 в цьому прикладі - являють собою операційний блок, який виконує операцію циклічного зсуву бітів відповідних підключів в залежності від перетворюваних підблоків. Цей алгоритм орієнтований на реалізацію у вигляді програми для комп'ютерів. Сучасні мікропроцесори швидко здійснюють операцію циклічного зсуву в залежності від значення змінної, яка

UA 51836 C2

UA 51836 C2

зберігається в одному з регістрів. Завдяки цьому описаний алгоритм під час програмної реалізації забезпечує швидкість шифрування близько 40Мбіт/с для масового мікропроцесора Pentium/200. За умови завдання 10 раундів шифрування досягається швидкість близько 60Мбіт/с.

Приклад 3.

Цей приклад пояснює використання операції підстановки, яка залежить від перетворюваних блоків і виконується над підключами. Для цього прикладу блоки P_1 і P_2 являють собою операційний блок, який виконує операцію підстановки в залежності від відповідних підблоків. Під операцією підстановки мається на увазі операція заміни бінарного значення сигналу на вході операційного блоку P на інше бінарне значення (що встановлюється на вході операційного блоку P), яке вибирається в залежності від значення на вході блоку P відповідно додеякої таблиці заміни. Можуть бути реалізовані два варіанти підстановок:

(1) n-бітовий вхідний бінарний вектор замінюється на n-бітовий вихідний бінарний вектор, причому різним вхідним бінарним векторам відповідають різні вихідні бінарні вектори;

(2) m-бітовий бінарний вектор замінюється на n-бітовий бінарний вектор, де $n \geq m$, причому різним бінарним векторам можуть відповідати як різні, так і однакові вихідні бінарні вектори.

Пояснимо задания залежності операції підстановки першого типу від підблоку перетворюваних даних. Нехай операції підстановки виконуються над бінарними векторами довжиною n бітів, де n - ціле число. Тоді для визначення операції підстановки розміром nxn (позначення nxn означає, що вхідним для операції підстановки є бінарний вектор довжиною n бітів і вихідний бінарний вектор також має довжину n бітів) потрібно використання таблиці, яка має два рядки чисел:

0 1 2 3 ... N-1

α_0 α_1 α_2 α_3 ... α_{N-1}

де $N=2^n$ В цій таблиці в нижньому рядку присутні всі можливі значення n-бітового блоку рівно по одному разу, але в довільному порядку. Черговість розташування чисел в нижньому рядку визначає конкретний варіант таблиці підстановки, а отже і конкретний варіант операції підстановки, яка виконується з використанням цієї таблиці. Виконання операції підстановки здійснюється таким чином. Вибирається з верхнього рядка число, яке дорівнює значенню вхідного блока. Значення, яке знаходиться під цим числом у нижньому рядку, береться як вихідний блок. Таким чином, таблицю підстановки можна розташувати в оперативній пам'яті комп'ютера як послідовний запис n-бітових комп'ютерних слів, розміщених в комірках з адресами $W_0,W_1,W_2,...,W_{N-1}$. В цьому випадку значення вхідного бінарного вектора Y служить для обчислення адреси W_0+Y слова, яке беруть як вихідний бінарний вектор. Цей спосіб подання таблиці підстановки потребує використання об'єму пам'яті, який дорівнює $Nn=2^n n$ бітам. Виберемо кількість таблиць підстановки, яка дорівнює 2^L (об'єм потрібної пам'яті буде при цьому дорівнювати $2^L Nn$ бітам) і розташуємо таблиці підстановок безперервно одна за одною. За адресу таблиці з номером V візьмемо значення адреси Wo її першого n-бітового слова. Нехай адреса таблиці з номером V=0 є S. В цьому випадку адреса таблиці підстановки з будь-яким номером V дорівнює S+vN. Коли задано керуючий бінарний вектор, який визначає номер поточної таблиці підстановки v і поточний вхідний бінарний вектор, то операція підстановки виконується заміною поточного вхідного блоку на n-бітове слово, розташоване за адресою S+vN+Y, де Y - значення вхідного бінарного вектора, над яким виконується поточна операція підстановки. Використовуючи це співвідношення легко задати вибір таблиці підстановки з номером v і виконати підстановку над вхідним бінарним вектором із значенням Y. У випадку, який розглядався, задания залежності таблиць підстановки від значення керуючого бінарного вектора і виконання операції підстановки здійснюється мікропроцесором дуже швидко під час вибору відповідних значень параметрів L і n, наприклад при L=5 і n=8. При зазначених параметрах для розміщення таблиць підстановки потрібно 8 Кбайт оперативної пам'яті, що є прийнятним, оскільки сучасні комп'ютери мають об'єм оперативної пам'яті на багато порядків більше цієї величини (від 1 до 64Мбайт і більше).

Пояснимо задания залежності операції підстановки другого типу від підблоку даних на прикладі підстановок 16x32, які задаються за допомогою пронумерованої послідовності 32-бітових бінарних векторів X_j, $j=0,1,2,...,2^{16}-1$. Передбачається, що послідовність X_j є відомою і належить до опису алгоритму шифрування. Операція підстановки над 16-бітовим підключем k здійснюється в залежності від перетворюваного підблоку b таким чином:

(1) обчислюється номер $j=(b+k) \bmod 2^{16}$;

(2) 16-бітовий бінарний вектор k замінюється на 32-бітовий бінарний вектор X_j Шифрування 64-бітових блоків даних на основі операцій підстановки, які виконуються за допомогою послідовності 32-бітових бінарних векторів Xj ($j=0,1,2,...,2^{16}-1$) над підключами в залежності від перетворюваних підблоків даних, може бути здійснено, наприклад, таким чином. Ключ шифрування формується у вигляді 16 підключів $K_1,K_2,K_3,...,K_{32}$, кожен із яких має довжину 16 бітів. Вхідний блок даних розбивається на два 32-бітових підблоки $A=a_2|a_1$ і $B=b_2|b_1$, які представлені у вигляді конкатенації 16-бітових підблоків a_1,a_2 і b_1,b_2. Шифрування вхідного блоку описується таким алгоритмом:

1. Установити лічильник кількості раундів r=1.

2. Перетворити підблок B відповідно до виразу:

$B:=B \oplus F(K_{4r}, a_1)$,

де $F(K_{4r}, a_1)$ позначає операцію підстановки над підключем K_{4r}, що залежить від підблоку a_1.

3. Перетворити підблок A відповідно до виразу:

UA 51836 C2

UA 51836 C2

A:=A+B(mod 2^{32}).

4. Перетворити підблок A відповідно до виразу:

A:=A $\oplus$ F(K_{4r-1},b_1),

де F(K_{4r-1}, b_1) позначає операцію підстановки над підключем K_{4r-1} яка виконується в залежності від підблоку b_1.

5. Перетворити підблок B відповідно до виразу:

B:=B+A(mod2^{32}).

6. Перетворити підблок B відповідно до виразу:

B:=B $\oplus$ F(K_{4r-2}, a_2).

7. Перетворити підблок A відповідно до виразу:

A:=A+B(mod2^{32}).

8. Перетворити блок A відповідно до виразу:

A:=A $\oplus$ F(K_{4r-2}, b_2).

9. Перетворити підблок B відповідно до виразу:

B:=B+A(mod2^{32}).

10. Якщо $r \neq 4$, то приростити лічильник r:=r+1 і перейти до кроку 2, в противному разі СТОП.

Цей алгоритм використовує відому таблицю підстановки розміром 240Кбайт, що складає малу частину об'єму оперативної пам'яті сучасних комп'ютерів. Операція добування бінарних векторів із оперативної пам'яті за заданими адресами здійснюється малою кількістю машинних тактів, завдяки чому програмна реалізація способу блочного шифрування, який пропонується, з операціями підстановки, які виконуються над підключами в залежності від перетворюваних підблоків, забезпечує швидкість шифрування від 20 до 60Мбіт/с (в залежності від конкретної реалізації) для масового мікропроцесора Pentium/200.

Промислова придатність

Наведені приклади показують, що заявлений спосіб блочного шифрування дискретних даних є таким, що технічно реалізується, і дозволяє вирішити поставлене завдання.

Розглянуті приклади легко реалізуються, наприклад, в спеціалізованих мікроелектронних схемах шифрування (приклад 1) і у вигляді програм шифрування для комп'ютерів (приклади 2 і 3) і забезпечують швидкість шифрування до 1Гбіт/с і вище (приклад 1) під час апаратної реалізації і до 60Мбіт/с під час програмної реалізації і використання масового мікропроцесора Pentium/200 (приклади 2 і 3).

Формула винаходу

1. Спосіб блочного шифрування дискретних даних, який включає формування ключа шифрування у вигляді сукупності підключів, розбиття блоку даних на $N \geq 2$ підблоків і почергове перетворення підблоків шляхом виконання двомісної операції над підблоком і підключем, який **відрізняється** тим, що перед виконанням двомісної операції над i-тим підблоком і підключем над підключем виконують операцію перетворення, яка залежить від j-того підблоку, де $j \neq i$.

2. Спосіб за п. 1, який **відрізняється** тим, що як операцію перетворення, що залежить від j-того підблоку, використовують операцію перестановки бітів підключа, що залежить від j-того підблоку.

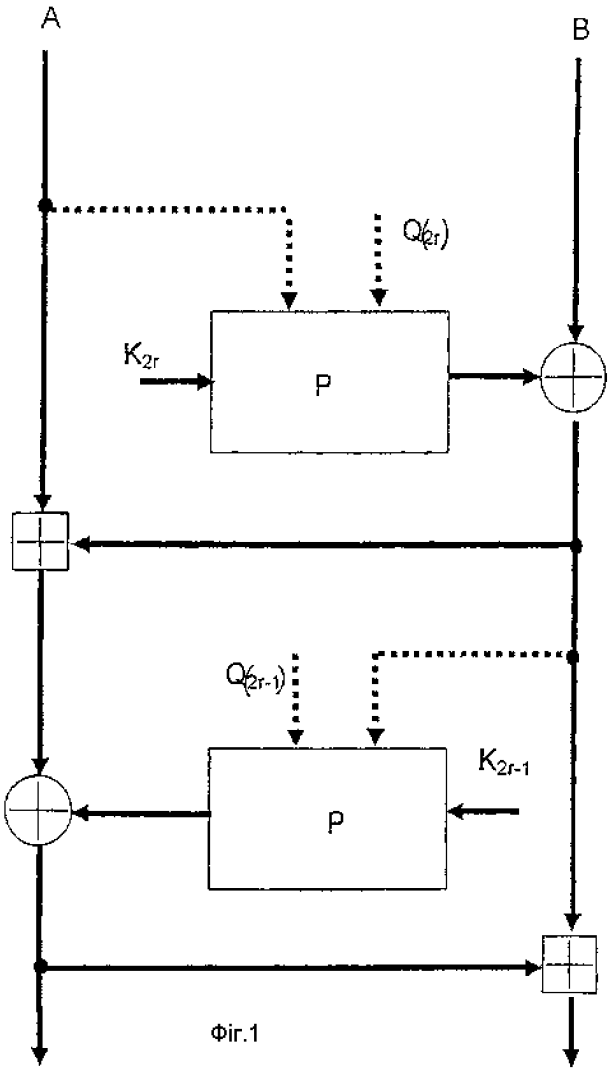
3. Спосіб за п. 1, який **відрізняється** тим, що як операцію перетворення, що залежить від j-того підблоку, використовують операцію циклічного зсуву бітів підключа, що залежить від j-того підблоку.

4. Спосіб за п. 1, який **відрізняється** тим, що як операцію перетворення, що залежить від j-того підблоку, використовують операцію підстановки, яка виконується над підключем в залежності від j-того підблоку.

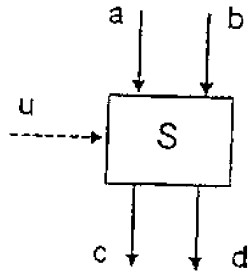
Офіційний бюлетень "Промислоава власність". Книга 1 "Винаходи, корисні моделі, топографії інтегральних мікросхем", 2002, N 12, 15.12.2002. Державний департамент інтелектуальної власності Міністерства освіти і науки України.

UA 51836 C2

UA 51836 C2



Фіг.1



Фіг.2

u=1

ВХІД		ВИХІД	
a	b	c	d
1	0	1	0
0	1	0	1
0	0	0	0
1	1	1	1

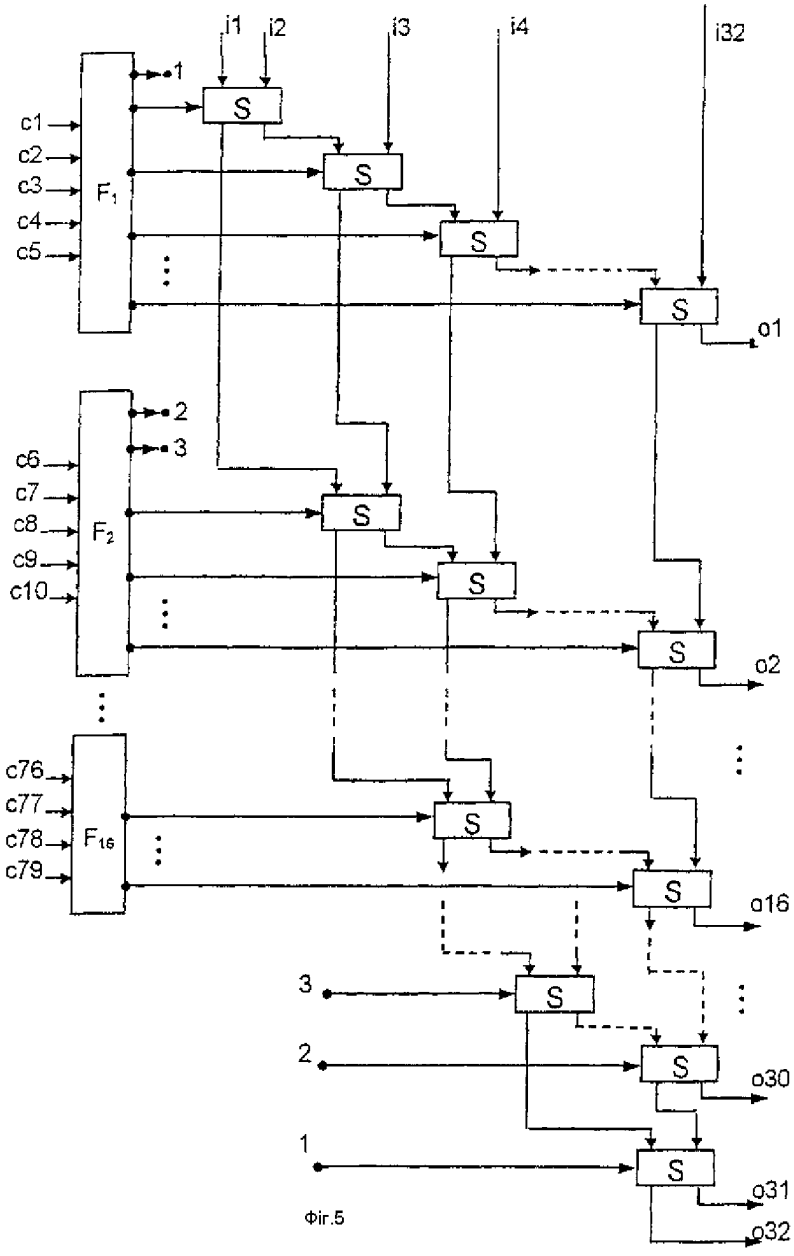
Фіг.3

UA 51836 C2

u=0

ВХІД		ВИХІД	
a	b	c	d
0	1	1	0
1	0	0	1
0	0	0	0
1	1	1	1

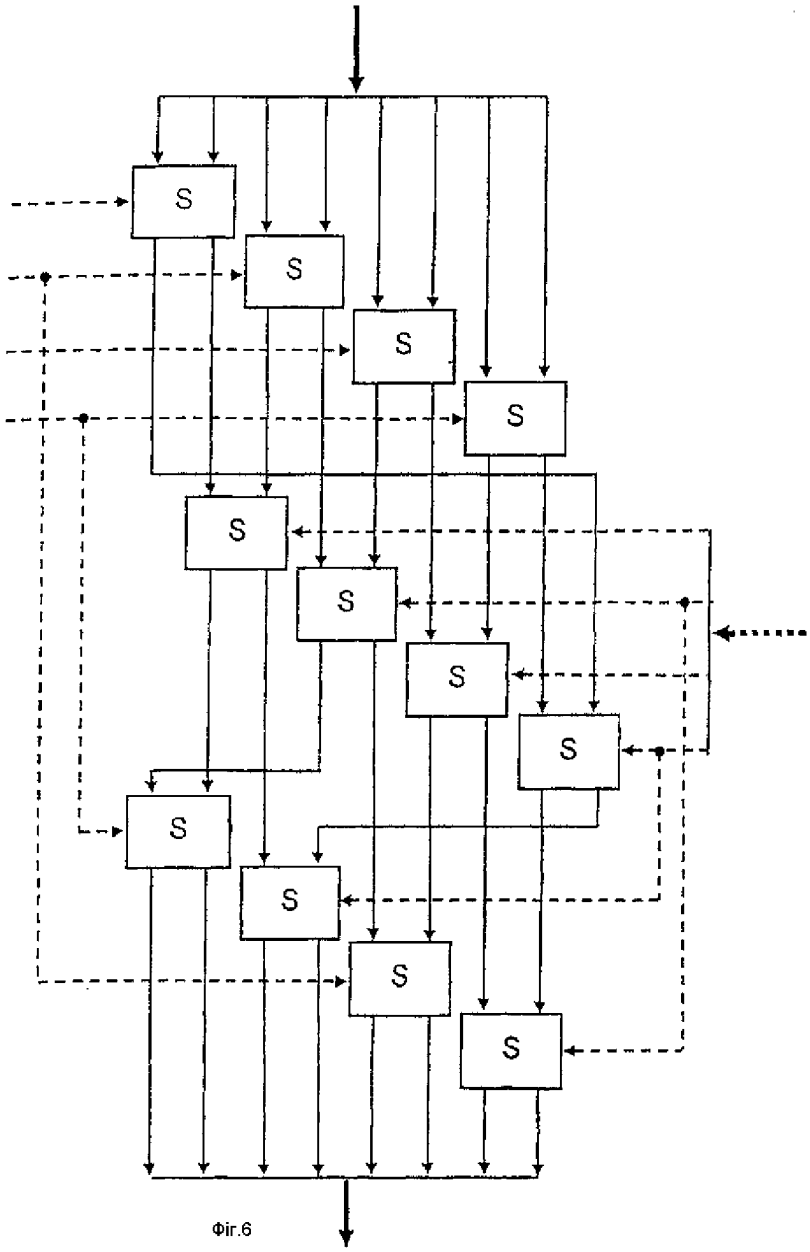
Фіг.4



Фіг.5

UA 51836 C2

UA 51836 C2



Фіг.6

UA 51836 C2

UA 51836 C2