

Міністерство освіти і науки України  
Вінницький національний технічний університет

**О. М. Бевз, Р. Н. Квстний**

**ШИФРУВАННЯ ДАНИХ  
НА ОСНОВІ ВИСОКОНЕЛІНІЙНИХ  
БУЛЕВИХ ФУНКЦІЙ ТА КОДІВ  
З МАКСИМАЛЬНОЮ ВІДСТАННЮ**

**Монографія**

Вінниця  
ВНТУ  
2010

УДК 681.3.06  
ББК 22.19  
Б 32

Рекомендовано до друку Вченою радою Вінницького національного технічного університету Міністерства освіти і науки України (протокол № 5 від 29.12.2008 р.)

*Рецензенти:*

**В. А. Лужецький**, доктор технічних наук, професор

**І. І. Хаймзон**, доктор технічних наук, професор

**Бевз, О. М.**

Б 32 Шифрування даних на основі високонелінійних булевих функцій та кодів з максимальною відстанню : монографія / О. М. Бевз, Р. Н. Кветний — Вінниця : ВНТУ, 2010. — 96 с.

ISBN 978-966-641-340-9

У монографії розроблено методи та алгоритми шифрування на основі високонелінійних булевих функцій та кодів з максимальною відстанню. Основу монографії склали результати досліджень в рамках кандидатської дисертації О. М. Бевза, що були виконані на кафедрі автоматики та інформаційно-вимірювальної техніки Вінницького національного технічного університету за участю та під керівництвом доктора технічних наук, професора Р. Н. Кветного.

**УДК 681.3.06**  
**ББК 22.19**

**ISBN 978-966-641-340-9**

© О. Бевз, Р. Кветний, 2010

## ЗМІСТ

ВСТУП.....	5
<b>РОЗДІЛ 1</b>	
<b>СУЧАСНІ КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ.....</b>	<b>6</b>
1.1. Класифікація криптографічних методів захисту інформації в комп'ютерних системах та мережах.....	6
1.2. Методи формування блочних шифрів.....	9
1.2.1. Формування розсіювання методом мережі Фейстеля.....	10
1.2.2. Формування розсіювання методом підстановочно- перестановочної мережі.....	13
1.3. Методи формування перемішування.....	17
1.4. Криптоаналітичні властивості симетричних шифрів.....	19
1.5. Криптографічні властивості нелінійних булевих функцій.....	23
1.6. Основні операції блочних шифрів.....	25
1.7. Виконання основних операцій блочних шифрів в процесорах комп'ютерних систем.....	28
1.8. Обґрунтування напрямку дослідження.....	31
<b>РОЗДІЛ 2</b>	
<b>ФОРМУВАННЯ ЛІНІЙНОГО ПЕРЕТВОРЕННЯ.....</b>	<b>32</b>
2.1. Дослідження лінійних та диференціальних властивостей лінійного перетворення.....	32
2.2. Визначення криптографічної стійкості лінійного перетворення на основі коду з максимальною відстанню.....	38
2.3. Визначення типу коду з максимальною відстанню для ефективної реалізації в комп'ютерних системах.....	44
<b>РОЗДІЛ 3</b>	
<b>ФОРМУВАННЯ БЛОКУ</b>	
<b>ПІДСТАНОВКИ ТА ПОТОКОВОГО ШИФРУ.....</b>	<b>52</b>
3.1. Формування восьмикоординатної високонелінійної збалансованої булевої функції для використання в S-боксах.....	52
3.1.1. Формування семикоординатної високонелінійної збалансованої булевої функції.....	53
3.1.2. Формування восьмикоординатної булевої функції та S-боксу.....	55
3.2. Оцінювання показника протидії S-боксу лінійному криптоаналізу.....	59
3.3. Диференціальні властивості S-боксу.....	61

3.4. Визначення стійкості раундових перетворень блочного шифру на основі запропонованої функції та коду з максимальною відстанню.....	62
3.5. Метод формування потокового шифру.....	63

## **РОЗДІЛ 4**

### **ПРАКТИЧНА РЕАЛІЗАЦІЯ МЕТОДІВ ШИФРУВАННЯ У КОМП'ЮТЕРНИХ СИСТЕМАХ.....**

4.1. Алгоритми для реалізації методів шифрування.....	69
4.2. Алгоритм для реалізації методу формування лінійного перетворення низького рівня.....	70
4.3. Алгоритм для реалізації методу формування нелінійного перетворення на основі прямого комп'ютерного обчислення.....	77
4.4. Алгоритм для реалізації методу формування нелінійного перетворення на основі табличних підстановок.....	79
4.5. Алгоритм для реалізації методу формування лінійного перетворення високого рівня.....	80
4.6. Методика захисту інформації на основі блочного шифру в комп'ютерних системах та мережах.....	82
4.7. Впровадження програми шифрування в автоматизовану службу обробки викликів.....	83
4.8. Впровадження програми шифрування в систему передавання інформації каналами зв'язку колективного користування АКБ «АВАЛЬ».....	86
4.9. Експериментальні дослідження.....	88

<b>ВИСНОВКИ.....</b>	<b>90</b>
----------------------	-----------

<b>ЛІТЕРАТУРА.....</b>	<b>91</b>
------------------------	-----------

## ВСТУП

**Актуальність теми.** Сучасні технології комп'ютерних систем та мереж дають розвиток широкому діапазону нових інформаційних сервісів та служб. В недалекому майбутньому передбачається, що ці служби будуть інтегровані в багатофункціональні обчислювальні мережі. Захист інформації від несанкціонованого доступу – одна з головних задач по забезпеченню конфіденційності, цілісності та автентичності даних, що передаються. Біля одного мільярда людей з'єднано за допомогою комп'ютерних систем та мереж в глобальну мережу Internet. Багато програмних додатків– електронна пошта, електронні банки, електронна комерція – вимагають обміну приватною інформацією. Для прикладу, в електронній комерції, коли покупець придбає різноманітні речі продавець вимагає номер кредитної карти. Якщо даний канал передавання інформації не закритий, зловмисники можуть легко отримати конфіденційні дані. Для того щоб це унеможливити, канали передавання інформації між віддаленими комп'ютерними системами повинні мати інформаційний захист.

Головним та важливим засобом для забезпечення захисту вищенаведених служб та додатків є криптографічні алгоритми. Сучасний термін «криптографія» означає сукупність математичних та логічних засобів для забезпечення інформаційного захисту комп'ютерних систем та мереж. Криптографічна технологія призначена для захисту логічного рівня фізичних каналів комп'ютерних мереж. З іншого боку, криптоаналіз забезпечує визначення технічної та математичної слабкості криптографічних алгоритмів. Класи криптографічних алгоритмів та криптоаналітичних атак наведені в [1].

Формування високопродуктивних схем та алгоритмів шифрування/дешифрування з високою криптографічною стійкістю є важливим етапом в проектуванні інформаційно-захисених високошвидкісних комп'ютерних мереж [2].

Багато додатків вимагають створення комп'ютерних мереж з інформаційним захистом при застосуванні відкритих ліній зв'язку. Ці обчислювальні системи відомі як Віртуальні Приватні Мережі (Virtual Private Networks - VPNs). VPN вимагають шифрування на швидкості, що перевищує швидкість асинхронного режиму передавання – більше за 1 Гбіт/с. Тому необхідно розробляти методи та алгоритми шифрування з високою криптологічною стійкістю, які працюють в комп'ютерних системах та мережах та мають швидкість роботи понад 1 Гбіт/с.

У монографії розроблено методи та алгоритми шифрування на основі високонелінійних булевих функцій та кодів з максимальною відстанню. Основу монографії склали результати досліджень в рамках кандидатської дисертації О. М. Бевза, що були виконані на кафедрі автоматики та інформаційно-виміральної техніки за участю та під керівництвом доктора технічних наук, професора Р. Н. Кветного.

# РОЗДІЛ 1

## СУЧАСНІ КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

### 1.1. Класифікація криптографічних методів захисту інформації в комп'ютерних системах та мережах

В теперешній час великий обсяг конфіденційної інформації передається між комп'ютерними системами звичайними лініями зв'язку. Комп'ютерні системи і мережі – один з найвразливіших компонентів сучасних організацій та банківських установ. Тому постає нагальна потреба здійснювати захист інформації в комп'ютерних системах та мережах від несанкціонованого доступу.

Передавання інформації в комп'ютерних мережах зумовлюють такі головні види загроз безпеки мережевої взаємодії: перехоплення даних, які передають мережею, з метою викрадення, модифікування чи переадресування, несанкціоноване відсилання даних від імені іншого користувача, заперечення користувачами автентичності даних і фактів відсилання-отримання інформації. Одним із можливих способів усунення загроз інформаційної безпеки є використання криптографічних перетворень [3].

Реалізація повного та комплексного захисту інформації в комп'ютерних системах та мережах повинна задовольняти три криптографічні вимоги: конфіденційність, автентичність та цілісність даних.

Конфіденційність – це властивість інформації бути відомою лише допущеним та тим суб'єктам, хто пройшов перевірку. Для інших суб'єктів інформація є закритою.

Автентичність – процес підтвердження ідентичності. Система чи об'єкт повинні знати, що отримана інформація надішла від дійсного джерела повідомлення.

Цілісність даних – властивість даних не змінюватися, при функціонуванні системи.

Для задовільнення цих трьох вимог в сучасних комп'ютерних системах та мережах існують три основні криптографічні системи захисту інформації – шифрування з закритими ключами, шифрування з відкритими ключами та хеш-функції.

Шифри забезпечують конфіденційність шляхом перетворення даних в повідомлення, яке важко зрозуміти. На вхід шифру надходить відкритий текст (плантекст), а на виході отримується шифротекст. В шифрі відкритий текст перетворюється в шифротекст із застосуванням ключа шифрування. В алгоритмі дешифрування шифротекст

перетворюється в відкритий текст зворотним чином. Сукупність процесів шифрування та дешифрування мають назву шифри. В ідеальному випадку без наявності ключа відсутня можливість перетворити шифротекст на відкритий текст. В реальному випадку потужні криптографічні алгоритми значним чином ускладнюють відкриття відкритого тексту з шифротексту за відсутності ключа. Тому спроби зламу шифру за відсутності ключа, шляхом перебору, займають дуже багато часу, навіть з використанням потужних комп'ютерів.

Для прикладу нехай довжина ключа шифрування дорівнює 128 бітів. Тому для зламу шифру необхідно виконати  $2^{128}$  операцій. Якщо обчислювальна машина виконує біля  $2^{49}$  операцій за секунду, то процес зламу займе  $2^{79}$  секунд. В році  $2^{25}$  секунд, таким чином необхідно  $2^{54}$  роки для зламу шифру, що має ключ шифрування  $2^{128}$  біти. Але вік всесвіту становить лише  $2^{34}$  роки [1].

Криптографічні перетворення класифікують різними способами, але найчастіше їх розподіляють в залежності від способу використання та за типом ключа:

- безключеві – не використовуються ключі (хеш-функції, генерація псевдовипадкових чисел, односторонні перестановки);
- перетворення з таємним ключем – використовується ключевий параметр – секретний ключ (симетричне шифрування, цифровий підпис, хеш-функції, ідентифікація);
- перетворення з відкритим ключем – використовують в своїх обчисленнях два ключі – відкритий та закритий (асиметричне шифрування, цифровий підпис).

Симетричні шифри в свою чергу розподіляються на блочні та поточні шифри. Ці шифри використовують однаковий ключ для шифрування та дешифрування (рис. 1.1).

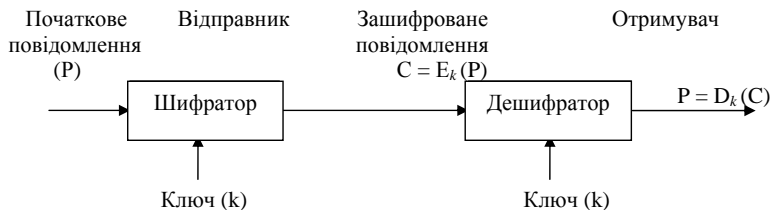


Рис. 1.1. Шифрування-дешифрування з закритим ключем

За наявності ключа шифротекст перетворюється системою шифрування у відкритий текст. Тому доступ до ключа шифрування повинен бути обмежений.

Процес шифрування описується виразом:

$$C = E_k(P), \quad (1.1)$$

де  $P$  – відкритий текст,

$k$  – ключ шифрування,

$C$  – шифротекст.

Процес дешифрування описується виразом:

$$P = D_k(C), \quad (1.2)$$

Цей тип шифрування має велику кількість представників. Найвідоміші з них – DES [4], AES [5], RC6 [6], MARS [7], Twofish [8], Serpent [9], LOKI 91[10], ГОСТ 28147-89 [11]. Криптографічні властивості цих шифрів наведено в [12-19].

В системах шифрування з відкритим ключем (асиметричні шифри) на відміну від симетричних шифрів використовуються два ключа – відкритий (публічний) та закритий (секретний) (рис. 1.2). Ці ключі математично пов'язані між собою. Шифротекст отримується з відкритого тексту відкритим ключем шифрування  $k_1$ . Відкритий текст отримується з шифротексту закритим ключем дешифрування  $k_2$ . Ця система визначається трьома алгоритмами: генерація ключів, шифрування та розшифрування. Алгоритм генерації відкритий. Алгоритми шифрування  $E_{k_1}$  та розшифрування  $D_{k_2}$  такі, що для будь-якого відкритого тексту  $m$  виконується рівність  $D_{k_2}(E_{k_1}(m))=m$ .



Рис. 1.2. Система шифрування-дешифрування з відкритим ключем

Асиметрична система шифрування на відміну від симетричної забезпечує не лише конфіденційність, а ще й може використовуватися для виконання автентифікації. Так віддалений вузол надсилає серверу зашифроване закритим ключем повідомлення. Після того як сервер



отримає шифротекст він дешифрує його відкритим ключем. Якщо дешифрування пройшло вірно, то автентичність вузла коректна.

Хеш-функцією  $H$  називається математична, або інша функція, що перетворює дані  $M$  довільної довжини в дані  $h$  фіксованої довжини [1, 20]:

$$h = H(M), \quad (1.3)$$

Як правило вихідні дані хеш-функції мають менший розмір ніж вхідні. В якості хеш-функцій найчастіше виступають однобічні функції. Головною задачею хеш функції є неможливість отримати за вихідними даними вхідні.

Хеш-алгоритми можуть використовуватись для визначення цілісності даних. Так після отримання повідомлення обчислюється хеш і порівнюється з хешем повідомлення, отриманого по закритим каналам. Якщо вони однакові, то повідомлення не модифікувалося.

Також хеш-алгоритми можуть використовуватися для автентифікації даних [21].

## 1.2. Методи формування блочних шифрів

Як було визначено Шенноном, для ефективного забезпечення закритості повідомлення шифри повинні використовувати два основних та головних принципи – «перемішування» (confusion) та «розсіювання» (diffusion) [22].

«Перемішування» – це сукупність операцій, які усувають зв'язок між відкритим текстом та шифротекстом. Усунення зв'язку між шифротекстом та відкритим текстом виконується шляхом знищення між ними статистичних закономірностей та надлишковості.

«Розсіювання» – поширення впливу одного знаку відкритого тексту на багато знаків шифротексту. Розсіювання змінює надлишковість відкритого тексту, шляхом розповсюдження її по всьому шифротексту. Найпростіший спосіб створити розсіювання є виконання транспозиції (перестановки). Елементарний перестановочний шифр лише переставляє букви відкритого тексту. Сучасні шифри для виконання розсіювання ще використовують операції розміщення частин повідомлення по всьому повідомленню.

«Перемішування» в сучасних шифрах виконується підстановкою S-боксами. Підстановка виконує заміну одних блоків даних іншими блоками даних.

Розсіювання в сучасних комп'ютерних системах доцільніше виконати бітовими перестановками, але ці операції не підтримуються сучасними процесорами. Формування розсіювання в блочних шифрах виконується за допомогою мережі Фейстеля (Feistel network) [23], [24], [25] та підстановочно-перестановочною мережі (Substitution-permutation network - SPN) [23], [24]. Методи формування розсіювання повністю визначають тип архітектури блочного шифру.

В таблиці 1.1 наведені сучасні блочні шифри та типи архітектури, які їм відповідають.

Таблиця 1.1

Сучасні блочні шифри та відповідні типи архітектури

Назва шифру	Тип архітектури (метод формування розсіювання)
CAST-256	Feistel network
Deal	Feistel network
DFC	Feistel network
Frog	SPN
LOKI	Feistel network
Mars	Feistel network
RC6	Feistel network
Rijndael	SPN
Safer K-64	SPN
Serpent	SPN
Twofish	Feistel network

### 1.2.1. Формування розсіювання методом мережі Фейстеля

Як зазначено вище одним з поширених методів формування «розсіювання» в блочних шифрах є класична мережа Фейстеля [23] (рис. 1.3).

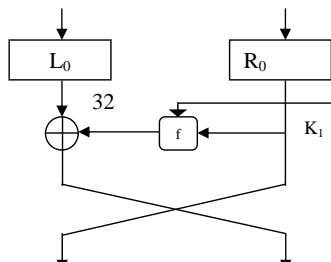


Рис. 1.3. Мережа Фейстеля

Цей метод використовували майже всі блочні шифри першого покоління. Формування розсіювання в цьому методі виконується зміною місцями лівої та правої частини. Блок шифрування поділяється на дві однакові за розмірами частини: праву (R) та ліву (L), які перетворюються певною кількістю ітерацій (раундів).

На кожному раунді з лівої частини і частини ключа  $k$  за допомогою функції шифрування  $f$  створюється елемент даних, що підсумовується за модулем 2 з правою частиною (R):  $R' = R + f(L, k)$ . Після цього ліва і права частини міняються місцями. Операція заміни місцями лівої L та правої частини R в одному раунді відповідає добутку на двовірну квадратну матрицю (1.4):

$$LR \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} = RL, \quad (1.4)$$

Перевагою такого методу є ефективність та компактність реалізації в апаратному та програмному варіантах. Причиною цього є зворотність перетворення і різниця лише в порядку застосування функції шифрування в раунді процедури зашифрування та розшифрування. Паліндроміальність (зворотня ідентичність) послідовності раундових функцій та використання однієї функції шифрування є причиною різниці процедур шифрування і розшифрування лише в порядку використання ключевих елементів.

Стійкість до криптоаналізу мережі Фейстеля залежить від раундових функцій і кількості раундів.

Для підвищення ступеня розсіювання, та для збільшення об'єму перетворення інформації за одиницю часу використовується узагальнена або розширена мережа Фейстеля (рис. 1.4). Ця мережа складається з чотирьох гілок. Перестановка, що виконується узагальненою мережею Фейстеля задається добутком на матрицю:

$$ABCD \begin{vmatrix} 0001 \\ 1000 \\ 0100 \\ 0010 \end{vmatrix} = BCDA, \quad (1.5)$$

Прикладом застосування узагальненої мережі Фейстеля є шифр RC6 [6].

В середині 90-х років минулого століття виникли значні зміни в криптографії та мікроелектроніці. В криптографії були розроблені ефективні методи криптоаналізу: диференційний [26], лінійний [27], та інші [28].

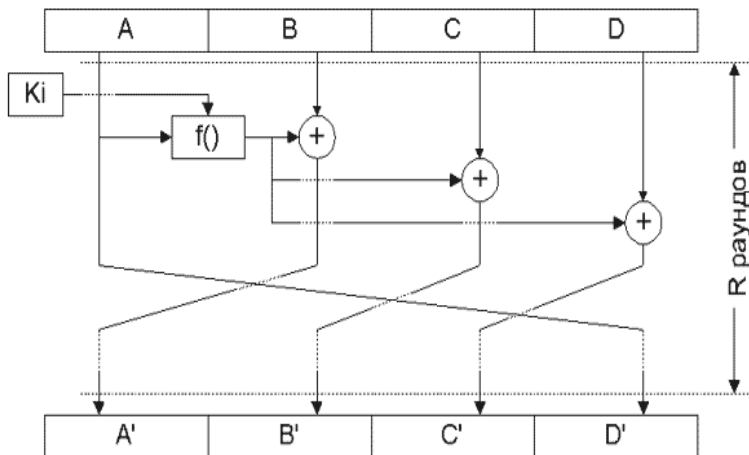


Рис. 1.4. Узагальнена мережа Фейстеля

Ці методи дозволили отримувати відкритий текст з шифротексту без знання ключа шифрування. В мікроелектроніці збільшилися можливості електронних пристроїв. Швидкодія та об'єм пам'яті збільшилися на декілька порядків. Це привело до пропорційного збільшення можливостей екстенсивних методів криптоаналізу, таких як повний перебір можливих даних.

Тому діалектичним розвитком класичної мережі Фейстеля стала незбалансована мережа Фейстеля (unbalanced Feistel network-UFN) [29] (рис. 1.5).

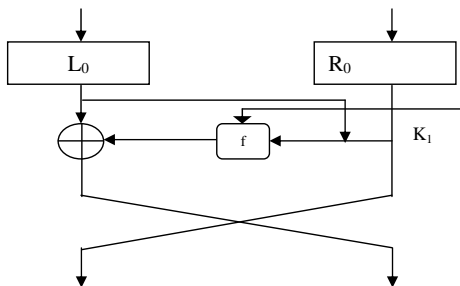


Рис. 1.5. Незбалансована мережа Фейстеля

В цьому типі мережі ліва частина –  $x_L$  та права частина –  $x_R$  не рівні за розміром (звичайна мережа Фейстеля має назву збалансована [23]).

Якщо в раунді  $r$  довжина лівої частини  $x^r_l - s$  бітів, а правої частини  $x^r_r - t$  бітів, то раундова функція виконує відображення з простору  $t -$  бітів, в простір  $s -$  бітів, тобто  $f: \{0,1\}^t \rightarrow \{0,1\}^s$ .

Вхідні частини в наступний раунд  $x^{r+1}_l$  та  $x^{r+1}_r$  визначаються

$$x^{r+1}_l \| x^{r+1}_r = x^r_r \| (f(x^r_r) + x^r_l), \quad (1.6)$$

де  $\|$  – оператор конкатенації.

Застосування цієї мережі дозволяє ускладнити характер залежності значення функції шифрування від своїх аргументів завдяки їх більшому розміру. В [29] продемонстровані і доведені криптографічні властивості цієї архітектури.

### **1.2.2. Формування розсіювання методом підстановочно-перестановочної мережі**

Інший метод формування «розсіювання» є підстановочно-перестановочна мережа (substitution-permutation network) [24, 25]. Підстановочно-перестановочна мережа наведена на рис. 1.6.

Цей метод створює «розсіювання» за допомогою перестановки бітів перед входом в наступний раунд. Частина мережі, що має назву S-бокс (substitution box), створює «перемішування» вхідних бітів.

Підстановочно-перестановочна мережа складається з певної кількості раундів. Кожний раунд складається з трьох кроків. Перед входом в перший раунд плантекст розбивається на блоки.

На першому кроці вхідні біти додаються за модулем два з підключачами цього раунду.

На другому кроці раунду біти перетворюються S-боксами.

На третьому кроці раунду перетворені біти одного S-боксу переставляються місцями з бітами інших S-боксів.

Перестановка в останньому раунді шифрування не застосовується через те, що вона не додає криптографічної стійкості.

Процес розшифрування відбувається зворотним чином. Останній підключ додається за модулем два з шифртекстом і в кожному раунді за допомогою зворотної перестановки, перетворюються S-боксами та бітовими перестановками.

Крок перестановки виконує операцію зміни однієї послідовності біт на іншу.

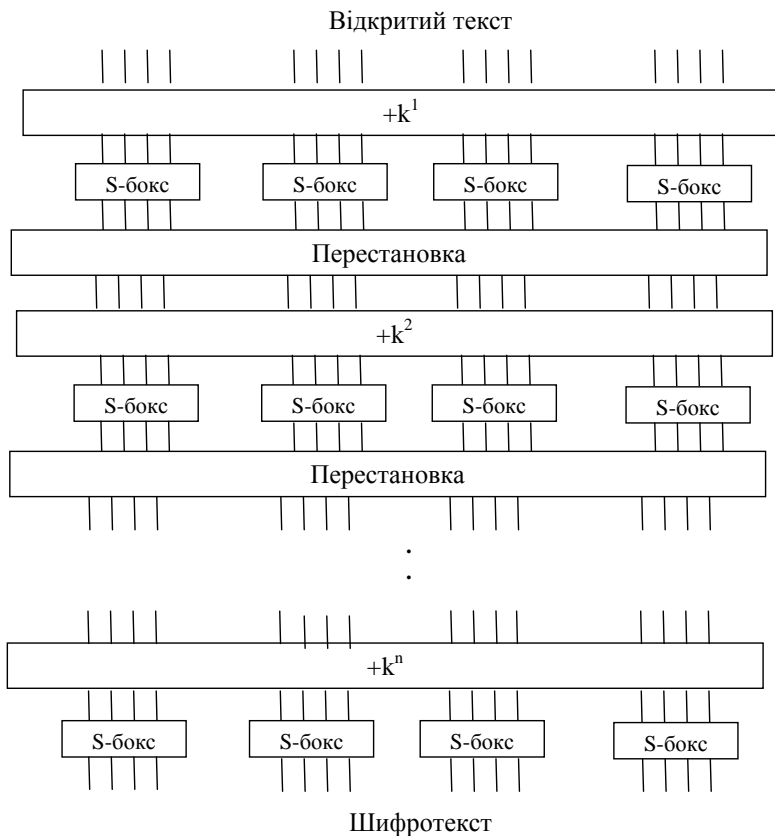


Рис. 1.6. Підстановочно-перестановочна мережа

Якщо початкова послідовність біт (вектор) –  $X = \{0,1\}^n$ , а кінцева –  $Y = \{0,1\}^n$ , ( $n$  – кількість бітів в перетворенні), то згідно лінійної алгебри [30], операція перестановки виконує множення на певну матрицю  $\chi$  з елементами 0 та 1:

$$Y = \chi X, \quad (1.7)$$

З виразів 1.4, 1.5 та 1.7 очевидно, що мережа Фейстеля – це окремий випадок підстановочно-перестановочної мережі; мережа Фейстеля та підстановочно-перестановочна мережа – це лінійне перетворення.

Стійкість підстановочно-перестановочної мережі залежить від S-боксів та виду перестановок. Перевагою підстановочно-перестановочної мережі є стійкість до різних варіантів криптоаналізу. Це наслідок потенційно вищого ступеня нелінійності шифрувального перетворення. Обґрунтування стійкості підстановочно-перестановочної мережі складне через непередбачуваність властивостей ланцюгів перетворення.

Недоліком підстановочно-перестановочної мережі є неефективність реалізації в сучасних комп'ютерних системах та мережах через дві основні причини. Однією з причин є відсутність підтримки бітових операцій процесорами в сучасних комп'ютерних системах та мережах.

Одним з шляхів усунення цього недоліку є спосіб, що використовує перестановку бітів двома етапами. На першому етапі виконується перестановка не бітів а байтів, а на другому етапі виконується добуток на певну матрицю. Цей спосіб реалізований в шифрі Rijndael [5] (рис. 1.7).

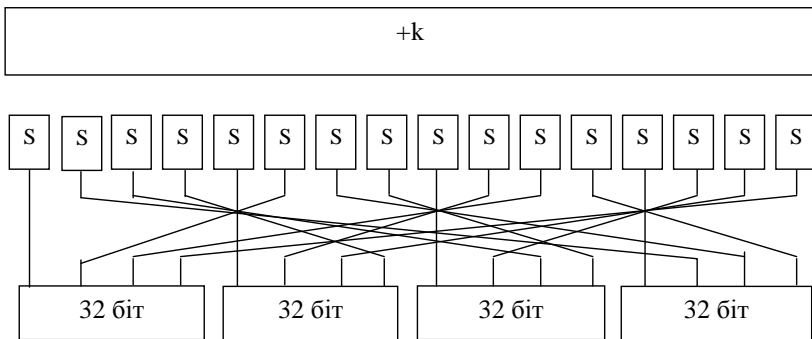


Рис. 1.7. Один раунд шифру Rijndael (AES)

Rijndael використовує підстановочно-перестановочну мережу, яка складається з 16 S-боксів розміром 8 X 8 в кожному раунді.

SPN цього типу це відображення  $\pi: \{0,1\}^{128} \rightarrow \{0,1\}^{128}$  з властивістю, що вхідні і вихідні бітові послідовності складаються з чотирьох 32-бітних слів  $x = (x_1 x_2 x_3 x_4)$  та  $y = (y_1 y_2 y_3 y_4)$ . Кожному з чотирьох вхідних байт в  $x_i$  відповідають переставлені чотири вихідні байти  $y_i$ .

Крім підстановочно-перестановочної мережі, зображеної на рис. 1.7 цей шифр для формування дифузії використовує лінійне

перетворення  $\Omega: \{0.1\}^{128} \rightarrow \{0.1\}^{128}$ , яке складається з паралельного застосування чотирьох лінійних перетворень  $\Omega = (\Omega_1 \Omega_2 \Omega_3 \Omega_4)$ .

Іншим недоліком цього методу є різниця в процедурах зашифрування та розшифрування. З цієї причини їх неможливо сумістити, що приводить до ускладнення реалізації вдвічі.

Ряд перспективних досліджень формування розсіювання запропоновано та створено на основі методу керованих перестановок [31-33].

Сучасні процесори комп'ютерних систем орієнтовані на роботу з байтами, їхні інструкції обмежено підтримують роботу з даними меншого розміру. На сучасних процесорах комп'ютерних систем бітові перестановки можуть бути реалізовані з використанням методу логічних операцій чи методу табличних підстановок [34].

В методі логічних операцій, кожний біт вилучається інструкцією логічного множення (інструкція AND), зсувається на свою нову позицію (інструкція SHIFT), а потім конкатенується з попередньо переставленими бітами (інструкція OR).

Метод табличних підстановок виконує перестановку біт швидше. Цей метод розподіляє біти на декілька підблоків і виконує перестановку бітів в підблоці шляхом застосування певної таблиці. В такій таблиці якщо стовпці відповідають певному підблоку, то рядки відповідають певному виду перестановки. Кінцева перестановка знаходиться на перетині певного стовпця з певним рядком. Коли біти всіх підблоків переставлені, вони об'єднуються інструкцією OR. Кількість інструкцій OR залежить від кількості підблоків.

Так для прикладу 64-бітна перестановка може бути виконана однією табличною перестановкою, якщо всі результати звести в таблицю розміром  $2^{64} \times 8$  байт. Це нереально. Для виконання такої перестановки 64 біти розподіляються на 8 байтів. Кожний байт переставляється окремою табличною перестановкою. Така таблиця має 256 елементів. Для реалізації цього методу необхідно 23 інструкцій. Вісім інструкцій EXTRACT (для вилучення певного байту), вісім табличних підстановок та сім інструкцій OR.

Метод табличних підстановок має меншу кількість інструкцій для реалізації перестановки ніж метод логічних операцій, але вимагає додаткового об'єму пам'яті. Об'єм пам'яті залежить від кількості перестановок, які необхідно реалізувати.

В таблиці 1.2 наведені кількість інструкцій та об'єм пам'яті, необхідний для реалізації 64-бітної перестановки описаними вище методами.

Метод табличної перестановки вимагає 16 Кбайт об'єму пам'яті для виконання певного виду перестановки. Кількість інструкцій для



реалізації цього методу може бути більше за 23 через помилки кеш-пам'яті процесору.

Таблиця 1.2

Залежність кількості інструкцій та об'єму пам'яті від методу перестановки

Назва методу перестановки	Кількість інструкцій	Об'єм пам'яті
Таблична перестановка	23	16 Кбайт
Логічні інструкції	256	0

### 1.3. Методи формування перемішування

Одним з підходів створення перемішування є застосування блоків підстановки (Substitution box- S-бокс). S-бокс розміром  $n \times m$  становить собою відображення  $S: \{0,1\}^n \rightarrow \{0,1\}^m$ . Змінна  $n$  – показує розмір в бітах вхідної послідовності, а змінна  $m$  – розмір вихідної послідовності.

Існують два основних методи формування S-боксів: табличні підстановки та S-бокси, створені на основі алгебраїчних функцій. Так в шифрі DES [4] S-бокс становить собою таблицю, що складається з чотирьох строк та шістнадцяти стовпців. Кожний елемент в таблиці є чотирибітне число. Вхідні біти S-боксу особливим чином визначають елемент таблиці, що є значенням вихідних бітів S-боксу. На вхід S-боксу надходять шість бітів  $b_1b_2b_3b_4b_5b_6$ .

Біти  $b_1$  та  $b_6$  об'єднуються, утворюючи цифру від 0 до 3. Значення цієї цифри визначає номер строки таблиці. Біти  $b_2b_3b_4b_5$  також об'єднуються і утворюють число від 0 до 15. Значення цього числа визначає номер стовпця таблиці.

Перевагою такого методу є відсутність математичної структури, яка може бути ефективно використана криптоаналізом. Недоліком такого методу є необхідність розташування таблиць підстановки в оперативному запам'ятовувальному пристрою комп'ютера.

Іншим методом створення S-боксів є формування S-боксу на основі алгебраїчних функцій. Так в шифрі LOKI 91[10] на вхід S-боксу надходять дванадцять бітів  $b_1b_2b_3b_4b_5b_6b_7b_8b_9b_{10}b_{11}b_{12}$  біти  $b_1b_2$  та  $b_{11}b_{12}$  формують число  $c$ , біти  $b_3b_4b_5b_6b_7b_8b_9b_{10}$  формують число  $r$ . Зміст S-боксу визначається за формулою:

$$S(r, c) = (c + ((17r) \oplus 0xFF) \& 0xFF)^{31} \bmod P, \quad (1.8)$$

Коефіцієнт  $P$  визначається таблицею 1.3.

Таблиця 1.3

Значення коефіцієнту  $P$  в залежності від раунду  $R$

R	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
P	375	279	391	395	397	415	419	425	433	445	451	463	471	477	487

Перевагою такого методу є компактність S-боксів і можливість реалізації їх в тих додатках комп'ютерних систем, які не можуть використовувати ОЗП та ПЗП для розміщення великих таблиць. Недоліком такого S-боксу є слабкість до диференційного аналізу [26]. Причиною цього є алгебраїчна простота функції (1.8) та її невідповідність суворому критерію розповсюдження (SAC-strict avalanche criterion). Усунення такого недоліку виконується застосуванням алгебраїчного перетворення, яке має високу алгебраїчну складність та високі криптографічні показники. Так в S-боксах шифра Rijndael [5] використовується обчислення зворотного полінома в полі Галуа  $GF(2^8)$  за модулем багаточлена  $m(x) = x^8 + x^4 + x^3 + x + 1$ :

$$S = x^{-1}, \quad (1.9)$$

Зворотне перетворення в  $GF(2^8)$  відповідає піднесенню до степеня 255. Кожний вхідний байт цього S-боксу представляється поліномом. Так, наприклад, байт 10100111 – відповідає поліному  $1 + x^2 + x^5 + x^6 + x^7$ . Його зворотне перетворення відповідає поліному  $x^2 + x^5$ , який відповідає числу 00100100.

Але такий метод має такий недолік. Операції добутку в скінченному полі в комп'ютерних системах виконується за допомогою зсувів на певну кількість біт та додаванням за модулем два [19]. Для виконання добутку різних поліномів необхідно виконати різну кількість зсувів. Тому час обчислення добутку поліномів буде різний. Цей факт використовує криптоаналіз потужності.

З огляду на перелічені вище методи формування перемішування та розсіювання ці методи для ефективного захисту інформації в комп'ютерних системах мають бути компромісним варіантом між трьома чинниками. Ці чинники – криптографічна стійкість перетворення, що використовується в методах формування перемішування та розсіювання, швидкість реалізації в комп'ютерній системі, розмір пам'яті комп'ютерної системи.

## 1.4. Криптоаналітичні властивості симетричних шифрів

Криптографічна стійкість симетричного шифру визначається здатністю протидіяти певним типам криптоаналізу [1].

Найбільш потужними методами криптоаналізу є лінійний [27] та диференційний [26]. Тому необхідно проаналізувати показники, які визначають стійкість шифра проти цих методів.

Лінійні перетворення (перестановки) та нелінійні перетворення (підстановки) являють собою булеві відображення. Булеве відображення в загальному вигляді – це відображення з простору  $d$ -розмірних векторів в простір  $r$ -розмірних векторів:  $B: \{0,1\}^d \rightarrow \{0,1\}^r$ . Іноді  $r = d$ . Це відображення може бути розглянуте як сукупність кількості  $r$  булевих функцій:  $B = (f_1, f_2, \dots, f_r)$ . Булева функція  $f_i$  – це відображення з простору  $d$  біт в простір одного біта:  $f_i: \{0,1\}^d \rightarrow \{0,1\}$ .

Критичним чинником лінійного криптоаналізу є високе значення лінійної ймовірності булевого відображення. Лінійна ймовірність булевого відображення [35] – це показник його нелінійності. Нелінійність – це відстань Хемінга булевого відображення до найближчої афіної функції. Лінійна ймовірність  $LP(v, w)$  відображення  $B: \{0,1\}^d \rightarrow \{0,1\}^d$  відносно векторів  $v, w \in \{0,1\}^d$  визначається виразом [35]:

$$LP(v, w) = \left( 2 \Pr \{ vx = wB(x) \} - 1 \right)^2, \quad (1.10)$$

де  $x \in \{0,1\}^d$  неформально розподілена випадкова величина.

Критичним чинником диференціального криптоаналізу є високе значення диференційної ймовірності булевого відображення. Диференційна ймовірність булевого відображення [36] – це показник розподілу його вхідних-вихідних диференціалів. Якщо  $v$  та  $v^*$   $d$ -розмірні вхідні вектори відображення  $B: \{0,1\}^d \rightarrow \{0,1\}^d$ , то диференціал входу визначається з виразу [26]:

$$\Delta v = v + v^*. \quad (1.11)$$

Диференціал виходу  $\Delta w$  відображення  $B: \{0,1\}^d \rightarrow \{0,1\}^d$  визначається з виразу:

$$\Delta w = w + w^* = B(v) + B(v^*), \quad (1.12)$$

Диференціальна ймовірність  $DP(\Delta v, \Delta w)$  булевого відображення визначається з виразу:

$$DP(\Delta v, \Delta w) = \text{Prob}\{B(v) + B(v + \Delta v)\} = \Delta w. \quad (1.13)$$

Результати обчислення лінійної ймовірності  $LP(v, w)$  та диференціальної ймовірності  $DP(\Delta v, \Delta w)$  по всім векторам  $v, w \in \{0,1\}^d$  створюють матрицю розміром  $2^d \times 2^d$ . Рядками і стовпцями цих матриць є значення векторів  $v, w \in \{0,1\}^d$  для лінійної ймовірності або вектори  $\Delta v, \Delta w$  для диференційного ймовірності.

З виразів (1.10) та (1.13) очевидно, що значення лінійної ймовірності  $LP(v, w)$  та диференціальної ймовірності  $DP(\Delta v, \Delta w)$  обмежені інтервалом  $[0,1]$ .

Проаналізуємо математичний зміст лінійної ймовірності. Коли значення  $LP(v, w)$  дорівнює 0, то  $v \cdot x = w \cdot B(x)$  в половині випадків. Тому значення ймовірності  $\text{Prob}\{v \cdot x = w \cdot B(x)\}$  дорівнює 0,5 і кореляції між значеннями  $x$  та  $B(x)$  не існує. Ненульове значення лінійної ймовірності  $LP(v, w)$  показує, що існує кореляція між вхідними і вихідними значеннями булевого відображення  $B$ , що активно використовується лінійним криптоаналізом. Якщо значення лінійної ймовірності  $LP(v, w)$  дорівнює 1, то або  $v \cdot x = w \cdot B(x)$  з ймовірністю 1, або  $v \cdot x \neq w \cdot B(x)$  з ймовірністю 1. Самі негативні варіанти такі:  $LP(0, 0) = 1$ ;  $LP(v, 0) = 0$  для  $v \neq 0$  та  $LP(0, w) = 0$  для  $w \neq 0$ .

Так в лінійному криптоаналізі [27] розглядаються раунди шифрування з другого по останній ( $2 \dots R$ ) як одна функція (відображення), що залежить від сукупного ключа  $k^\circ$  ( $k^\circ = [k_2 k_3 \dots k_n]$ ) і виконує відображення  $\{0,1\}^d \rightarrow \{0,1\}^d$ . Результативність цього аналізу залежить від векторів  $v, w \in \{0,1\}^d$ , значення яких зводять до максимального значення  $LP(v, w)$  відносно цієї функції.

Результативність лінійного криптоаналізу визначається кількістю пар  $N$  плантекст-шифртекст, які необхідні для його здійснення. Саме значення  $LP(v, w)$  і визначає кількість таких пар [27].

Для максимальної протидії лінійному криптоаналізу ймовірність, що вихідний відносний вектор  $w$  відповідає вхідному відносному вектору  $v$  має бути рівно розподілена і становити  $(0,5)^d$ . Максимальне значення лінійної ймовірності відображення послідовності раундів шифрування ( $1 \dots R$ ) –  $\max LP^{[1..R]}(v, w)$  – один з критичних чинників лінійного криптоаналізу. Пряме обчислення цього значення складне з двох причин. По-перше, необхідно для всіх векторів  $v, w \in \{0,1\}^d$  зашифрувати всі можливі вектори  $x \in \{0,1\}^d$  по раундам  $1..R$ , що

## ЛІТЕРАТУРА

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Брюс Шнайер. – М.: Триумф, 2002. – 816 с.
2. Лужецкий В. А. Блочный симметричный шифр на основе арифметических операций за модулем  $2^N$  / В. В. Сокирук, В. А. Лужецкий // Современные методы кодирования в электронных системах (СМКЭС-2004): Міжнародна науково-технічна конференція, 2004: тези доповідей. – Суми. – С. 55 – 56
3. Зима В. М. Безопасность глобальных сетевых технологий / В. М. Зима., А. А. Молдовян, Н. А. Молдовян – СПб.: БХВ-Петербург, 2000. – 320 с.
4. National Bureau of Standart (NBS). Data Encryption Standart (DES) // Federal Information Processing Standards Publication 46-2. – December 1993.
5. Daemen J. The Design of Rijndael. AES: The Advanced Encryption Standard / Joahn Daemen, Vincent Rijmen // Springer – Berlin. – 2002. – V. 234. – P. 24 – 28
6. The RC6 block cipher / [R. Rivest, J. Robshshaw, R. Sidney, and Y. Yin] // NIST AES proposal. – August 1998.
7. Burwick C. et al. MARS: a candidate cipher for AES // /NIST AES proposal. – June 1998.
8. Twofish: A 128-Bit Block Cipher / [B. Schneier, J. Kelsey, D. Whiting, C. Hall, N. Ferguson] // NIST AES proposal. – June 1998. – Режим доступу <http://www.schneier.com/paper-twofish-paper.pdf>
9. Biham E. Serpent: A New Block Cipher Proposal / E. Biham, R. Anderson, L. Knudsen // Proceeding in Fast Software Encryption (FSE 98): Lecture Notes in Computer Science. – Springer-Verlag. – Vol 1372. – P. 222 – 238
10. Brown L. LOKI: A cryptographic primitive for authentication and secrecy applications / L. Brown, J. Pieprzyk, J. Sebery // Advances in Cryptology – AUSCRYPT `90.: Lecture Notes in Computer Science. – Springer-Verlag. – Vol 453. – P. 229 – 236.
11. Стандарт шифрования ГОСТ 28147-89. – М.: Издательство стандартов. – 1989. – 50 с.
12. E Biham. How to Forge DES-Encrypted Messages in  $2^{28}$  Steps // Technical Report CS884. – Technion. – August 1996.
13. Murphy S. Essential Algebraic Structure within the AES / S. Murphy, M. Robshaw // Proceedings of Crypto`02, Advances in Cryptology.: Lecture Notes in Computer Science. – Springer-Verlag. – Vol. 718. – 2002. – P. 196 – 208.

14. Knudsen L. Cryptanalysis of LOKI91 / L. Knudsen // Advanced in Cryptology -Asiacrypt '92.: Lecture Notes in Computer Science. – Springer-Verlag. – Vol. 718. – 1992. – P. 196 – 208.
15. Contini S., Rivest R., Robshaw M., Shi Z., and Yin Y. The security of the RC6 block cipher // Technical Report. – Режим доступа: [www.rsa.com/rsalabs/aes](http://www.rsa.com/rsalabs/aes). - september 2007
16. Schneier B. Impossible Differentials in Twofish. – Режим доступа: <http://www.schneier.com/paper-twofish-impossible.pdf>
17. Biham E. Impossible Differential on 8-round MARS Core / E. Biham, V. Furman // Presented in 3<sup>rd</sup> AES conference. – NY USA. – April 2000.
18. Брикелл Э. Криптоанализ: обзор новейших результатов / Э. Брикелл, Э. Одлижко // ТИИЭР. – 1998. – № 5. – С. 75 – 94.
19. Блочные криптосистемы. Основные свойства и методы анализа стойкости / А. А. Варфоломеев, А. Е. Жуков, А. Б. Мельников, А. М. Устюжанин – М.: МИФИ, 1998. – 198 с.
20. National Institute of Standards and technology. Secure hash standard // Federal Information Processing Standards Publication 180-1. – April 1994.
21. Lloyd B. PPP authentication protocols / B. Lloyd // The Internet Engineering Task Force (IETF) Internet Draft. – 1994. – RFC-1661.
22. Шеннон К. Теория связи в секретных системах / Клод Шеннон – М.: Связь. – 1978. – 40 с.
23. Feistel H. Cryptography and computer privacy / Horst Feistel // Scientific American. – 1973. – Vol. 228. – No. 5. – P. 15 – 23.
24. Feistel H. Some cryptographic techniques for machine-to-machine data communications / H. Feistel, W. Nortz, J. Smith // Proceedings of the IEEE. – 1975. – Vol. 63. – No. 11. – P. 1545 – 1554.
25. Feistel H. Block cipher cryptographic system. – 1974. – U. S. Patent No. 3798359.
26. Biham E. A. Differential cryptanalysis of the full 16-round DES / E. Biham, A. Shamir // Advances in Cryptology – CRYPTO`92.: Lecture Notes in Computer Science. – Springer-Verlag. – 1993. – Vol. 740. – P. 487 – 496.
27. Matsui M. Linear cryptanalysis method for DES cipher / M. Matsui // Advanced in Cryptology – Eurocrypt`93: Lecture Notes in Computer Science. – Springer-Verlag. – 1993. – Vol. 765. – P. 386 – 397.
28. Jakobsen T. The Interpolation Attack on Block Ciphers / T. Jakobsen, L. Knudsen // Proceedings of Fast Software Encryption`97: Lecture Notes in Computer Science. – Springer-Verlag. – 1997. – Vol. 1267. – P. 28 – 40.

29. Schneier B. Unbalanced Feistel networks and block-cipher design / B. Schneier, J. Kelsey // Fast Software Encryption: Third International Workshop, Lecture Notes in Computer Science. – Springer-Verlag. – 1996. – Vol. 1039. – P. 121 – 144.
30. Пискунов Н. С. Дифференциальное и интегральное исчисление / Н. С. Пискунов – М.: Наука. – 1976. – 575 с.
31. Молдовян Н. А. Скоростные блочные шифры / Н. А. Молдовян. – СПб.: СПбГУ. – 1998. – 230 с.
32. Молдовян А. А. Перспективы разработки скоростных шифров на основе управляемых перестановок / А. А. Молдовян, Н. А. Молдовян, Л. Е. Алексеев // Безопасность информационных технологий. – № 1. – М.: МИФИ. – 1999. – С. 41 – 47.
33. Изотов Б. В. Модели управляемых подстановочных операций и синтез блочных алгоритмов защиты информации: дис. канд. техн. наук: 05.13.19 / Борис Викторович Изотов. – СПб, 2001. – 179 с.
34. Lee R. Efficient permutation instructions for fast software cryptography / R. Lee, Z. Shi, X. Yang // IEEE Micro. – 2001. – Vol. 21. – No. 6. – P. 56 – 59.
35. Harpes C. A generalization of linear cryptanalysis and the applicability of Matsui's piling-up lemma / C. Harpes, G. Kramer, J. Massey // Advanced in Cryptology – Eurocrypt'95: Lecture Notes in Computer Science. – Springer-Verlag. – 1995. – Vol. 921. – P. 24 – 38.
36. Provable security against differential and linear cryptanalysis for the SPN structure / S. Hong, S. Lee, J. Lim, J. Sung, D. Cheon // Fast Software Encryption – FSE'00: Lecture Notes in Computer Science. – Springer-Verlag. – 2001. – Vol. 1978. – P. 273 – 283.
37. Matsui M. The first experimental cryptanalysis of the Data Encryption Standard / M. Matsui // Advanced in Cryptology – CRYPTO '94: Lecture Notes in Computer Science. – Springer-Verlag. – 1994. – Vol. 839. – P. 1 – 11.
38. Kanda M. Practical security evaluation against differential and linear cryptanalysis for Feistel ciphers with SPN round function / M. Kanda // Seventh Annual International Workshop on Selected Areas in Cryptography-SAC'00: Lecture Notes in Computer Science. – Springer-Verlag. – 2001. – Vol. 2012. – P. 324 – 338.
39. Nyberg K. Perfect nonlinear S-boxes / Nyberg K. // Advances in Cryptology – EUROCRYPT '91: Lecture Notes in Computer Science. – Springer-Verlag. – 1991. – Vol. 547. – P. 378 – 386.
40. Meier W. Nonlinearity criteria for cryptographic functions / W. Meier, O. Staffelbach // Advances in Cryptology – EUROCRYPT '89: Lecture Notes in Computer Science. – Springer-Verlag. – 1990. – Vol. 434. – P. 549 – 562.

41. Мак-Вильямс Дж. Теория кодов, исправляющих ошибки / Дж Мак-Вильямс, А. Слоэн – М.: Связь, 1979. – 744 с.
42. Rothaus O. On bent functions / O. Rothaus // Journal of combinatorial theory. – Ser. A. – V. 20. – P. 300 – 305.
43. Dillon J. A survey of bent function / J. Dillon // The NSA Technical Journal. – 1972. – P. 191 – 215.
44. Golomb S. Deep space range measurements / S. Golomb // Jet Propulsion Laboratory. – Pasadena. – CA Research Summary. – 1960. – No. 36-1. – P. 3 – 28.
45. Intel Corporation. Intel Itanium processor: high performance on security algorithms. Режим доступа [www.intel.com/design/itanium/downloads/itaniumssl.pdf](http://www.intel.com/design/itanium/downloads/itaniumssl.pdf).
46. Морисита И. Аппаратные средства микроЭВМ / И. Морисита – М.: Мир, 1988. – 280 с.
47. Biham E. On Matsui's linear cryptanalysis / E. Biham // Advances in Cryptology – EUROCRYPT '94.: Lecture Notes in Computer Science. – Springer-Verlag. – 1995. – Vol. 950. – P. 341 – 355.
48. Бевз О. М. Криптографічні властивості підстановочно-перестановочних мереж / О. М. Бевз // Наукові праці Донецького національного технічного університету. – Серія: «Обчислювальна техніка та автоматизація». – 2006. – Вип. 107. – Донецьк, 2006. – С. 12 – 16.
49. Бевз О. Паралелізована хеш-функція з двома ключами / Олександр Бевз, Володимир Папінов // Вісник Вінницького політехнічного інституту. – 2003. – № 6. – С. 322 – 325.
50. The block cipher Hierocrypt / K. Ohkuma, H. Muratani, F. Sano, S. Kawamura // Proceedings of Selected Areas in Cryptography – SAC2000.: Lecture Notes in Computer Science. – Springer-Verlag. – 2001. – Vol. 2012. – P. 72 – 88.
51. The cipher SHARK [Rijmen V., Daemen J., Preneel B., Bosselaers A., Win E] // Proceedings of Fast Software Encryption - FSE'96: Lecture Notes in Computer Science. – Springer-Verlag. – 1997. – Vol. 1039. – P. 99 – 112.
52. Daemen J. The block cipher Square / J. Daemen, L. Knudsen, V. Rijmen // Proceedings of Fast Software Encryption - FSE'97: Lecture Notes in Computer Science. – Springer-Verlag. – 1997. – Vol. 1267. – P. 54 – 68.
53. Бевз О. Протистояння диференційному і лінійному криптоаналізу збалансованими булевими функціями / Олександр Бевз, Роман Кветний // Наукові праці Донецького Національного Технічного Університету. Серія: Обчислювальна техніка та автоматизація. – Вип. 64. – С. 150 – 155



54. Бевз О. М. Кореляційні та диференційні властивості S-боксів на основі високонелінійних функцій / О. М. Бевз // Інформаційні технології та комп'ютерна інженерія. – 2006. – № 1(5). – С. 154 – 158.
55. Propagation characteristics of boolean functions / [B. Preneel, W. Van Leekwijk, V. Linden, R. Goevarts, J. Vanderwalle] // Advances in Cryptology. – EUROCRYPT'90. – Springer-Verlag. – Berlin. – 1991. – P. 161 – 173.
56. Intel. Wilamette Processor Software Developer's Guide // March 2007. – Order Number 245355-001.
57. Daimen J. Correlation matrices / J. Daimen, R. Govarets, J. Vandewalle // Fast Software Encryption. – Second International Workshop: Lecture Notes in Computer Science. – Springer-Verlag. – 1991. – Vol. 1008. – P. 275 – 285.
58. Practical and provable security against differential and linear cryptanalysis for substitution-permutation networks / [J. Kang, S. Hong, S. Lee, etc.] // ETRI Journal. – Vol. 23. – No. 4. – December 2001.
59. GJ Kühn. Algorithms for Self-Synchronising Ciphers // Proceeding COMSIG 90. – P. 28 – 29.
60. Бевз О. М. Кореляційні властивості фільтр-генератора з суттєво нелінійною булевою функцією / Р. Н. Кветний, О. М. Бевз, О. О. Юдін // Вісник Черкаського державного технологічного університету. – № 2. – С. 107 – 111.
61. Бевз О. Використання булевих високонелінійних функцій для створення поточного шифру / Олександр Бевз, Володимир Папінов // Інформаційні технології та комп'ютерна інженерія. – 2005. – № 3. – С. 263 – 267.
62. Домарев В. В. Защита информации и безопасность компьютерных систем / В. В. Домарев – К.: Диасофт, 1999. – 480 с.
63. Карасик И. Программные и аппаратные средства защиты информации для персональных компьютеров / И. Карасик – Компьютер Пресс. – 1992. – № 3. – С. 37 – 46.
64. Саати Т. Аналитическое планирование. Организация систем / Т. Саати, К. Кернс – М.: Радио и связь, 1991. – 224 с.
65. Халяпин Д Б Основы защиты информации / Д. Б. Халяпин, В. И. Ярочкин – М.: ИПКИР, 1994. – 228 с.

*Наукове видання*

**Бевз Олександр Миколайович,  
Квстний Роман Наумович**

**ШИФРУВАННЯ ДАНИХ НА ОСНОВІ  
ВИСОКОНЕЛІНІЙНИХ БУЛЕВИХ ФУНКЦІЙ ТА  
КОДІВ З МАКСИМАЛЬНОЮ ВІДСТАННЮ**

Монографія

Редактор С. Малішевська  
Оригінал-макет підготовлено О. Бевзом

Підписано до друку 11.01.2010 р.  
Формат 29,7×42¼ . Папір офсетний.  
Гарнітура Times New Roman.  
Друк різнографічний. Ум. друк. арк. 5,54.  
Наклад 100 прим. Зам № 2010-007.

Вінницький національний технічний університет,  
комп'ютерний інформаційно-видавничий центр.  
21021, м. Вінниця, Хмельницьке шосе, 95,  
ВНТУ, ГНК, к. 114  
Тел. (0432) 59-85-32  
Свідоцтво суб'єкта видавничої справи  
серія ДК № 3516 від 01.07.2009 р.

Віддруковано у Вінницькому національному технічному університеті,  
в комп'ютерному інформаційно-видавничому центрі.  
21021, м. Вінниця, Хмельницьке шосе, 95,  
ВНТУ, ГНК, к. 114  
Тел. (0432) 59-81-59  
Свідоцтво суб'єкта видавничої справи  
серія ДК № 3516 від 01.07.2009 р.