МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ УНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

ІНСТИТУТ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ

А. М. Олексійчук, А. А. Матійко

Методи побудови та аналізу симетричних криптосистем

Підручник

Затверджено Вченою радою КПІ ім. Ігоря Сікорського
як підручник для здобувачів ступеня магістра
за спеціальністю 125 Кібербезпека та захист інформації

Електронне мережне навчальне видання

Київ
КПІ ім. Ігоря Сікорського
2025

УДК 004.056

Автори: *Олексійчук Антон Миколайович*, д.т.н., професор
Матійко Александра Андріївна, PhD

Рецензенти: *Ковальчук Людмила Василівна*, д.т.н., професор, провідний науковий співробітник відділу математичного та комп'ютерного моделювання ІПНЕ ім. Г.Є. Пухова
Самойлов Ігор Володимирович, к.т.н., доцент, доцент Спеціальної кафедри № 1 ІССЗІ КПІ ім. Ігоря Сікорського

Відповідальний редактор: *Голь Владислав Дмитрович*, к.т.н., професор, завідувач Спеціальної кафедри № 1 ІССЗІ КПІ ім. Ігоря Сікорського

Гриф надано Вченою радою КПІ ім. Ігоря Сікорського
(протокол № 3 від 10.03.2025 р.)

Олексійчук А.М., Матійко А.А.
Методи побудови та аналізу симетричних криптосистем [Електронний ресурс]: підруч. для здобувачів ступеня магістра за спец. 125 Кібербезпека та захист інформації / А.М. Олексійчук, А.А. Матійко; КПІ ім. Ігоря Сікорського. – Електрон. текст. дані (1 файл). – Київ: КПІ ім. Ігоря Сікорського, 2025. – 157 с.

Підручник присвячено вивченню сучасних методів побудови та криптоаналізу блокових і потокових шифрів, їхніх математичних моделей, окремих компонент, атак на них та відповідних методів обґрунтування їхньої стійкості. Основну увагу зосереджено на роз'ясненні найважливіших понять та методології досліджень в галузі симетричної криптографії. Відмінними рисами підручника є оригінальність змісту та використання належного рівня загальності для кращого розуміння основних концепцій. Низку результатів викладено у навчальній літературі вперше.

Призначено для здобувачів вищої освіти другого (магістерського) рівня за спеціальністю 125 Кібербезпека та захист інформації.

УДК 004.056

Реєстр. № 24/25-020. Обсяг 3,8 авт. арк.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
проспект Берестейський, 37, м. Київ, 03056
https://kpi.ua
Свідоцтво про внесення до Державного реєстру видавців, виготовлювачів і розповсюджувачів видавничої продукції ДК № 5354 від 25.05.2017 р.

ЗМІСТ

Вступ

Цей підручник створено на основі матеріалів лекцій з однойменної навчальної дисципліни відповідно до освітньо-професійної програми підготовки здобувачів вищої освіти ступеня магістр за спеціальністю 125 Кібербезпека та захист інформації. Мета навчальної дисципліни полягає у формуванні в здобувачів теоретичних знань та практичних вмінь у галузі побудови та аналізу симетричних криптосистем, а також у підготовці їх до подальшого самостійного освоєння перспективних методів криптографічного захисту інформації.

Підручник складається з чотирьох розділів, присвячених вивченню низки понять та результатів, які утворюють основу сучасних методів побудови та криптоаналізу блокових і потокових шифрів, їхніх математичних моделей, окремих компонент, атак на них та відповідних методів обґрунтування їхньої стійкості. Наприкінці кожного розділу є завдання для самоконтролю, більшість з яких спрямована на розвиток ідей і методів, викладених в основній частині книги. До переліку посилань, поряд із сучасними публікаціями, включено низку класичних робіт, які належать видатним фахівцям у галузі симетричної криптографії.

При відборі матеріалу автори намагалися приділити максимальну увагу роз'ясненню найважливіших понять та методології досліджень в галузі потокових і потокових шифрів, що надало б можливість читачеві швидше опанувати цей предмет на сучасному рівні.

Відмінними рисами підручника є оригінальність змісту та використання належного рівня загальності викладення для кращого розуміння основних концепцій. Низку результатів, зокрема, в § 2.3 – § 2.5, викладено у

навчальній літературі вперше. При написанні розділів 3 і 4 значною мірою використано окремі пункти навчального посібника [1].

Автори сподіваються, що опанувавши теоретичний матеріал та розв'язавши більшість завдань у цьому підручнику, читач набуде можливості краще орієнтуватися в сучасній науковій літературі з методів побудови та аналізу симетричних криптосистем.

Перелік термінів та позначень

Відображенням f множини X у множину Y називають правило, згідно з яким кожному елементу множини X ставиться у відповідність єдиний елемент множини Y. Це відображення позначають символом $f: X \to Y$.

Відображення $f: X \to Y$ називається *ін'єктивним*, якщо виконується умова $\forall x_1, x_2 \in X (x_1 \neq x_2): f(x_1) \neq f(x_2)$, тобто різні елементи множини X мають різні образи.

Відображення $f: X \to Y$ називається *сюр'єктивним*, якщо виконується умова $\forall y \in Y \; \exists x \in X: f(x) = y$, тобто для кожного елемента множини Y існує принаймні один прообраз.

Відображення $f: X \to Y$ називається *бієктивним*, якщо воно одночасно є сюр'єктивним та ін'єктивним. В цьому випадку *обернене до* f *відображення* визначається за правилом

$$f^{-1}(y) = x \Leftrightarrow f(x) = y, \; x \in X, y \in Y.$$

Перетворенням множини X називається відображення $f: X \to X$. Бієктивне перетворення називається *підстановкою* на множині X.

Композиція $g \circ f$ *відображень* $f: X \to Y$ та $g: Y \to Z$ визначається за формулою $(g \circ f)(x) = g(f(x)), \; x \in X$.

Декартовий добуток $X \times Y$ множин X та Y визначається як множина всіх упорядкованих пар (x, y), де перший елемент пари належить множині X, а другий – множині Y:

$$X \times Y = \{(x, y) \mid x \in X, y \in Y\}.$$

Декартовий добуток n *множин* визначається рекурсивно:

$$X_1 \times X_2 \times ... \times X_n = (X_1 \times X_2 \times ... \times X_{n-1}) \times X_n,\ n = 3, 4, ...;$$

n -й декартовий степінь множини X визначається за формулою

$$X^n = \{(x_1, ..., x_n) \mid x_i \in X,\ i = 1, 2, ..., n\}.$$

Надалі використовуються такі позначення та скорочення

◄ – початок доведення;

► – закінчення доведення;

$|X|$ – потужність скінченної множини X;

V_n – множина двійкових векторів довжини n;

$\overline{i, j}$ – множина $\{i, i+1, \ldots, j\}$, де i, j – невід'ємні цілі числа.

$\delta_{\alpha,\beta}$ – символ Кронекера: $\delta_{\alpha,\beta} = 1$, якщо $\alpha = \beta$; $\delta_{\alpha,\beta} = 0$, якщо $\alpha \neq \beta$;

$\mathbf{R}$ – множина дійсних чисел;

$\mathbf{GF}(q)$ – скінченне поле з q елементів;

$\oplus$ – додавання за модулем 2.

$A \otimes B$ – тензорний добуток матриць A і B;

$d(x, y)$ – відстань Геммінга між векторами $x, y \in V_n$;

T_f – вектор-стовпець значень булевої функції f;

P_f – вектор-стовпець коефіцієнтів полінома Жегалкіна булевої функції f;

$\| f \|$, $wt(f)$ – вага булевої функції f;

$\deg f$ – степінь полінома Жегалкіна булевої функції f;

$\min \deg I$ – мінімальний степінь ідеалу I кільця булевих функцій;

$\mathrm{Ann}(f)$ – анулятор булевої функції f;

$\mathrm{rank}(M)$ – ранг матриці M;

$\langle f, g \rangle$ – скалярний добуток псевдобулевих функцій f і g;

$\| f \|_2$ – евклідова норма псевдобулевої функції f;

H_n – матриця Адамара порядку 2^n;

N_f – нелінійність булевої функції f.

$\hat{f}(\alpha)$ – коефіцієнт Уолша-Адамара булевої функції f, який відповідає вектору $\alpha \in V_n$;

$C_f(\alpha)$ – коефіцієнт Фур'є псевдобулевої функції f, який відповідає вектору $\alpha \in V_n$;

$\log x$ – логарифм за основою 2.

$f(n) = O(g(n)) \quad \Leftrightarrow \quad \exists C > 0 : | f(n) | \leq C | g(n) |$ для кожного $n = 1, 2, \ldots$;

SPN – Substitution-Permutation Network;

ЛРЗ – лінійний регістр зсуву.

1. ВСТУП ДО МЕТОДІВ ПОБУДОВИ ТА АНАЛІЗУ СИМЕТРИЧНИХ КРИПТОСИТЕМ

§ 1.1. Призначення, класифікація та загальні принципи побудови симетричних криптосистем

Сформулюємо означення основних понять, що використовуються далі.

Зазвичай *криптографічною системою* або *криптосистемою* називають систему забезпечення безпеки інформації криптографічними методами в частині конфіденційності, цілісності, автентифікації, неможливості відмови від авторства або невідслідковності. При цьому *криптографічними* називають такі методи, що (на відміну від організаційних, технічних тощо) базуються на математичних перетворення інформації, яка захищається. Ці перетворення залежать від *ключових параметрів* (*ключів*), які є доступними лише авторизованим користувачам відповідної інформаційної системи.

Стійкість криптосистеми (security of a cryptosystem) визначається як її здатність протистояти всіляким атакам на неї з боку противника. Саме стійкість характеризує здатність криптосистеми виконувати визначену функцію із забезпечення безпеки інформації, тобто відповідність криптосистеми її призначенню.

На сьогодні серед фахівців нема цілком узгодженої думки стосовно того, що являє собою сучасна криптографія, наскільки суттєво вона відрізняється від криптології та якими є її предмет і методи. Поряд з тим, переважна більшість погоджується з такими означеннями.

Криптографія – це галузь знань та практичної діяльності, що пов'язана з розробкою криптосистем і криптографічних протоколів, а також відповідних засобів криптографічного захисту інформації.

Криптологія – галузь знань, яка досліджує математичні моделі та властивості криптосистем.

Криптоаналіз – розділ криптології, який досліджує методи оцінювання й обґрунтування стійкості криптосистем.

Зауважимо, що криптоаналіз є невід'ємною частиною процесу створення криптосистем. Він має дві сторони: негативну, яка полягає у побудові атак на криптосистеми, тобто їх зламуванні; позитивну, яка полягає в обґрунтуванні стійкості криптосистем, тобто доведенні того, що для них не існує ефективних атак з певного класу. Отже, якщо в результаті аналізу криптосистеми вдається знайти її слабкості, то з'являються атаки на неї. Якщо ж, навпаки, виявляється, що в певному класі атак нема ефективних, отримують обґрунтування стійкості криптосистеми відносно зазначених атак.

За типом ключів, що використовуються, криптосистеми поділяють на *симетричні* (*із секретним ключем*; secret або private key) та *асиметричні* (*з відкритим ключем*; public key).

За призначенням криптосистеми поділяють на такі класи.

1. *Шифросистеми* (*шифри*) забезпечують конфіденційність інформації, тобто неможливість отримати доступ до її змісту особам, які не мають на це права.

2. *Системи автентифікації* (зокрема, ідентифікації, імітозахисту) забезпечують автентичність (тобто справжність) сторін інформаційної взаємодії, цілісність повідомлень, що передаються.

3. *Системи цифрового підпису* забезпечують неможливість відмови від авторства створених повідомлень.

Є також численні види *криптографічних примітивів* (наприклад, псевдовипадкові генератори, коди автентифікації повідомлень, ґеш-функції), а також *криптографічних протоколів* – розподілених алгоритмів (тобто таких, що виконуються, принаймні, двома сторонами), які мають різне призначення, наприклад, протоколи передачі, узгодження або розподілу ключів, протоколи розділення секрету, протоколи ідентифікації тощо. Усі вони активно вивчаються в межах криптографії та криптоаналізу.

За стійкістю криптосистеми поділяють на *теоретико-інформаційно* (*безумовно*) *стійкі* (information theoretical secure або unconditional secure) та *обчислювально стійкі* (computational secure).

Теоретико-інформаційна стійкість вимірюється за допомогою кількості інформації про невідомий об'єкт (ключ або відкритий текст), яка міститься у доступних противнику даних. Це стійкість відносно атак противника, який має необмежені обчислювальні ресурси.

Обчислювальна стійкість вимірюється кількістю операцій, які треба виконати для відновлення невідомого об'єкту (ключа), виходячи з доступних даних. Це стійкість відносно атак противника, що має обмежені ресурси.

Класичним прикладом безумовно стійкої шифросистеми є *шифр Вернама* (one-time pad), що визначається за правилом

$$y = x \oplus k ,$$

де x, y, k – двійкові послідовності однакової довжини, x – відкритий текст, y – шифрований текст, k – ключ, який вибирається випадково рівноймовірно та знищується після застосування.

Шифр Вернама є досконалим за Шенноном, оскільки шифрований текст не містить жодної апостеріорної інформації про відкритий текст. Недоліком цього шифру є його малопрактичність, обумовлена необхідністю передачі захищеними каналами зв'язку великої кількості ключів, довжини яких повинні бути не менше за довжини відкритих повідомлень. Такий недолік притаманний усім безумовно стійким криптосистемам чи протоколам. Тому переважна більшість сучасних криптосистем відноситься до класу обчислювально стійких, що використовують секретні ключі відносно малого розміру (декілька сотень чи тисяч бітів). Основним принципом побудови таких криптосистем є гармонійне поєднання вимог до стійкості та практичності у їхніх конструкціях.

Зазвичай вимога до стійкості симетричної криптосистеми формулюється просто: не повинно існувати атак на криптосистему, обчислювальна складність яких є помітно менше за складність повного перебору ключів. Переважно задовольнити цю вимогу вдається тільки відносно обмеженої кількості відомих (а не усіх можливих) атак; при цьому обґрунтування стійкості криптосистеми покладається на її розробника. Практичність криптосистеми визначається, головним чином, швидкістю виконання процедур, які вона реалізує (наприклад, зашифрування/розшифрування чи формування або перевірки цифрового підпису) на різноманітних обчислювальних платформах.

Інший принцип побудови криптосистем полягає у застосуванні для цього простих (з алгоритмічного погляду) компонент, що мають прозорі криптографічні властивості. Надмірна складність є ворогом безпеки, тому будь-яка криптосистема повинна будуватись за простими та зрозумілими правилами, які гарантують можливість дослідження та обґрунтування її стійкості.

Зазначені принципи уточнюються та розкриваються надалі при вивченні потокових і блокових шифрів.

§ 1.2. Означення та елементарні властивості алгебраїчних моделей шифрів

Як зазначено вище, об'єктом вивчення в цьому курсі є симетричні шифросистеми (шифри), призначені для забезпечення конфіденційності повідомлень, що передаються відкритими каналами зв'язку. Для оцінювання чи обґрунтування стійкості таких шифросистем використовують їхні формальні означення або математичні моделі. Нижче розглядається одна з найпоширеніших моделей такого типу, запропонована в 1945 році К. Шенноном [2], яка називається алгебраїчною.

1.1. ОЗНАЧЕННЯ. *Алгебраїчною моделлю шифру* (або *шифром*) називається система

$$\mathcal{A} = (X, K, Y, f), \tag{1.1}$$

де X, K, Y – непорожні скінченні множини, $f : X \times K \to Y$ – відображення, що задовольняє такі умови:

а) f є сюр'єктивним, тобто для будь-якого $y \in Y$ існують елементи $x \in X$, $k \in K$ такі, що $f(x,k) = y$;

б) для будь-яких $k \in K$, $x_1, x_2 \in X$ справедлива імплікація

$$(x_1 \neq x_2) \Rightarrow (f(x_1,k) \neq f(x_2,k)).$$

Множини X, Y і K називають відповідно *множиною відкритих текстів, множиною шифрованих текстів* (*шифротекстів*) і *множиною ключів шифру* $\mathcal{A}$, а відображення f *– функцією шифрування*. Елементи множин X та Y називаються відповідно *відкритими* та *шифрованими текстами* (або *відкритими* та *шифрованими повідомленнями*), а елементи множини K *– ключами* шифру $\mathcal{A}$.

Говорять, що шифротекст $y \in Y$ *отримано шляхом зашифрування відкритого тексту* $x \in X$ *на ключі* $k \in K$, якщо виконується рівність

$$f(x,k) = y. \tag{1.2}$$

Співвідношення (1.2) називається *рівнянням зашифрування* для алгебраїчної моделі (1.1).

Неформально умова а) в 1.1 означає, що множина шифрованих текстів шифру $\mathcal{A}$ містить тільки ті повідомлення, які можуть бути отримані шляхом зашифрування будь-яких відкритих текстів на будь-яких ключах цього шифру. Дана умова забезпечує можливість розшифрування будь-якого шифротексту $y \in Y$ на деякому ключі $k \in K$ та називається *умовою можливості розшифрування.*

Умова б) в 1.1 може бути сформульована таким чином: в результаті зашифрування на будь-якому ключі $k \in K$ різних відкритих текстів $x_1, x_2 \in X$ отримуються різні шифровані тексти $y_1 = f(x_1,k)$, $y_2 = f(x_2,k)$. Іншими словами, для будь-якого ключа $k \in K$ та довільного шифротексту $y \in Y$ існує *не більше одного* відкритого тексту $x \in X$, результатом зашифрування якого на ключі k є шифротекст y.

Еквівалентне формулювання: для будь-яких $y \in Y$, $k \in K$ рівняння шифрування (1.2) має не більше одного розв'язку $x \in X$. Таким чином, умова б) гарантує однозначність розшифрування шифрованих повідомлень шифру $\mathcal{A}$ на ключах з множини K та називається *умовою однозначності розшифрування*.

Єдиний відкритий текст $x \in X$ (якщо він існує), який задовольняє рівняння (1.2), називається *відритим текстом, отриманим при розшифруванні шифротексту* y *на ключі* k, та позначається

$$x = k^{-1}y . \tag{1.3}$$

Співвідношення (1.3) називається *рівнянням розшифрування* для алгебраїчної моделі (1.1).

Надалі будемо іноді писати $y = kx$ замість $y = f(x,k)$. У такому випадку рівняння шифрування (1.2) можна записати у вигляді

$$kx = y . \tag{1.4}$$

Зауважимо, що рівності (1.3) та (1.4) є рівносильними. Кожне з них символічно виражає зазначений вище взаємозв'язок між відкритим текстом x та шифротекстом y, який полягає в тому, що x та y є результатами взаємних перетворень, що визначаються функцією шифрування f та ключем k шифру $\mathcal{A}$.

Нехай $\mathcal{A} = (X, K, Y, f)$ – довільний шифр. Для будь-якого ключа $k \in K$ задамо *часткову функцію* $f_k : X \to Y$ функції шифрування f, вважаючи $f_k(x) = f(x,k)$, $x \in X$.

1.2. ОЗНАЧЕННЯ. Функція f_k називається *шифрувальним перетворенням шифру* $\mathcal{A}$, *що відповідає ключу* $k \in K$.

Отже, шифр (1.1) являє собою набір $(f_k : k \in K)$ шифрувальних перетворень множини відритих повідомлень у множину шифрованих повідомлень. При цьому ключ k відіграє роль параметра, який однозначно визначає (фіксує) одне з шифрувальних перетворень даного шифру, а саме, перетворення f_k. Згідно з умовою б) означення 1.1, кожне шифрувальне перетворення є ін'єктивним відображенням множини X у множину Y.

Зауважимо, що у загальному випадку шифрувальні перетворення f_k та $f_{k'}$, які відповідають різним ключам k та k' шифру $\mathcal{A}$, можуть збігатися (саме тому говорять про набір, а не про множину шифрувальних перетворень).

1.3. ОЗНАЧЕННЯ. Ключі k та k' шифру $\mathcal{A}$ називаються (*криптографічно*) *еквівалентними*, якщо для кожного $x \in X$ справедлива рівність $f_k(x) = f_{k'}(x)$. У протилежному випадку зазначені ключі називаються *нееквівалентними*.

Отже, ключі k та k' є еквівалентними, якщо при зашифруванні на них будь-якого відкритого тесту отримуються однакові шифровані тексти. Криптографічно еквівалентні ключі є фактично нерозрізненними, оскільки збігаються шифрувальні перетворення, що їм відповідають.

Наявність малої кількості нееквівалентних ключів є суттєвою слабкістю шифру. Тому на практиці слушно розрізняти ключі лише з точністю до еквівалентності. Проте необхідно мати на увазі, що часто-густо повний опис класів еквівалентних ключів даного шифру (і навіть доведення існування або відсутності таких ключів) являє собою досить складну задачу.

З означення 1.1 випливає, що кожен шифр із заданими множиною відкритих текстів X, множиною ключів K та множиною шифрованих текстів Y однозначно визначається відображенням $f: X \times K \to Y$, яке задовольняє умови а), б). В свою чергу, таке відображення може бути задано за допомогою прямокутної таблиці, що складається з елементів множини Y, рядки якої занумеровані елементами множини K, а стовпці – елементами множини X (рис. 1.1). Навпаки, кожна така таблиця однозначно визначає відображення $f: X \times K \to Y$ за таким правилом: для будь-яких $x \in X$, $k \in K$ значення $f(x,k)$ дорівнює елементу $y \in Y$, розташованому в таблиці на перетинанні рядка з номером k та стовпця з номером x. Зрозуміло, що при цьому різні таблиці з елементами $y \in Y$ визначають різні відображення декартова добутку $X \times K$ у множину Y.

	…	x	…
…			
k	…	$f_k(x)$	…
…			

Рис. 1.1. Таблиця відображення $f: X \times K \to Y$

Табличний спосіб задання відображень надає змогу наочно описати функції шифрування, тобто такі відображення $f: X \times K \to Y$, що задовольняють умови а), б) означення 1.1.

Позначимо символом $\mathrm{T}(f)$ таблицю, що відповідає довільному відображенню f множини $X \times K$ у множину Y. Безпосередньо з умов а) та б) випливає таке твердження.

1.4. ТВЕРДЖЕННЯ. Відображення $f : X \times K \to Y$ є функцією шифрування деякого шифру з множиною відкритих текстів X, множиною ключів K та множиною шифрованих текстів Y тоді й тільки тоді, коли виконуються умови

а′) у таблиці $\mathrm{T}(f)$ містяться всі елементи множини Y;

б′) елементи кожного рядка таблиці $\mathrm{T}(f)$ є попарно різними. ►

Отже, довільний шифр $\mathcal{A}$ вигляду (1.1) з функцією шифрування f можна однозначно визначити за допомогою таблиці $\mathrm{T}(f)$, яка задовольняє умови а′), б′). При цьому для будь-яких $x \in X$, $k \in K$ шифрований тест $y = kx$, що отримується шляхом зашифрування відкритого тексту x на ключі k, міститься в таблиці $\mathrm{T}(f)$ на перетинанні рядка з номером k та стовпця з номером x. Таблиця $\mathrm{T}(f)$ називається *таблицею шифрування шифру* $\mathcal{A}$ і позначається символом $\mathrm{T}(\mathcal{A})$.

Рядки таблиці шифрування будь-якого шифру мають просту та наочну інтерпретацію. Дійсно, на підставі означення 1.2 для будь-якого ключа $k \in K$ рядок з номером k таблиці $\mathrm{T}(\mathcal{A})$ дорівнює вектору значень шифрувального перетворення f_k. Звідси випливає, зокрема, що ключі k та k' шифру A є еквівалентними тоді й тільки тоді, коли відповідні їм рядки таблиці шифрування $\mathrm{T}(\mathcal{A})$ збігаються.

§ 1.3. Ендоморфні, транзитивні та регулярні шифри

Покажемо, що кількість відкритих повідомлень довільного шифру не перевищує кількості його шифрованих повідомлень.

1.5. ТВЕРДЖЕННЯ. Для будь-якого шифру $\mathcal{A}$ вигляду (1.1) справедлива нерівність

$$|X| \le |Y|. \tag{1.5}$$

◄ На підставі умови б′) означення 1.1 в кожному рядку таблиці шифрування шифру $\mathcal{A}$ знаходиться $|X|$ різних елементів множини Y. Отже, множина Y має не менш ніж $|X|$ елементів, тобто виконується нерівність (1.5). ►

Зауважимо, що у загальному випадку знак нерівності в (1.5) є строгим. Однак з практичного погляду викликають інтерес такі шифри, множини відкритих та шифрованих повідомлень яких мають однакову потужність. Це пояснюється тим, що на практиці зростання числа можливих шифрованих повідомлень тягне за собою збільшення їхньої довжини, що знижує швидкість передачі даних. Крім того, часто-густо потрібну стійкість шифрування можна забезпечити й без додаткового збільшення кількості шифрованих повідомлень.

1.6. ОЗНАЧЕННЯ. Шифр $\mathcal{A}$ вигляду (1.1) називається *ендоморфним*, якщо множини його відкритих та шифрованих повідомлень збігаються, тобто виконується рівність $X = Y$. За умови

$$|X| = |Y| \tag{1.6}$$

шифр $\mathcal{A}$ називається *майже ендоморфним*.

Поняття ендоморфного шифру введено К. Шенноном [2].

Розглянемо докладніше будову майже ендоморфних шифрів. Нехай $\mathcal{A} = (X, K, Y, f)$ є таким шифром. Внаслідок рівності (1.6) існує бієктивне

відображення $h: Y \to X$. Визначимо новий шифр $\mathcal{A}_h = (X, K, X, h \circ f)$, множини відкритих і шифрованих текстів якого збігаються, а функція шифрування дорівнює композиції відображень f та h, що визначається за формулою $(h \circ f)(x,k) = h(f(x,k))$, $x \in X$, $k \in K$. (Читачеві рекомендується самостійно перевірити, що побудована система $\mathcal{A}_h$ задовольняє умови а), б) означення 1.1, тобто дійсно є шифром).

Шифри $\mathcal{A}$ та $\mathcal{A}_h$ називаються *подібними*. Зазвичай такі шифри мають однакові властивості, що дозволяє, у певному сенсі, не розрізняти їх та вивчати лише один з них.

Отже, при дослідженні властивостей маже ендоморфного шифру $\mathcal{A}$ здебільшого вважають, що множини відкритих та шифрованих повідомлень цього шифру збігаються. Таке припущення іноді надає змогу уникнути деяких формальних труднощів, пов'язаних з аналізом властивостей майже ендоморфних шифрів. Зокрема, за умови $X = Y$ шифрувальні перетворення шифру (1.1) є підстановками на множині X, що дає можливість використовувати операцію композиції підстановок. Проте слід зазначити, що хоча з теоретичної точки зору заміна майже ендоморфного шифру $\mathcal{A}$ подібним йому шифром $\mathcal{A}_h$ є зазвичай припустимою, реалізувати таку заміну на практиці може виявитися складно.

Перейдемо до вивчення найважливіших класів алгебраїчних моделей шифрів.

1.7 ОЗНАЧЕННЯ. Шифр вигляду (1.1) називається *транзитивним*, якщо для будь-яких $x \in X$, $y \in Y$ існує ключ $k \in K$ такий, що $kx = y$.

Як випливає з означення 1.7, транзитивні шифри (і тільки вони) володіють такою важливою властивістю: *для будь-якого шифротексту $y \in Y$ множина повідомлень, що отримуються при розшифруванні y на*

усіх ключах $k \in K$, *містить усі відкриті тексти*. Зазначена властивість є вкрай бажаною для розробників шифросистем. Дійсно, якщо $\mathcal{A}$ – транзитивний шифр, а y – шифрований текст, отриманий в результаті зашифрування деякого відкритого тексту x на ключі k, то визначити x за y без знання k є принципово неможливим (у рамках алгебраїчного підходу до криптоаналізу шифру $\mathcal{A}$ на основі єдиного відомого шифрованого тексту), оскільки в результаті розшифрування повідомлення y на усіх ключах шифру $\mathcal{A}$ отримуються всі можливі відкриті повідомлення. При цьому жодному з них (без додаткової інформації про x або k) не можна віддати будь-яку перевагу перед іншим повідомленням.

Безпосередньо з означення 1.7 випливає наступний критерій транзитивності шифру.

1.8. ТВЕРДЖЕННЯ. Шифр $\mathcal{A}$ є транзитивним тоді й тільки тоді, коли у кожному стовпці таблиці шифрування $\mathrm{T}(A)$ містяться всі шифровані повідомлення (елементи множини Y). ►

Оскільки довжина стовпців таблиці $\mathrm{T}(A)$ дорівнює числу ключів шифру $\mathcal{A}$, то з твердження 1.7 випливає такий результат.

1.9. НАСЛІДОК. Для будь-якого транзитивного шифру $\mathcal{A}$ вигляду (1.1) виконується нерівність

$$|Y| \le |K|. \blacktriangleright \qquad (1.7)$$

Таким чином, на підставі нерівностей (1.5) та (1.7) *довжина ключа будь-якого транзитивного шифру є не менше довжини відкритого повідомлення*. Зазначена властивість транзитивних шифрів істотно обмежує їхнє практичне використання в системах зв'язку з великою кількістю або-

нентів або великим обсягом інформації, що передається. Значні витрати, пов'язані із створенням, зберіганням та розподілом великої кількості ключів захищеними каналами зв'язку, роблять використання транзитивних шифрів у сучасних інформаційних системах дуже дорогим та непрактичним. Бажання мінімізувати кількість ключів шифру (за умовою зберігання потрібної криптографічної стійкості) приводить до наступних понять.

1.10. ОЗНАЧЕННЯ. Шифр вигляду (1.1) називається *регулярним*, якщо для будь-яких $x \in X$, $y \in Y$ існує не більш одного ключа $k \in K$ такого, що $kx = y$. Транзитивний та регулярний шифр називається *мінімальним.*

1.11. ТВЕРДЖЕННЯ. Для будь-якого шифру $\mathcal{A}$ є еквівалентними такі твердження:

(а) $\mathcal{A}$ – регулярний шифр;

(б) елементи будь-якого стовпця таблиці шифрування шифру $\mathcal{A}$ є попарно різними;

(в) при розшифруванні будь-якого шифротексту $y \in Y$ на різних ключах отримуються різні відкриті тексти.

◄ (а) $\Rightarrow$ (б). Припустимо, що деякий стовпець з номером $x \in X$ таблиці $\mathrm{T}(\mathcal{A})$ містить однакові шифротексти (які дорівнюють y) в рядках з номерами k_1 та k_2, де $k_1 \neq k_2$. Тоді на підставі рівностей $k_1 x = k_2 x = y$ існує принаймні два різних ключі (k_1 та k_2), які перетворюють відкритий текст x у шифрований текст y, що суперечить регулярності шифру $\mathcal{A}$.

(б) $\Rightarrow$ (в). Припустимо протилежне: існують шифротекст $y \in Y$ та різні ключі k_1, k_2 шифру $\mathcal{A}$ такі, що $(k_1)^{-1} y = (k_2)^{-1} y = x$. Тоді елементи стовпця з номером x таблиці $\mathrm{T}(\mathcal{A})$, що знаходяться в рядках з номерами k_1 та k_2, дорівнюють y. Отже, отримано протиріччя з твердженням (б).

(в) $\Rightarrow$ (а). Аналогічно попередньому: якщо шифр $\mathcal{A}$ не є регулярним, то існують елементи $x \in X$, $y \in Y$, $k_1, k_2 \in K$ такі, що $k_1 \neq k_2$ та $k_1 x = k_2 x = y$. Отже, мають місце рівності $(k_1)^{-1} y = (k_2)^{-1} y = x$, які суперечать твердженню (в). ►

З умови (в) твердження 1.11 випливає, зокрема, що кількість ключів регулярного шифру не перевищує кількості відкритих повідомлень.

1.12. НАСЛІДОК. Для будь-якого регулярного шифру $\mathcal{A}$ вигляду (1.1) справедлива нерівність

$$|K| \leq |X|. \blacktriangleright \tag{1.8}$$

Поєднуючи твердження наслідків 1.9 та 1.12, отримаємо такий результат.

1.13. НАСЛІДОК. Для будь-якого мінімального шифру $\mathcal{A} = (X, K, Y, f)$ виконуються рівності

$$|K| = |X| = |Y|. \blacktriangleright \tag{1.9}$$

Встановимо зараз необхідні та достатні умови, за якими шифр $\mathcal{A}$ є мінімальним. Як показує наступне твердження, мінімальні шифри можуть бути охарактеризовані як транзитивні шифри з найменшим (або як регулярні шифри з найбільшим) можливим числом ключів.

1.14. ТВЕРДЖЕННЯ. Для будь-якого шифру $\mathcal{A} = (X, K, Y, f)$ є еквівалентними такі твердження:

(а) $\mathcal{A}$ – мінімальний шифр;

(б) $\mathcal{A}$ – транзитивний шифр, що задовольняє умову (1.9);

(в) $\mathcal{A}$ – регулярний шифр, що задовольняє умову (1.9).

◄ Імплікації (а) $\Rightarrow$ (б), (а) $\Rightarrow$ (в) випливають безпосередньо з означення мінімального шифру та наслідку 1.13.

Покажемо, що (б) $\Rightarrow$ (а). На підставі рівності (1.9) і транзитивності шифру $\mathcal{A}$ кожен стовпець таблиці $\mathrm{T}(\mathcal{A})$ містить $|K|=|Y|$ шифрованих повідомлень, серед яких знаходяться всі елементи множини Y. Отже, елементи будь-якого стовпця таблиці $\mathrm{T}(\mathcal{A})$ є попарно різними, що на підставі твердження 1.11 тягне регулярність шифру $\mathcal{A}$. Таким чином, $\mathcal{A}$ є мінімальним шифром, що й треба було довести.

Справжність імплікації (в) $\Rightarrow$ (а) доводиться аналогічно. ►

Властивість мінімальності шифру є прикладом певного компромісу між його високою стійкістю (в даному випадку – транзитивністю) та практичністю (відповідно – регулярністю). На сьогодні мінімальні шифри використовуються для задання *законів накладання гами* в алгоритмах потокового шифрування. Добре відомими прикладами мінімальних шифрів є шифри Цезаря та Віженера.

Як випливає з тверджень 1.4, 1.11 та 1.14, квадратна таблиця розміру $n\times n$ з елементами $0,1,...,n-1$ є таблицею шифрування мінімального шифру тоді й тільки тоді, коли елементи кожного її рядка та, відповідно, кожного її стовпця є попарно різними. Такі таблиці отримали спеціальну назву.

1.15. ОЗНАЧЕННЯ. Прямокутна таблиця розміру $k\times n$, що складається з елементів скінченної множини потужності n, називається *латинським прямокутником*, якщо в кожному рядку та в кожному стовпці цієї таблиці містяться попарно різні елементи. За умови $k=n$ латинський прямокутник називається *латинським квадратом*.

Отже, на підставі тверджень 1.4, 1.11, 1.14 таблиця шифрування регулярного ендоморфного шифру є латинським прямокутником, а таблиця шифрування мінімального ендоморфного шифру – латинським квадратом.

§ 1.4. Параметри, що характеризують криптографічні властивості булевих відображень

Для побудови сучасних потокових та блокових шифрів здебільшого використовують допоміжні відображення, що є (векторними) булевими функціями. Відзначимо, наприклад, функції ускладнення генераторів гами та підстановки (вузли заміни або s-блоки), які застосовуються в алгоритмах блокового шифрування. Криптографічні властивості булевих відображень характеризуються низкою числових параметрів, означення яких наведені нижче.

Для будь-якого натурального n позначимо V_n множину двійкових векторів довжини n.

1.16. ОЗНАЧЕННЯ. Відображення $f: V_n \to \{0,1\}$ називається *булевою функцією від n змінних*, а відображення $f: V_n \to V_m$, де $m > 1$, – *векторною булевою функцією*.

Зазвичай відображення $f: V_n \to V_m$ задається за допомогою таблиці (рис. 1.2). Для будь-якого $x \in V_n$ значення $f(x)$ є двійковим вектором довжини m. Позначаючи $f_i(x)$ i-у координату цього вектора, $i \in \overline{1,m}$, отримаємо m булевих функцій $f_1,..., f_m$, які називаються *координатними функціями* відображення f. Це відображення записують у вигляді $f = (f_1,..., f_m)$. Таким чином, дослідження відображення (векторної функ-

ції) f зводиться до вивчення властивостей звичайних (не векторних) булевих функцій $f_1,..., f_m$.

$x = (x_1,..., x_n)$	$f(x) = f(x_1,..., x_n)$
(0, …, 0, 0)	f(0, ..., 0, 0)
(0, …, 0, 1)	f(0, ..., 0, 1)
.	.
.	.
.	.
(1, …,1, 0)	f(1, ..., 1, 0)
(1, …,1, 1)	f(1, ..., 1, 1)

Рис. 1.2. Таблиця відображення f

Найважливішими криптографічними параметрами булевих функцій є *метричні параметри* (зокрема, вага функції та її нелінійність), а також *алгебраїчні параметри* (зокрема, алгебраїчний степінь функції).

1.17. ОЗНАЧЕННЯ *Відстанню* (*Геммінга*) *між векторами* $x = (x_1,..., x_n),\ y = (y_1,..., y_n) \in V_n$ називається число

$$d(x, y) = |\{i \in \overline{1, n} : x_i \neq y_i\}|.$$

Вага вектора $x \in V_n$ визначається як відстань між ним та нульовим вектором довжини n і позначається $\| x \|$ або $wt(x)$.

Відстань між функціями $f, g : V_n \to \{0,1\}$ визначається як відстань між векторами їхніх значень: $d(f, g) = |\{x \in V_n : f(x) \neq g(x)\}|$.

Вагою $\| f \|$ (або $wt(f)$) функції f називається число одиниць у векторі її значень. Справедлива рівність $d(f, g) = \| f \oplus g \|$.

Функція f від n змінних називається *зрівноваженою* (або *збалансованою*), якщо її вага дорівнює 2^{n-1}.

1.18. ОЗНАЧЕННЯ Булева функція вигляду

$$l(x_1,...,x_n) = a_1x_1 \oplus ... \oplus a_nx_n \oplus a_0, \qquad (1.10)$$

де $a_0, a_1,..., a_n \in \{0,1\}$, називається *афінною*. Якщо при цьому $a_0 = 0$, то афінна функція називається *лінійною*.

1.19. ОЗНАЧЕННЯ. *Нелінійність* функції $f : V_n \to \{0,1\}$ визначається як відстань від f до множини афінних функцій:

$$N_f = \min\{ d(f,l) : l \in A_n \},$$

де A_n – множина усіх функцій вигляду (1.10).

Афінні булеві функції мають дуже просту аналітичну будову та передбачувані властивості. Окрім того, системи лінійних булевих рівнянь (на відміну від систем нелінійних, зокрема, квадратичних рівнянь) розв'язуються за поліноміальний час. Тому афінні функції є найслабкішими в криптографічному сенсі. Отже, якісна криптографічна функція повинна бути достатньо далекою від афінних, тобто мати достатньо високу нелінійність. Крім того, така функція повинна бути збалансованою (див. задачу 8).

1.20. ОЗНАЧЕННЯ. *Поліномом Жегалкіна* (чи *алгебраїчною нормальною формою*) називається поліном вигляду

$$P(x_1,...,x_n) = \bigoplus_{\alpha \in V_n} c_\alpha x^\alpha, \qquad (1.11)$$

де $c_\alpha \in \{0,1\}$, $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ для будь-якого $\alpha = (\alpha_1,...,\alpha_n) \in V_n$.

Іншими словами, поліном Жегалкіна – це такий поліном над полем з двох елементів, у вираз якого кожна змінна входить з показником степеня не вище за 1.

1.21. ТВЕРДЖЕННЯ. Для кожної булевої функції від n змінних існує єдиний поліном Жегалкіна, що представляє цю функцію.

◄ Індукція за n. Якщо $n=1$, то кожна з чотирьох функцій від однієї змінної ($0, 1, x, \bar{x} = x \oplus 1$) задається поліномом Жегалкіна. Індуктивний перехід від $n-1$ до n випливає з рівності

$$f(x_1, x_2, ..., x_n) = x_1 f(1, x_2, ..., x_n) \oplus (x_1 \oplus 1) f(0, x_2, ..., x_n) .$$

Нарешті, єдиність полінома Жегалкіна для кожної булевої функції випливає з того, що число таких поліномів дорівнює числу функцій від n змінних, а саме 2^{2^n} .►

1.22. ПРИКЛАД. Наведемо поліноми Жегалкіна для деяких булевих функцій:

1) константи 0, 1;

2) додавання за модулем 2: $\mathrm{XOR}(x, y) = x \oplus y$;

3) кон'юнкція: $x \wedge y = xy$;

4) диз'юнкція: $x \vee y = xy \oplus x \oplus y$;

5) заперечення $\bar{x} = x \oplus 1$.

1.23. ОЗНАЧЕННЯ. *Степенем монома* $x^{\alpha} = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ називається вага вектора $\alpha = (\alpha_1, ..., \alpha_n) \in V_n$. *Степінь полінома* (1.11) визначається як максимальний степінь мономів, що входять у вираз цього полінома:

$$\deg P = \max\{\| \alpha \| : c_{\alpha} = 1\} .$$

1.24. ОЗНАЧЕННЯ. (*Алгебраїчний*) *степінь* $\deg f$ (або *степінь нелінійності*) ненульової функції $f : V_n \to \{0,1\}$ визначається як степінь її полінома Жегалкіна.

На підставі означення 1.18 степінь афінної функції не перевищує 1. З алгебраїчного погляду, булеві функції, віддалені від афінних, можна охарактеризувати як такі, що мають достатньо великий степінь.

Розглянемо зараз найважливіші криптографічні параметри підстановок на множині V_n.

Нехай $s = (s_1,...,s_n)$ – підстановка (s-блок; s-box) з координатними функціями $s_1,...,s_n : V_n \to \{0,1\}$.

1.25. ОЗНАЧЕННЯ. *Компонентою, що відповідає вектору* $\alpha = (\alpha_1,...,\alpha_n) \in V_n \setminus \{0\}$, *підстановки* s називається функція

$$\alpha s(x) = \alpha_1 s_1(x) \oplus ... \oplus \alpha_n s_n(x), \ x \in V_n.$$

Всього існує $2^n - 1$ (не обов'язково різних) компонент підстановки s.

1.26. ОЗНАЧЕННЯ. *Нелінійність* N_s (*степінь* $\deg s$) *підстановки* s визначається як мінімальна нелінійність (мінімальний степінь) її компонент.

1.27. ОЗНАЧЕННЯ. *Таблиця різниць* і *таблиця лінійних апроксимацій* підстановки $s : V_n \to V_n$ визначаються як квадратні матриці з елементами

$$d_s(\alpha,\beta) = 2^{-n} \left| \{x \in V_n : s(x \oplus \alpha) \oplus s(x) = \beta\} \right|, \ \alpha,\beta \in V_n \qquad (1.12)$$

та

$$l_s(\alpha,\beta)=\left(2^{-n}\sum_{x\in V_n}(-1)^{\alpha x\oplus\beta s(x)}\right)^2,\ \alpha,\beta\in V_n \qquad (1.13)$$

відповідно. *Максимальні елементи таблиці різниць* і *таблиці лінійних апроксимацій* визначається, відповідно, за формулами

$$d_{\max}(s)=\max\{d_s(\alpha,\beta):\alpha,\beta\in V_n\setminus\{0\}\}, \qquad (1.14)$$

$$l_{\max}(s)=\max\{l_s(\alpha,\beta):\alpha,\beta\in V_n\setminus\{0\}\}. \qquad (1.15)$$

Найважливіші криптографічні вимоги до підстановок на множині V_n можна сформулювати таким чином: якісна у криптографічному сенсі підстановка повинна мати достатньо великий алгебраїчний степінь (для протидії алгебраїчним атакам), достатньо велику нелінійність або достатньо малий максимальний елемент таблиці лінійних апроксимацій (для протидії лінійному методу криптоаналізу), а також достатньо малий максимальний елемент таблиці різниць (для протидії різницевому методу криптоаналізу; див. нижче § 2.4, 2.5).

1.28. ПРИКЛАД. Підстановка Ніберг [3] визначається за формулою $\sigma(x)=x^{-1}$, $x\in\mathbf{GF}(2^8)\setminus\{0\}$; $\sigma(0)=0$ (при цьому елементи поля $\mathbf{GF}(2^8)$ звичайним чином ототожнюються з двійковими векторами довжини 8). Вона широко використовується в сучасних алгоритмах блокового шифрування та має параметри $d_{\max}(\sigma)=l_{\max}(\sigma)=2^{-6}$, $\deg s=7$, які є оптимальними серед усіх підстановок на множині V_8.

§ 1.5. Швидкий алгоритм побудови полінома Жегалкіна за вектором значень булевої функції

Для дослідження криптографічних властивостей булевих функцій та підстановок, що використовуються при побудові симетричних шифросистем, потрібні ефективні за трудомісткістю алгоритми обчислення наведених вище параметрів. В цьому параграфі представлений один з таких алгоритмів.

Для його викладення сформулюємо додаткові поняття та результати.

1.29. ОЗНАЧЕННЯ. Нехай $A=(a_{ij})$ та $B=(b_{kl})$ – квадратні матриці над полем F розміру $m\times m$ та $n\times n$ відповідно, $i,j\in\overline{1,m}$, $k,l\in\overline{1,n}$. *Тензорним* (або *кронекеровим*) *добутком матриці* A *на матрицю* B називається матриця $A\otimes B=(a_{ij}b_{kl})$ порядку mn, що складається зі всіх можливих добутків елементів матриці A на елементи матриці B.

Матрицю $A\otimes B$ можна записати у вигляді

$$A\otimes B=\begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1m}B \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1}B & a_{m1}B & \cdots & a_{mm}B \end{pmatrix},$$

де $a_{ij}B$ є результатом множення всіх елементів матриці B на елемент a_{ij}, $i,j\in\overline{1,m}$.

Операція тензорного добутку має такі властивості:

$$(A+B)\otimes C=A\otimes C+B\otimes C,\ C\otimes(A+B)=C\otimes A+C\otimes B,$$

$$(A\otimes B)\otimes C = A\otimes(B\otimes C),\ (A\otimes B)(C\otimes D) = AC\otimes BD,$$

перевірка яких здійснюється безпосередньо, виходячи з означення 1.29 Тут A, B, C і D позначають довільні квадратні матриці над полем F, для яких мають сенс вирази в обох частинах наведених рівностей.

З останньої рівності випливає, зокрема, що матриця $A\otimes B$ є оборотною тоді й тільки тоді, коли є оборотною кожна з матриць A і B. При цьому виконується рівність

$$(A\otimes B)^{-1} = A^{-1}\otimes B^{-1}. \qquad (1.16)$$

Асоціативність операції тензорного добутку надає змогу звичайним чином ввести поняття *n-го тензорного степеня* $A^{[n]}$ довільної квадратної матриці A:

$$A^{[n]} = \underbrace{A\otimes A\otimes\ldots\otimes A}_{n},\ n = 1,2,\ldots.$$

Зауважимо, що на підставі рівності (1.16) тензорний степінь оборотної матриці A є оборотною матрицею. При цьому

$$\left(A^{[n]}\right)^{-1} = \left(A^{-1}\right)^{[n]},\ n = 1,2,\ldots. \qquad (1.17)$$

Нехай $f = f(x_1,\ldots,x_n)$ – булева функція від n змінних. Позначимо $T_f = (f(x))_{x\in V_n}$ і $P_f = (p_\alpha^f)_{\alpha\in V_n}$ відповідно вектор значень і вектор коефіцієнтів полінома Жегалкіна функції f. Далі розглядатимемо ці вектори

як булеві матриці розміру $2^n \times 1$, тобто вектор-стовпці довжини 2^n над полем з двох елементів.

Розглянемо булеву матрицю другого порядку

$$C = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Помітимо, що ця матриця є оборотною над полем $\mathbf{GF}(2)$, і обернена до неї матриця збігається з нею самою:

$$C^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

1.30. ТВЕРДЖЕННЯ. Для будь-якої булевої функції $f = f(x_1,...,x_n)$ мають місце такі рівності матриць над полем з двох елементів:

$$P_f = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{[n]} T_f, \qquad (1.18)$$

$$T_f = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{[n]} P_f. \qquad (1.19)$$

◄ Доведемо рівність (1.18), використовуючи індукцію за n (рівність (1.19) є безпосереднім наслідком попередньої).

Нехай $n=1$ і $f(x_1)$ – булева функція від однієї змінної. Позначимо $f_0 = f(0)$, $f_1 = f(1)$. Справедлива рівність $f(x_1) = x_1(f_1 \oplus f_0) \oplus f_0$, з якої

випливає, що коефіцієнти полінома Жегалкіна функції f визначаються за формулами $p_1^f = f_1 \oplus f_0$, $p_0^f = f_0$. Таким чином,

$$P_f = \begin{pmatrix} p_0^f \\ p_1^f \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} f_0 \\ f_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} T_f ,$$

і, отже, при $n=1$ рівність (1.18) доведено.

Припустимо зараз, що ця рівність виконується для будь-якої булевої функції від $n-1$ змінних та доведемо її для булевих функцій від n змінних.

Розглянемо довільну функцію $f = f(x_1,...,x_n)$ та позначимо

$$f_0(x_2,...,x_n) = f(0, x_2,...,x_n),\ (x_2,...,x_n) \in V_{n-1},$$

$$f_1(x_2,...,x_n) = f(1, x_2,...,x_n),\ (x_2,...,x_n) \in V_{n-1}.$$

Нехай $P_0(x_2,...,x_n)$ – поліном Жегалкіна функції f_0, $P_1(x_2,...,x_n)$ – поліном Жегалкіна функції f_1. Тоді виконується рівність

$$P_f(x_1,...,x_n) = x_1(P_1(x_2,...,x_n) \oplus P_0(x_2,...,x_n)) \oplus P_0(x_2,...,x_n),$$

з якої випливає таке співвідношення, що пов'язує вектор P_f коефіцієнтів полінома Жегалкіна функції f з векторами P_{f_0}, P_{f_1} коефіцієнтів поліномів Жегалкіна її компонент:

$$P_f = \begin{pmatrix} P_{f_0} \\ P_{f_1} \oplus P_{f_0} \end{pmatrix}. \qquad (1.20)$$

Далі, за припущенням індукції

$$P_{f_0} = C^{[n-1]} T_{f_0},\ P_{f_1} = C^{[n-1]} T_{f_1}. \qquad (1.21)$$

Таким чином, на підставі рівностей (1.20), (1.21) та означення тензорного степеня матриці мають місце співвідношення

$$P_f = \begin{pmatrix} C^{[n-1]} T_{f_0} \\ C^{[n-1]} T_{f_1} \oplus C^{[n-1]} T_{f_0} \end{pmatrix} = \begin{pmatrix} C^{[n-1]} & 0 \\ C^{[n-1]} & C^{[n-1]} \end{pmatrix} \begin{pmatrix} T_{f_0} \\ T_{f_1} \end{pmatrix} =$$

$$= \left(\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \otimes C^{[n-1]} \right) \begin{pmatrix} T_{f_0} \\ T_{f_1} \end{pmatrix} = C^{[n]} \begin{pmatrix} T_{f_0} \\ T_{f_1} \end{pmatrix} = C^{[n]} T_f,$$

які встановлюють справедливість рівності (1.18) для функції f. ►

Зауважимо, що отримані співвідношення (1.18), (1.19) можна безпосередньо використовувати для знаходження полінома Жегалкіна булевої функції за її таблицею істинності або для обчислення значень функції за коефіцієнтами її полінома Жегалкіна.

1.31. ПРИКЛАД. Знайдемо поліном Жегалкіна функції $f(x_1, x_2, x_3)$, яка задається вектором значень $T_f = (10110110)^T$ (тут і далі символ T позначає операцію транспонування матриці).

Перш за все, знайдемо 3-й тензорний степінь матриці C:

$$C^{[2]} = \begin{pmatrix} C & 0 \\ C & C \end{pmatrix} = \begin{pmatrix} 1\,0\,0\,0 \\ 1\,1\,0\,0 \\ 1\,0\,1\,0 \\ 1\,1\,1\,1 \end{pmatrix},$$

$$C^{[3]} = \begin{pmatrix} C^{[2]} & 0 \\ C^{[2]} & C^{[2]} \end{pmatrix} = \begin{pmatrix} 1\,0\,0\,0\,0\,0\,0\,0 \\ 1\,1\,0\,0\;\;0\,0\,0\,0 \\ 1\,0\,1\,0\;\;0\,0\,0\,0 \\ 1\,1\,1\;\;1\;\;0\,0\,0\,0 \\ 1\,0\,0\,0\;\;1\,0\,0\,0 \\ 1\,1\,0\,0\;\;\;1\,1\,0\,0 \\ 1\,0\,1\,0\;\;\;1\,0\,1\,0 \\ 1\,1\,1\;\;1\;\;\;1\,1\;\;1\,1 \end{pmatrix}. \qquad (1.22)$$

Тепер, виконуючи множення вектор-стовпця значень функції f на матрицю (1.22) (всі обчислення виконуються в полі $\mathbf{GF}(2)$), на підставі формули (1.18) отримаємо вектор коефіцієнтів полінома Жегалкіна заданої функції: $P_f = (1\,1\,0\,1\,1\,0\,1\,1)^T$.

Таким чином, поліном Жегалкіна функції f дорівнює $P_f(x_1, x_2, x_3) = 1 \oplus x_3 \oplus x_2x_3 \oplus x_1 \oplus x_1x_2 \oplus x_1x_2x_3$. ►

Зауважимо, що для обчислення вектора P_f за формулою (1.18) необхідно виконати $2^n(2^{n+1}-1)$ додавань чи множень в полі $\mathbf{GF}(2)$ (матриця $C^{[n]}$ має 2^n рядків і для множення кожної з них на вектор-стовпець T_f потрібно виконати 2^n множень і $2^n - 1$ додавань за модулем 2). Крім того, треба виділити 4^n бітів пам'яті для зберігання елементів матриці $C^{[n]}$.

Поряд з тим, існує більш ефективний, *швидкий алгоритм знаходження вектора коефіцієнтів полінома Жегалкіна булевої функції, заданої вектором значень*. Цей алгоритм не потребує пам'яті для зберігання матриці $C^{[n]}$ і надає змогу обчислювати вектор P_f з використанням тільки $n2^{n-1}$ операцій додавання за модулем 2.

Алгоритм полягає в застосуванні до вхідного вектора $T = T_f$ рекурсивної *процедури* $\Lambda(n)$, яка має такий вигляд.

Вхід: булев вектор-стовпець $T = (T_0, T_1)$, де $T_0, T_1 \in V_{2^{n-1}}$.

Вихід: булев вектор-стовпець $P = C^{[n]}T$.

Алгоритм обчислення.

Якщо $n = 1$, то вважаємо

$$P_0 = T_0,\ P_1 = T_0 \oplus T_1,\ P = (P_0, P_1). \tag{1.23}$$

Якщо $n \geq 2$, то обчислюємо вектори P_0 та P_1, застосовуючи процедуру $\Lambda(n-1)$ до векторів T_0 та $T_0 \oplus T_1$ відповідно. Далі записуємо шуканий вектор P у вигляді $P = (P_0, P_1)$.

Зауважимо, що в результаті застосування описаної процедури до вектора значень функції f дійсно отримується вектор коефіцієнтів її полінома Жегалкіна. Це випливає безпосередньо з рівності (1.18) та співвідношень

$$C^{[n]}T = \begin{pmatrix} C^{[n-1]} & 0 \\ C^{[n-1]} & C^{[n-1]} \end{pmatrix} \begin{pmatrix} T_0 \\ T_1 \end{pmatrix} = \begin{pmatrix} C^{[n-1]}T_0 \\ C^{[n-1]}(T_0 \oplus T_1) \end{pmatrix}. \tag{1.24}$$

Отже, на підставі рівностей (1.24) для обчислення вектора $P = C^{[n]}T$ за допомогою процедури $\Lambda(n)$ вхідний вектор T "розбивається" на дві "половини" T_0, T_1, після чого до кожного з векторів T_0, $T_0 \oplus T_1$ застосовується аналогічна процедура $\Lambda(n-1)$. В результаті отримуються "половини" $P_0 = C^{[n-1]}T_0$ і $P_1 = C^{[n-1]}(T_0 \oplus T_1)$ шуканого вектора P. Подібний метод розв'язання обчислювальних задач відомий під назвою "розділяй і володарюй". При його застосуванні вхідна задача "розбивається" на підзадачі, кожна з яких являє собою її зменшену версію. Далі ці підзадачі розв'язуються аналогічно шляхом "розбиття" їх на ще менші підзадачі, з розв'язків яких у підсумку формується розв'язок вхідної задачі. Переважно метод "розділяй і володарюй" приводить до ефективних (швидких) обчислювальних алгоритмів. Переконаємося в цьому, оцінивши трудомісткість описаної вище процедури $\Lambda(n)$.

Позначимо $t(n)$ число операцій додавання за модулем 2, що виконуються при обчисленні вектора коефіцієнтів полінома Жегалкіна за вектором значень булевої функції $f = f(x_1,...,x_n)$ з використанням швидкого алгоритму.

1.32. ТВЕРДЖЕННЯ. Для будь-якого натурального n виконується рівність

$$t(n) = 2^{n-1}n. \qquad (1.25)$$

◄ Отримаємо рекурентне співвідношення для чисел $t(n)$, $n = 1, 2, \ldots$.

Згідно з рівностями (1.23) при $n = 1$ для знаходження вектора P достатньо обчислити суму $P_1 = T_0 \oplus T_1$, де $T_0, T_1 \in V_1$. Отже,

$$t(1) = 1. \qquad (1.26)$$

Далі, при $n \geq 2$ для обчислення вектора P за допомогою процедури $\Lambda(n)$ необхідно виконати 2^{n-1} операцій додавання за модулем 2 (при знаходженні суми $T_0 \oplus T_1$, де $T_0, T_1 \in V_{n-1}$) і ще $2t(n-1)$ таких операцій (при застосуванні процедури $\Lambda(n-1)$ до векторів T_0 і $T_0 \oplus T_1$).

Таким чином,

$$t(n) = 2^{n-1} + 2t(n-1), \; n = 2, 3, \ldots. \qquad (1.27)$$

Позначимо $\tau(n) = 2^{-n} t(n)$, $n = 1, 2, \ldots$. На підставі формул (1.26), (1.27) мають місце рівності

$$\tau(1) = 1/2, \;\; \tau(n) = 1/2 + \tau(n-1), \; n = 2, 3, \ldots,$$

з яких випливає, що $\tau(n) = n/2$ для будь-якого натурального n. Отже, $t(n) = 2^n \tau(n) = n 2^{n-1}$, що й треба було довести. ►

1.33. ПРИКЛАД. Обчислимо коефіцієнти полінома Жегалкіна функції f з вектором значень $T_f = (10110110)^T$ за допомогою швидкого алгоритму.

На першому кроці обчислень "розбиваємо" вектор $T_f = (1\ 0\ 1\ 1\ 0\ 1\ 1\ 0)^T$ на дві "половини" $T_0 = (1\ 0\ 1\ 1)^T$, $T_1 = (0\ 1\ 1\ 0)^T$ та знаходимо вектор $T_2 = T_0 \oplus T_1 = (1\ 1\ 0\ 1)^T$.

Далі, на другому кроці застосовуємо до кожного з векторів T_0, T_2 процедуру $\Lambda(2)$. Позначимо $T_3 = (1\ 0)^T$ і $T_4 = (1\ 1)^T$ "половини" вектора T_0, $T_5 = (1\ 1)^T$ і $T_6 = (0\ 1)^T$ – "половини" вектора T_2. Знаходимо вектори $T_7 = T_3 \oplus T_4 = (0\ 1)^T$, $T_8 = T_5 \oplus T_6 = (1\ 0)^T$.

Нарешті, на третьому кроці застосовуємо процедуру $\Lambda(1)$ до кожного з чотирьох векторів T_3, T_7, T_5, T_8. В результаті отримаємо вектори $(1\ 1)^{\mathrm{T}}$, $(0\ 1)^{\mathrm{T}}$, $(1\ 0)^{\mathrm{T}}$ та $(1\ 1)^{\mathrm{T}}$ відповідно, з яких складаємо шуканий вектор коефіцієнтів полінома Жегалкіна функції f.

Отже, $P_f = (1\ 1\ 0\ 1\ 1\ 0\ 1\ 1)^{\mathrm{T}}$. ►

Зауважимо, що на підставі рівності (1.19) процедуру $\Lambda(n)$ можна застосувати також для обчислення вектора значень булевої функції за коефіцієнтами її поліному Жегалкіна.

1.34. ПРИКЛАД. Нехай БФ $f(x_1, x_2, x_3)$ задана поліномом Жегалкіна $f(x_1, x_2, x_3) = 1 \oplus x_1x_2 \oplus x_2x_3 \oplus x_1x_2x_3$. Знайдемо вектор значень цієї функції.

Спочатку за виразом полінома знаходимо вектор його коефіцієнтів $P_f = (1\ 0\ 0\ 1\ 0\ 0\ 1\ 1)^T$. Потім застосовуємо до цього вектора процедуру $\Lambda(3)$.

На першому кроці обчислень отримаємо вектори $P_0 = (1\ 0\ 0\ 1)^T$ та $P_2 = (1\ 0\ 0\ 1)^T \oplus (0\ 0\ 1\ 1)^T = (1\ 0\ 1\ 0)^T$. На другому кроці, застосовуючи процедуру $\Lambda(2)$ до векторів P_0, P_2 відповідно, отримаємо вектори

$$P_3 = (1\ 0)^T,\ P_7 = (1\ 0)^T \oplus (0\ 1)^T = (1\ 1)^T$$

та

$$P_5 = (1\ 0)^T,\ P_8 = (1\ 0)^T \oplus (1\ 0)^T = (0\ 0)^T.$$

На третьому кроці за допомогою процедури $\Lambda(1)$, що застосовуються до кожного з векторів P_3, P_7, P_5, P_8, обчислимо вектори $(1\ 1)^T$, $(1\ 0)^T$, $(1\ 1)^T$, $(0\ 0)^T$, які складають частини шуканого вектора значень БФ f.

Таким чином, $T_f = (1\ 1\ 1\ 0\ 1\ 1\ 0\ 0)^T$. ►

Завдання для самоконтролю

1. Нехай $(G, +)$ – скінченна абелева група, φ – підстановка на множині G. Доведіть, що при $X = K = Y = G$, $f(x,k) = \varphi(x+k)$, $x \in X$, $k \in K$ система (X, K, Y, f) є мінімальним шифром.

2. Побудуйте алгебраїчні моделі шифрів простої заміни та перестановки над довільним алфавітом. За яких умов ці шифри є регулярними чи транзитивними?

3. Добутком ендоморфних шифрів $\mathcal{A}_1 = (X, K_1, X, f_1)$ та $\mathcal{A}_2 = (X, K_2, X, f_2)$ називається система $\mathcal{A}_1\mathcal{A}_2 = (X, K, X, f)$, де $K = K_1 \times K_2$ і $f_k(x) = f_{k_2}(f_{k_1}(x))$ для будь-якого $k = (k_1, k_2) \in K$.

Переконайтесь, що ця система є шифром. Доведіть, що добуток транзитивних шифрів є транзитивним шифром.

4. Нехай φ – підстановка на множині V_n. Шифр Фейстеля з раундовою функцією φ визначається як система $\mathcal{A} = (X, K, Y, f)$, де

$X = Y = V_{2n}$, $K = V_n$, $f_k(x_1, x_2) = (x_2, x_1 \oplus \varphi(x_2 \oplus k))$, $x_1, x_2, k \in V_n$.

Доведіть, що цей шифр є регулярним, а його квадрат $\mathcal{A}^2 = \mathcal{A}\mathcal{A}$ – мінімальним.

5. Матриця перехідних ймовірностей шифру $\mathcal{A}$ вигляду (1.1) визначається як квадратна матриця $P(\mathcal{A})$ з елементами

$$P(\mathcal{A})_{x,y} = |K|^{-1} \cdot |\{k \in K : kx = y\}|, \ x \in X, \ y \in Y.$$

Доведіть, що

1) матриця $P(\mathcal{A})$ є стохастичною;

2) матриця перехідних ймовірностей ендоморфного шифру є двічі стохастичною;

3) шифр $\mathcal{A}$ є транзитивним (регулярним) тоді й тільки тоді, коли матриця $P(\mathcal{A})$ є додатною (складається тільки з елементів 0 та $|K|^{-1}$).

6. Доведіть, що для будь-яких ендоморфних шифрів $\mathcal{A}_1 = (X, K_1, X, f_1)$ та $\mathcal{A}_2 = (X, K_2, X, f_2)$ справедлива рівність $P(\mathcal{A}_1\mathcal{A}_2) = P(\mathcal{A}_1)P(\mathcal{A}_2)$.

7. Доведіть, що відмінна від константи афінна булева функція є зрівноваженою.

8. Нехай f – булева функція від n змінних. Розглянемо вузол ускладнення, який перетворює двійкову послідовність $x_1, x_2, \ldots$ на послідовність $y_1, y_2, \ldots$, де $y_i = f(x_i, x_{i+1}, \ldots, x_{i+n-1})$, $i = 1, 2, \ldots$. Припустимо, що знаки $x_1, x_2, \ldots$ є незалежними випадковими величинами, розподіленими за законом $\mathbf{P}(x_i = 0) = 1 - \mathbf{P}(x_i = 1) = 1/2$, $i = 1, 2, \ldots$. Переконайтесь, що зна-

ки $y_1, y_2, \ldots$ мають рівномірний розподіл на множині $\{0,1\}$ тоді й тільки тоді, коли функція f є зрівноваженою.

9. Доведіть, що довільна компонента будь-якої підстановки на множині V_n є зрівноваженою булевою функцією.

10. Доведіть, що булева функція від n змінних має алгебраїчний степінь n тоді й тільки тоді, коли її вага є непарним числом.

11. Наведіть для кожного натурального $n \geq 2$ приклад зрівноваженої булевої функції степеня $n-1$.

12. Побудуйте алгоритм обчислення значення (1.14) з часовою складністю $O(2^{2n})$.

13. Доведіть, що параметр (1.13) дорівнює

$$l_s(\alpha, \beta) = (2^{1-n} d(\alpha x, \beta s(x)) - 1)^2,$$

де $d(\alpha x, \beta s(x))$ позначає відстань Ґеммінга між зазначеними булевими функціями. Отримайте звідси співвідношення між максимальним елементом таблиці лінійних апроксимацій та нелінійністю підстановки s.

14. Доведіть, що таблиця різниць і таблиця лінійних апроксимацій довільної підстановки $s: V_n \to V_n$ є двічі стохастичними матрицями. Отримуйте звідси, що параметри (1.14) та (1.15) обмежені знизу числом $(2^n - 1)^{-1}$.

15. Обчисліть вагу булевої функції $x_1 x_2 \oplus x_3 x_4 \oplus \cdots \oplus x_9 x_{10}$.

16. Знайдіть поліном Жегалкіна булевої функції

$$f(x_1, x_2, \ldots, x_{17}) = x_1 \vee x_2 \vee \cdots \vee x_{17}.$$

17. Скільки існує булевих функцій від n змінних степеня k, де $k \in \overline{0,n}$?

18. Покажіть, що для обчислення полінома Жегалкіна за вектором значень булевої функції з використанням швидкого алгоритму достатньо 2^{n+1} бітів пам'яті.

19. Знайдіть поліном Жегалкіна функції f, якщо

1) $T_f = (1\,1\,1\,1\,0\,0\,0\,0)^T$;

2) $T_f = (0\,0\,1\,1\,0\,0\,1\,1)^T$;

3) $T_f = (0\,0\,1\,1\,1\,1\,0\,0)^T$.

20. Знайдіть вектор значень функції $f(x_1, x_2, x_3, x_4)$, якщо

1) $P_f = (1\,0\,1\,1\,0\,0\,1\,0\,0\,0\,1\,0\,1\,1\,0\,1)^T$;

2) $P_f = (1\,0\,0\,1\,1\,0\,1\,1\,1\,1\,1\,0\,1\,0\,0\,1)^T$;

3) $P_f = (0\,1\,1\,0\,1\,1\,0\,0\,1\,0\,0\,1\,0\,1\,0\,1)^T$.

2. ЗАГАЛЬНІ МЕТОДИ ПОБУДОВИ ТА АНАЛІЗУ БЛОКОВИХ ШИФРІВ

§ 2.1. Принципи побудови та основні класи сучасних блокових шифрів

2.1. ОЗНАЧЕННЯ. *Блоковим шифром* називається скінченний набір підстановок $F_\lambda : V_n \to V_n$, $\lambda \in \Lambda$. При цьому елементи множини V_n називаються *відкритими* (*шифрованими*) *повідомленнями*, елементи множини Λ – *ключами*, а підстановки F_λ – *шифрувальними перетвореннями* цього шифру.

Більшість сучасних блокових шифрів є ітераційними, шифрувальні перетворення яких задаються у вигляді композиції (послідовного виконання) однотипних простих перетворень, що залежать від раундових ключів.

Нехай K – скінченна множина, $(f_{i,k} : k \in K)$ – набір підстановок на множині V_n, $i \in \overline{1,r}$, $\theta : \Lambda \to K^r$ – відображення.

2.2. ОЗНАЧЕННЯ. *r-раундовий блоково-ітераційний шифр* з множиною відкритих (шифрованих) повідомлень V_n, множиною ключів Λ, *множиною раундових ключів* K та *розкладом ключів* θ визначається як набір підстановок

$$F_\lambda = f_{r,k(r)} \circ \cdots \circ f_{1,k(1)}, \tag{2.1}$$

де $(k(1), ..., k(r)) = \theta(\lambda)$ для будь-якого $\lambda \in \Lambda$. Елементи $k(1), ..., k(r)$ називаються *раундовими ключами*, а підстановки $f_{r,k(r)}, ..., f_{1,k(1)}$ – *раундовими*

шифрувальними перетвореннями цього шифру, які відповідають ключу шифрування λ (рис. 2.1).

Зазвичай при аналізі стійкості блоково-ітераційних шифрів відносно атак, які не враховують особливості розкладу ключів, у наведеному означенні вважають $\Lambda = K^r$, $\theta(\lambda) = \lambda = (k(1), ..., k(r))$, тобто вважають, що послідовність раундових ключів може бути довільним елементом множини K^r. Іноді до цієї умови додають також припущення, що на множині K^r задано рівномірний розподіл ймовірностей і для зашифрування довільного відкритого повідомлення $x \in V_n$ вибирається випадковий ключ $\theta(\lambda) = \lambda = (k(1), ..., k(r))$.

Надалі в цьому розділі слово шифр означає блоково-ітераційний шифр, якщо не зазначено протилежне.

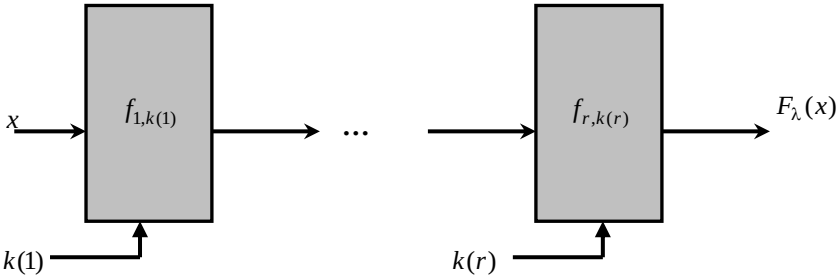

Рис. 2.1. Схематичне зображення блоково-ітераційного шифру

Ітераційний метод побудови блокових шифрів походить від К. Шеннона [2], який запропонував також терміни розсіювання та перемішування для неформального опису загальних умов, які повинні виконуватися для стійких блокових шифрів.

Розсіюванням називають розповсюдження впливу одного знаку відкритого повідомлення на багато знаків шифрованого, а *перемішуванням* – руйнування статистичних залежностей між відкритим та шифрованим повідомленнями. Ці умови зазвичай доповнюють вимогою про вплив кожного окремого знаку ключа на багато знаків шифрованого повідомлення.

Властивості розсіювання та перемішування мають на меті забезпечити, перш за все, криптографічну стійкість блокових шифрів відносно атак на основі відомих шифрованих повідомлень. З розвитком методів криптоаналізу, появою нових атак на блокові шифри ці загальні властивості постійно уточнюються та доповнюються більш конкретними вимогами. На сьогодні основним принципом побудови блокових шифрів є умова їхньої практичної стійкості до всіх відомих атак з можливістю ефективної реалізації алгоритмів шифрування на різноманітних платформах. Сучасний блоковий шифр повинен бути не тільки стійким, але й практичним. Саме тому для побудови блокових шифрів використовують ітераційні схеми, раундові перетворення яких можуть бути ефективно (програмно чи апаратно) реалізовані та одночасно створюють значний ефект розсіювання і перемішування при багатократному застосуванні.

В залежності від типу раундових перетворень більшість сучасних блокових шифрів можна розділити на два великих класи: SPN-шифри та шифри Фейстеля.

2.3. ОЗНАЧЕННЯ. Блоковий шифр вигляду (2.1) називається *SPN-шифром* (substitution-permutation network), якщо його раундові перетворення мають вигляд

$$f_{i,k}(z) = \varphi_i(z *_i k),\ z \in V_n,\ k \in K, \qquad (2.2)$$

де $K = V_n$, $*_i$ – комутативна групова операція на множині V_n, $i \in \overline{1,r}$,

$$\varphi_i(z) = (s_i^{(p-1)}(z^{(p-1)}),...,s_i^{(0)}(z^{(0)}))L_i\,,\ z = (z^{(p-1)},...,z^{(0)}) \in V_n\,, \qquad (2.3)$$

L_i – оборотна булева матриця порядку $n = pt$, $p,t \in \mathbf{N}$, $s_i^{(0)},...,s_i^{(p-1)}$ – підстановки на множині V_t та $z^{(j)} \in V_t$ для будь-якого $j \in \overline{0, p-1}$.

Підстановка φ_i вигляду (2.3) називається *раундовою функцією SPN-шифру в i-му раунді*, а підстановки $s_i^{(0)},...,s_i^{(p-1)}$ – його *вузлами заміни* або *s-блоками* (s-boxes) *в цьому раунді*.

На рис. 2.2 показана типова схема SPN-шифру з одним раундом шифрування (при цьому індекс i не зазначено).

Зазвичай операції $*_i$, $i \in \overline{1,r}$, збігаються з покоординатним булевим додаванням на множині V_n, проте є виключення з цього правила.

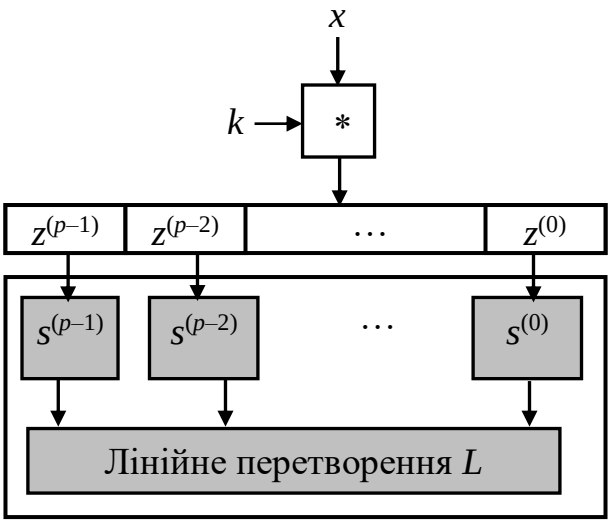

Рис. 2.2. Схема 1-раундового SPN-шифру

2.4. ОЗНАЧЕННЯ. Блоковий шифр вигляду (2.1) називається *шифром Фейстеля*, якщо $n = 2m$, $K = V_m$ та існують відображення $\psi_i : V_n \to V_m$, $i \in \overline{1,r}$, такі, що для будь-яких $x_1, x_2, k \in V_m$ виконуються рівності

$$f_{i,k}(x_1, x_2) = (x_2, x_1 \oplus \psi_i(x_2, k)), \ i \in \overline{1,r}. \tag{2.4}$$

Зазвичай відображення ψ_i визначається за формулою

$$\psi_i(z, k) = \varphi_i(z *_i k), \ z, k \in V_m, \tag{2.5}$$

де $*_i$ – комутативна групова операція на множині V_m, $i \in \overline{1,r}$, а φ_i є підстановкою вигляду (2.3) (із заміною в цій формулі n на m; див. рис. 2.3). Зазначена підстановка називається *раундовою функцією шифру Фейстеля*, а підстановки $s_i^{(0)}, \ldots, s_i^{(p-1)}$ – його *вузлами заміни в i-му раунді*.

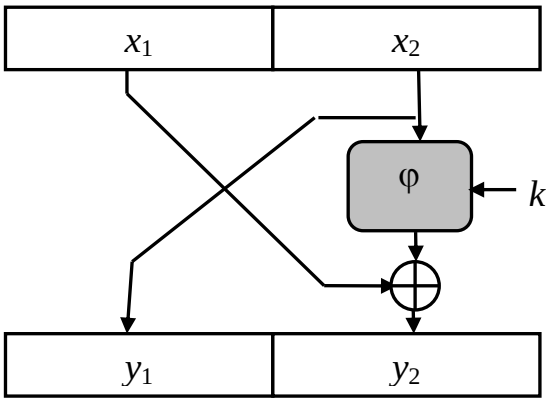

Рис. 2.3. Схема 1-раундового шифру Фейстеля

Класичними прикладами SPN-шифрів є Rijndael (AES) та "Калина", яким присвячено наступний параграф цього розділу.

Часто-густо вважається (хоча й не доведено), що SPN-шифри забезпечують краще розсіювання в порівнянні з таким способом шифрування, за яким в кожному раунді перетворюється тільки частина вхідного повідомлення. Тим не менш, шифри Фейстеля утворюють перспективний клас блокових шифрів, до якого відносяться, зокрема, такі алгоритми як DES, MISTY1, Camellia и ГОСТ. Відомі також блокові шифри, які не належать до зазначених вище класів, наприклад, алгоритми IDEA та FOX, побудовані за схемою Лея-Мессі, проте на сьогодні вони не отримали помітного застосування.

Як видно з формул (2.2) – (2.5), основними елементами блокового шифру (Фейстеля чи SPN) є його раундові функції φ_i та операції $*_i$, $i \in \overline{1,r}$, які визначають правила "накладання" раундових ключів на вхідні повідомлення в окремих раундах шифрування. Комутативну групову операцію $*_i$ іноді називають *ключовим суматором* в i-му раунді, $i \in \overline{1,r}$.

В залежності від виду ключового суматора переважну більшість блокових шифрів можна віднести до одного з таких класів.

1. *Шифри* з *двійковим ключовим суматором*. В цьому випадку операція $*_i$ збігається з покоординатним булевим додаванням на множині вхідних повідомлень: $x *_i k = x \oplus k$, $i \in \overline{1,r}$. Цей клас шифрів є найбільш численним та містить такі відомі алгоритми як DES, Camellia, Rijndael. Для шифрів Фейстеля та SPN з цього класу побудовано розвинути теорію оцінювання та обґрунтування стійкості відносно методів різницевого та лінійного криптоаналізу.

2. *Шифри з двійково-модулярним ключовим суматором*. В цьому випадку для будь-якого натурального l вектори $x, k \in V_l$ ототожнюються з l-розрядними двійковими числами, а операція $*_i$ визначається за формулою $x *_i k = (x + k) \bmod 2^l$, $i \in \overline{1,r}$. Найбільш відомим прикладом такого шифру є ГОСТ. Операція додавання за модулем 2^l є нелінійною відносно покоординатного булевого додавання на множині V_l, що збільшує ефект перемішування при зашифруванні повідомлень. В той же час, наявність такої операції ускладнює аналіз стійкості блокового шифру, наприклад, робить неможливим застосування класичних методів при дослідженні його стійкості відносно різницевого та лінійного криптоаналізу.

3. *Шифри зі змішаним ключовим суматором.* В цьому випадку операція $*_i$ залежить від номера раунду шифрування або визначається як деяка суперпозиція зазначених вище операцій. Прикладом є шифр "Калина" з довжиною блоку $n = 256$ бітів, у якому $*_i = \oplus$ для $i \in \overline{2, r-1}$, $*_i = \overset{\circ}{+}$ для $i \in \{1, r\}$, а операція $\overset{\circ}{+}$ на множині V_{256} визначається за формулою

$$x \overset{\circ}{+} k = (x^{(1)} + k^{(1)}, ..., x^{(4)} + k^{(4)}), \tag{2.6}$$

де $x = (x^{(1)}, ..., x^{(4)})$, $k = (k^{(1)}, ..., k^{(4)})$, $x^{(\nu)}, k^{(\nu)} \in V_{64}$, $\nu \in \overline{1,4}$, а $+$ позначає додавання за модулем 2^{64}.

Тип ключового суматора, поряд з властивостями раундових функцій, здійснює безпосередній вплив на стійкість блокового шифру.

Як видно з формули (2.3), раундова функція шифру Фейстеля або SPN в кожному раунді задається набором s-блоків та лінійним відобра-

женням. Ці об'єкти повинні володіти низкою спеціальних властивостей, список яких постійно розширюється з розвитком методів криптоаналізу.

Іншими параметрами, від яких залежить стійкість блокового шифру, є довжина блоку, довжина ключа та число раундів шифрування. Довжина блоку сучасного блокового шифру повинна складати не менше 64 бітів. Від цього параметра залежить стійкість шифру відносно атак на основі колізій, причому для забезпечення стійкості на рівні 2^n потрібен шифр з довжиною блоку не менше ніж $2n$ бітів. Зауважимо, що у багатьох додатках використовуються шифри з малої довжиною блоку (64 біти). Наприклад, з семи алгоритмів (TDEA, MISTY1, CAST-128, HIGHT, Rijndael, Camellia, SEED), затверджених Міжнародною організацією зі стандартизації (ISO), перші чотири мають довжину блоку 64 біти. З іншого боку, s-блоки у виразі раундової функції блокового шифру зазвичай є перетвореннями векторів невеликої довжини (8 бітів), що надає змогу проводити вичерпний аналіз їхніх криптографічних властивостей та ефективно реалізовувати їх за допомогою програмних чи апаратних засобів.

Отже, підсумовуючи, можна зробити такі висновки:

– основним принципом побудови сучасних блокових шифрів є умова їхньої практичної стійкості до усіх відомих атак поряд з можливістю ефективної реалізації алгоритмів шифрування на різних платформах;

– стійкість блокового шифру визначається властивостями його раундових функцій, типом ключового суматора, довжиною блоку, довжиною ключа та кількістю раундів шифрування;

– переважна більшість сучасних блокових шифрів відноситься до класу SPN-шифрів або шифрів Фейстеля, які описуються співвідношеннями (2.2), (2.3) та (2.4), (2.5) відповідно.

§ 2.2. Алгоритми шифрування Rijndael та "Калина"

Алгоритм Rijndael (відомий також під назвою AES) [4] є стандартом шифрування Сполучених Штатів Америки. Вважаючи, що читач знайомий з описом цього алгоритму, відзначимо особливості його побудови, які безпосередньо впливають на його стійкість.

Rijndael є блоковим шифром з довжиною блоку n та довжиною ключа n_k, які можуть приймати одне з трьох значень: 128, 192, 256 бітів. Алгоритм складається з n_r раундів, де параметр n_r визначається за числами n та n_k згідно з табл. 2.1.

Таблиця 2.1

Кількість раундів в алгоритмі шифрування Rijndael

n_r	$n=128$	$n=192$	$n=256$
$n_k=128$	10	12	14
$n_k=192$	12	12	14
$n_k=256$	14	14	14

В Rijndael використовуються чотири базові перетворення, означення яких наведено нижче:

1) K (AddRoundKey) – додавання до вхідного повідомлення раундового ключа;

2) S (ByteSub) – застосування нелінійних вузлів заміни;

3) R (ShiftRow) – циклічний зсув рядків;

4) M (MixColumn) – перемішування стовпців.

Зашифрування відкритого тексту полягає у виконанні таких дій:

1) обчисленні (за допомогою окремої процедури – розкладу ключів) $n_r + 1$ раундових ключів за ключем шифрування;

2) додаванні першого раундового ключа до відкритого тексту;

3) виконанні $n_r - 1$ проміжних раундів;

4) виконанні останнього раунду.

Кожен проміжний раунд полягає в послідовному застосуванні до вхідного повідомлення перетворень S, R, M, K; в останньому раунді здійснюються перетворення S, R, K. Наприклад, при $n_r = 2$ правило зашифрування відкритого тексту x описується так: $y = x\,K(SMRK)SRK$ (тут перетворення застосовуються справа наліво).

Перейдемо до означення наведених перетворень.

Перш за все, задамо структуру поля на множині V_8, яка складається з двійкових векторів довжини 8 (байтів). Для цього позначимо

$$m(x) = x^8 \oplus x^4 \oplus x^3 \oplus x \oplus 1$$

незвідний поліном степеня 8 над полем з двох елементів і ототожнимо кожен вектор $a = (a_0, a_1, ..., a_7) \in V_8$ з поліномом $a_0 \oplus a_1 x \oplus \cdots \oplus a_7 x^7$. Додавання цих поліномів здійснюватимемо звичайним чином, а множення – за модулем полінома $m(x)$. В результаті отримаємо поле з 2^8 елементів, яке позначимо F_{2^8}.

Далі, позначимо σ підстановку Ніберг (див. приклад 1.28), яка визначається за формулою $\sigma(x) = x^{-1}$, $x \in F_{2^8} \setminus \{0\}$; $\sigma(0) = 0$, та задамо *вузол заміни* s *шифру* Rijndael як композицію двох підстановок: σ та деякої фіксованої афінної підстановки на множині V_8. Вигляд цієї підстановки не

має суттєвого значення для подальшого викладення і тут не наводиться (див. п. 4.2.1 в [4]). Вона застосовується в алгоритмі Rijndael для усунення небажаної властивості $\sigma(0)=0$, а також для ускладнення поліноміального представлення підстановки Ніберг, яка задається мономом $\sigma(x)=x^{2^8-2}$ над полем F_{2^8}).

Будь-який двійковий вектор довжини $n\in\{128,192,256\}$ записуватимемо у вигляді прямокутної таблиці розміру $4\times(n/32)$, рядками якої є послідовні фрагменти (підвектори) цього вектора довжини $n/32$ байтів кожен.

Наприклад, розглянемо довільний вектор $x\in V_{192}$, який "розіб'ємо" на байти: $x=(x_0,x_1,...,x_{23})$, де $x_i\in V_8$, $i\in\overline{0,23}$. Тоді, таблиця, що відповідає цьому вектору, має такий вигляд:

$$x=\begin{pmatrix} x_0 & x_1 & x_2 & x_3 & x_4 & x_5 \\ x_6 & x_7 & x_8 & x_9 & x_{10} & x_{11} \\ x_{12} & x_{13} & x_{14} & x_{15} & x_{16} & x_{17} \\ x_{18} & x_{19} & x_{20} & x_{21} & x_{22} & x_{23} \end{pmatrix}. \qquad (2.7)$$

Надалі вважатимемо, що відкриті, шифровані та проміжні повідомлення, а також раундові ключі алгоритму Rijndael записуються у вигляді таких таблиць, причому їхні рядки нумеруються зверху вниз числами 0, 1, 2, 3.

Визначимо, нарешті, згадані вище перетворення S, R, M, K.

Перше з них полягає у застосуванні підстановки s (вузлу заміни шифру Rijndael) до кожного елементу таблиці, яка представляє вхідне по-

відомлення. Наприклад, для повідомлення x вигляду (2.7) значення $S(x)$ визначається за формулою

$$S(x)=\begin{pmatrix} s(x_0)\ s(x_1)\ s(x_2)\ s(x_3)\ s(x_4)\ s(x_5) \\ s(x_6)\ s(x_7)\ s(x_8)\ s(x_9)\ s(x_{10})\ s(x_{11}) \\ s(x_{12})\ s(x_{13})\ s(x_{14})\ s(x_{15})\ s(x_{16})\ s(x_{17}) \\ s(x_{18})\ s(x_{19})\ s(x_{20})\ s(x_{21})\ s(x_{22})\ s(x_{23}) \end{pmatrix}.$$

Перетворення R полягає в циклічному зсуві i-го рядка таблиці вхідного повідомлення на i позицій ліворуч, $i \in \overline{0,3}$:

$$R(x)=\begin{pmatrix} x_0\ x_1\ x_2\ x_3\ x_4\ x_5 \\ x_7\ x_8\ x_9\ x_{10}\ x_{11}\ x_6 \\ x_{14}\ x_{15}\ x_{16}\ x_{17}\ x_{12}\ x_{13} \\ x_{21}\ x_{22}\ x_{23}\ x_{18}\ x_{19}\ x_{20} \end{pmatrix}.$$

Перетворення M визначається за допомогою певної фіксованої 4×4-матриці D над полем F_{2^8} і полягає у множенні кожного стовпця таблиці повідомлення x на цю матрицю (нагадаємо, що елементи таблиці є байтами, на множині яких задано структуру поля порядку 2^8). Отже, для повідомлення x вигляду (2.7) значення $M(x)$ записується у вигляді таблиці, перший стовпець якої дорівнює $D(x_0\ x_6\ x_{12}\ x_{18})^T$, другий стовпець дорівнює $D(x_1\ x_7\ x_{13}\ x_{19})^T$ і т.д., аж до шостого стовпця, який дорівнює $D(x_5\ x_{11}\ x_{17}\ x_{23})^T$ (верхній індекс T позначає операцію транспонування рядка). Явний вираз матриці D наведено в [4], п. 4.2.3.

Нарешті, перетворення K полягає у додаванні за модулем 2 до вхідного повідомлення x відповідного раундового ключа.

Окремою процедурою алгоритму Rijndael є розклад ключів, за допомогою якого за ключем шифрування λ формується послідовність раундових ключів $\theta(\lambda) = (k(1), ..., k(n_r + 1))$ (див. означення 2.2). Опис цієї процедури наведено в [4], п. 4.3.

З представленого означення алгоритму випливає, що він являє собою $(n_r + 1)$ -раундовий SPN-шифр, який описується співвідношеннями (2.1), (2.2) та (2.3). При цьому вузли заміни $s_i^{(0)}, ..., s_i^{(p-1)}$ у формулі (2.3) збігаються з підстановкою s в кожному раунді з номером $i \le n_r$ та є тотожними підстановками в останньому, $(n_r + 1)$ -му, раунді. Окрім того, лінійне перетворення L_i у формулі (2.3) визначається таким чином (див. задачу 6):

$$L_i = R \circ M \text{, якщо } i \le n_r - 1;$$

$$L_i = R \text{, якщо } i = n_r;$$

$$L_i(x) = x, \ x \in V_n \text{, якщо } i = n_r + 1.$$

Представлення алгоритму Rijndael у вигляді SPN-шифру надає змогу проаналізувати його стійкість до різних атак, використовуючи загальні методи, розвинені для таких шифрів. Зауважимо, що перші атаки на редуковані версії шифру (з меншою кількістю раундів) з'явилися майже одразу після його опублікування, але на сьогодні відомо лише одну атаку на Rijndael, яка є ефективніше за перебірну (а саме, атаку зі складністю $2^{126,67}$ на шифр с довжиною ключа 128 бітів [5]).

Серед недоліків алгоритму, виявлених в процесі його дослідження, звичайно відзначають слабкість розкладу ключів (пов'язану, головним чином, з аналітичними залежностями між раундовими ключами; див., наприклад, [6]) та простоту алгебраїчного опису окремих компонент алгоритму, перш за все, його вузла заміни (див., наприклад, [7]). Останній факт свого часу спровокував багато спекуляцій стосовно можливості зламування шифру Rijndael за допомогою алгебраїчних атак, хоча жодної такої атаки запропоновано не було. Поряд з тим, враховуючи багаторічний досвід дослідження цього шифру, а також інших блокових шифрів, у 2014 році в Україні стандартизовано алгоритм блокового шифрування, відомий під назвою "Калина" [8].

Як і Rijndael, алгоритм "Калина" є SPN-шифром. Він має довжину блоку n та довжину ключа $n_k \geq n$, які можуть приймати одне з трьох значень: 128, 256, 512. Алгоритм складається з n_r раундів, де параметр n_r визначається за числами n та n_k згідно з табл. 2.2.

Таблиця 2.2

Кількість раундів в алгоритмі шифрування "Калина"

n, n_k	n_r
128, 128	10
128, 256	14
256, 256	14
256, 512	18
512, 512	18

Головні відмінності між алгоритмами "Калина" та Rijndael полягають у застосуванні в першому з них

– спеціально розробленого розкладу ключів;

– операції додавання за модулем 2^{64} у ключовому суматорі в першому та останньому раундах шифрування;

– s-блоків, які (на відміну від вузла заміни шифру Rijndael) не мають простих поліноміальних представлень та обрані випадково з дотриманням низки криптографічних умов.

Отже, "Калина" є $(n_r + 1)$-раундовим SPN-шифром, який описується співвідношеннями (2.1), (2.2) та (2.3). При цьому будь-який вузол заміни $s_i^{(0)}, ..., s_i^{(p-1)}$ збігається з одним з чотирьох зазначених вище s-блоків у кожному раунді з номером $i \le n_r$ та є тотожною підстановкою в останньому, $(n_r + 1)$-му, раунді. Операція $*_i$ у формулі (2.2) є додаванням за модулем 2 при $i \in \overline{2, n_r}$ та визначається за формулою (2.6), якщо $i \in \{1, n_r + 1\}$ та $n = 256$ (і має аналогічний вигляд для двох інших значень n). Нарешті, лінійне перетворення L_i у формулі (2.3) задається аналогічно відповідному перетворенню в алгоритмі Rijndael.

Обґрунтування стійкості шифру "Калина" відносно низки відомих атак наведено в [9]. Зауважимо, що на відміну від Rijndael, на сьогодні не відомо атак на повну версію цього шифру (з максимальним числом раундів), ефективніших за перебір ключів.

§ 2.3. Поняття стійкого блокового шифру

Як зазначено в § 1.1, стійкість характеризує здатність криптосистеми протистояти всіляким атакам на неї. Зокрема, блоковий шифр є стійким, якщо для нього не існує атак, ефективніших за повний перебір ключів або

відкритих текстів (в залежності від типу атаки). При цьому йдеться не тільки про атаки на основі єдиного відомого шифротексту, а про усі алгоритми, які надають змогу виявляти відмінності між заданим шифром та *ідеальним блоковим шифром* з такою ж довжиною блоку, тобто суто випадковою підстановкою на множині V_n.

Сформулюємо точне означення стійкого блокового шифру.

Розглянемо таку *гру між Дослідником та Криптоаналітиком*.

Дослідник випадково рівноймовірно вибирає ключ k заданого блокового шифру та надає Криптоаналітику доступ до оракула Φ, який з ймовірністю $1/2$ збігається з шифрувальним перетворенням цього шифру при ключі k (гіпотеза H_0) і з такою ж ймовірністю реалізує випадкову рівноймовірну підстановку на множині V_n (гіпотеза H_1).

Криптоаналітик може подавати на вхід оракула Φ будь-які повідомлення $x_1, x_2, \ldots$ і отримувати відповідні вихідні повідомлення $\Phi(x_1), \Phi(x_2), \ldots$. Він може також подавати на вхід оракула Φ^{-1} (який реалізує оборотну до Φ підстановку) довільні повідомлення $y_1, y_2, \ldots$ та отримувати повідомлення $\Phi^{-1}(y_1), \Phi^{-1}(y_2), \ldots$. Мета Криптоаналітика – визначити, яка з гіпотез H_0 або H_1 є справжньою.

2.5. ОЗНАЧЕННЯ. Нехай $T > 0$, $0 < \varepsilon < 1/2$. Блоковий шифр називається (T, ε)-*стійким*, якщо будь-який статистичний критерій для розрізнення зазначених гіпотез із середньою ймовірністю помилки не вище ε виконує принаймні T умовних операцій. (Нагадаємо, що середня ймовірність помилки критерію визначається за формулою

$$1/2 \cdot (\Pr(H_1 \mid H_0) + \Pr(H_0 \mid H_1)),$$

де $\Pr(H_1 \mid H_0)$ та $\Pr(H_0 \mid H_1)$ – ймовірності помилок першого та другого роду відповідно).

Блоковий шифр вважається *стійким*, що він є (T, ε)-стійким при значеннях T, порівняних із заздалегідь визначеним порогом (security level) та значеннях ε, не надто близьких до $1/2$. Наприклад, можна вважати стійким блоковий шифр з довжиною ключа $l = 128$ бітів за умови $T = 2^{128}$, $\varepsilon = 1/2 - 2^{-20}$.

Означення 2.5 є важливим, оскільки описує простий та зрозумілий інтерфейс між шифром та іншими компонентами системи захисту інформації. Якщо блоковий шифр є стійким у зазначеному сенсі, його можна вважати ідеальним шифром, і навпаки, якщо він не поводить себе як ідеальний шифр, то це створює певні ризики для безпеки відповідної інформаційної системи. Використовуючи стійкий блоковий шифр, не треба пам'ятати про його особливості або недоліки, оскільки такий шифр володіє усіма властивостями, які очікують від "нормального" блокового шифру. Оскільки концепція ідеального шифру є дуже простою, то це помітно полегшує роботу проектувальників систем захисту інформації [10].

Хоча означення 2.5 є загальновизнаним, на сьогодні не існує методів доведення стійкості блокових шифрів, які використовуються на практиці. Зокрема, не відомо, чи є стійкими у зазначеному сенсі такі алгоритми шифрування як Rijndael та "Калина" (нагадаємо, що на шифр Rijndael с довжиною ключа 128 бітів існує атака зі складністю $2^{126,67}$ [5]). Виходячи з цього, стійкість сучасних блокових шифрів оцінюють тільки відносно відомих методів криптоаналізу.

Шифр вважається *практично стійким*, якщо для нього не відомо атак, ефективніших за повний перебір ключів або відкритих текстів, потрібних для реалізації атаки.

Відзначимо основні ознаки, за якими класифікують атаки на блокові шифри.

1. *Мета противника*. В залежності від неї можна поділити атаки на розрізнювальні та ті, що спрямовані на відновлення ключів.

Якщо противник має на меті відрізнити шифрувальне перетворення заданого блокового шифру від суто випадкової підстановки (як сказано в означенні 2.5), то така атака називається *розрізнювальною* або *розпізнавальною* (distinguishing attack) на відміну від атаки, *спрямованої на відновлення ключа* (key recovery attack).

2. *Можливості противника*. Ця ознака визначає, як саме обмежений доступ противника до оракула, що реалізує зашифрування або розшифрування повідомлень при випадково обраному невідомому ключі. В залежності від можливостей противника виділяють *атаки на основі відомого шифротексту, атаки на основі відомих відкритих текстів, атаки на основі підібраних відкритих текстів і атаки на основі підібраних шифрованих текстів*.

При проведенні атак на основі підібраних відкритих текстів противник має вільний доступ до оракула Φ та може отримувати повідомлення $\Phi(x_1), ..., \Phi(x_t)$ для будь-яких відкритих текстів $x_1, ..., x_t$. При цьому кількість t зазначених текстів, потрібних для реалізації атаки, є одним з показників її ефективності. Зокрема, блоковий шифр вважається стійким до такої атаки, якщо для її успішного виконання потрібно зашифрувати майже всі 2^n відкритих текстів, де n – довжина блоку. При проведенні атак на основі підібраних шифрованих текстів противник має доступ до кожного з оракулів Φ, Φ^{-1} і може отримувати повідомлення $\Phi(x_1), ..., \Phi(x_t)$ та $\Phi^{-1}(x_1), ..., \Phi^{-1}(x_t)$ для будь-яких $x_1, ..., x_t \in V_n$.

Зауважимо, що переважна більшість відомих сьогодні атак на блокові шифри є атаками на основі підібраних відкритих текстів.

3. *Метод криптоаналізу*. В залежності від методів, які використовуються для розв'язання криптоаналітичних задач, виділяють *алгебраїчні* та *статистичні* атаки.

Алгебраїчними називають атаки, що базуються на розв'язанні систем алгебраїчних рівнянь, які пов'язують відкриті та шифровані тексти з ключем шифрування. Статистичні атаки базуються на ймовірнісно-статистичних методах і зазвичай полягають у розв'язанні задач перевірки (двох або декількох) статистичних гіпотез. До цього класу відносяться майже усі відомі атаки на блокові шифри (за виключенням невеликої кількості суто алгебраїчних та повного перебору ключів). Історично першими з них є різницева та лінійна атаки на шифр DES, запропоновані на початку 90-х років минулого століття.

§ 2.4. Різницевий метод криптоаналізу

Різницевий (або диференціальний) метод криптоаналізу запропоновано Е. Біхамом та А. Шаміром [11] стосовно шифру DES. Згодом цей метод розвинено та поширено на інші блокові (а також деякі потокові) шифри та ґеш-функції. Нижче описано класичну різницеву атаку "останнього раунду" на довільний блоковий шифр та доведено твердження про нижню межу складності цієї атаки. Зазначений результат є основою для обґрунтування стійкості блокових шифрів відносно різницевого методу криптоаналізу.

Розглянемо r-раундовий блоковий шифр $\mathcal{B}$ з набором шифрувальних перетворень

$$F_\lambda = f_{r,k(r)} \circ \cdots \circ f_{1,k(1)},$$

де $\lambda = (k(1), ..., k(r)) \in K^r$, K – множина раундових ключів. Згідно з домовленістю, прийнятою в § 2.1, вважатимемо, що ключі $k(1), ..., k(r)$ вибираються з множини K незалежно один від одного, випадково та рівноймовірно.

Різницева атака на шифр $\mathcal{B}$ проводиться на основі підібраних відкритих текстів та має на меті відновлення ключа $k(r)$ в останньому раунді шифрування.

Для проведення атаки супротивник вибирає ненульові вектори $\alpha, \beta \in V_n$, генерує незалежні випадкові рівноймовірні відкриті тексти X_i, обчислює значення $X_i \oplus \alpha$ та знаходить відповідні шифровані тексти $Y_i = F_\lambda(X_i)$ та $Y_i' = F_\lambda(X_i \oplus \alpha)$, $i \in \overline{1,t}$. Далі криптоаналітик складає таблицю розміру $t \times |K|$, на перетині i-го рядку і k'-го стовпця якої розміщує значення

$$\xi_{k'}^{(i)} = \begin{cases} 1, \text{ якщо } f_{r,k'}^{-1}(Y_i') \oplus f_{r,k'}^{-1}(Y_i) = \beta; \\ 0 - \text{у протилежному випадку, } i \in \overline{1,t},\ k' \in K. \end{cases} \qquad (2.8)$$

Нарешті для відновлення ключа $k(r)$ криптоаналітик обчислює значення випадкових величин

$$\eta_{k'} = \sum_{i=1}^{t} \xi_{k'}^{(i)}, \ k' \in K, \tag{2.9}$$

та вважає $k(r)$ рівним такому елементу $\kappa^* \in K$, для якого досягається максимум значень $\eta_{k'}$ за всіма $k' \in K$. (Якщо існує більше одного елемента з такою властивістю, то криптоаналітик вибирає навмання будь-який з них).

Зрозуміло, що наведена атака є статистичною та може припускатися помилки, яка трапляється за умови $\kappa^* \neq k(r)$. Кажучи неформально, атака базується на тому, що пара випадкових відкритих текстів з фіксованою різницею α може перетворитися після $r-1$ раундів шифрування на пару текстів з фіксованою різницею β з імовірністю, що помітно відрізняється від "рівноймовірного" значення, яке дорівнює $(2^n - 1)^{-1}$ (див. задачу 11). Видається правдоподібним, що обчислюючи значення випадкових величин (2.9) та вибираючи ключ $k(r)$ як зазначено в описі наведеної атаки, можна статистично відрізнити справжнє значення цього ключа від інших (хибних) значень. Для того, щоб строго сформулювати та довести відповідне твердження, введемо таке поняття.

Для будь-якого $j \in \overline{1,r}$ позначимо $F_{k(1),\dots,k(j)} = f_{j,k(j)} \circ \cdots \circ f_{1,k(1)}$ шифрувальне перетворення шифра $\mathcal{P}$ в перших j раундах та задамо *ймовірність j-раудового диференціалу* (α,β) за формулою

$$D_j(\alpha,\beta) = |K|^{-j} \sum_{(k(1),\dots,k(j))\in K^j} \Pr\{F_{k(1),\dots,k(j)}(X \oplus \alpha) \oplus F_{k(1),\dots,k(j)}(X) = \beta\}, \tag{2.10}$$

де ймовірність Pr обчислюється відносно випадкового рівноймовірного вибору вектора X із множини V_n.

Ефективність наведеної атаки характеризується найменшою кількістю t зашифрувань, які треба зробити для відновлення ключа $k(r)$ з імовірністю помилки, що не перевищує задану межу.

Наступне твердження встановлює нижню оцінку цього параметра.

2.6. ТВЕРДЖЕННЯ. Нехай $0 < \varepsilon < 1 - |K|^{-1}$. Тоді для відновлення ключа $k(r)$ з імовірністю не менше ніж $|K|^{-1} + \varepsilon$ за допомогою наведеної атаки необхідно виконати

$$t \geq \frac{\varepsilon}{D_{\max}(r-1)} \tag{2.11}$$

зашифрувань, де

$$D_{\max}(r-1) = \max\{D_{r-1}(\alpha,\beta) : \alpha,\beta \in V_n \setminus \{0\}\}. \tag{2.12}$$

◄ Позначимо $\pi_t = \Pr\{\kappa^* = k(r)\}$, де ймовірність обчислюється відносно незалежного випадкового рівноймовірного вибору ключів $k(1), ..., k(r)$ та відкритих текстів X_i, $i \in \overline{1,t}$. Помітимо, що для доведення твердження достатньо переконатися у справжності такої нерівності:

$$\pi_t \leq |K|^{-1} + tD_{\max}(r-1). \tag{2.13}$$

З формули повної ймовірності та означення випадкового елемента κ^* випливають співвідношення

$$\pi_t = \sum_{k \in K} \Pr\{\kappa^* = k,\, k(r) = k\} \;=$$

$$= \sum_{k \in K} \left(\Pr\{\kappa^* = k,\, k(r) = k,\, \eta_k \geq 1\} + \Pr\{\kappa^* = k,\, k(r) = k,\, \eta_k = 0\} \right) \leq$$

$$\leq \sum_{k \in K} \left(\Pr\{\eta_k \geq 1,\, k(r) = k\} + \Pr\{ \bigcap_{k' \in K} \{\eta_{k'} = 0\},\, \kappa^* = k,\, k(r) = k\} \right). \qquad (2.14)$$

При цьому на підставі формул (2.8) – (2.10), умови незалежності та рівноймовірності раундових ключів $k(1), ..., k(r)$ і нерівності Маркова мають місце співвідношення

$$\Pr\{\eta_k \geq 1,\, k(r) = k\} =$$

$$= |K|^{-1} \Pr\left(\sum_{i=1}^{t} I\{F_{k(1),\ldots,k(r-1)}(X_i \oplus \alpha) \oplus F_{k(1),\ldots,k(r-1)}(X_i) = \beta\} \geq 1 \right) \leq$$

$$\leq |K|^{-1} \left(\sum_{i=1}^{t} \mathbf{E}\left(I\{F_{k(1),\ldots,k(r-1)}(X_i \oplus \alpha) \oplus F_{k(1),\ldots,k(r-1)}(X_i) = \beta\} \right) \right) =$$

$$\leq |K|^{-1}\, t \Pr\{F_{k(1),\ldots,k(r-1)}(X_i \oplus \alpha) \oplus F_{k(1),\ldots,k(r-1)}(X_i) = \beta\} \leq$$

$$\leq |K|^{-1}\, t D_{\max}(r-1)\,,\; k \in K \qquad (2.15)$$

(тут символ I позначає індикатор відповідної події, а символ $\mathbf{E}$ – математичне сподівання).

Далі, оскільки подія $\bigcap_{k' \in K} \{\eta_{k'} = 0\}$ тягне за собою випадковий рівноймовірний вибір значення елемента κ^* з множини K незалежно від конкретного значення раундового ключа $k(r)$, то

$$\Pr\{\bigcap_{k' \in K} \{\eta_{k'} = 0\}, \kappa^* = k, k(r) = k\} \leq$$

$$\leq |K|^{-1} \Pr\{k(r) = k\} = |K|^{-2}, \ k \in K. \qquad (2.16)$$

З формул (2.14) – (2.16) випливає нерівність (2.13). ►

З отриманого твердження випливає, що блоковий шифр є стійким відносно розглянутої різницевої атаки, якщо значення параметра (2.12) має порядок 2^{-n}. Дійсно, в цьому випадку для успішної (з ймовірністю не менше ніж $|K|^{-1} + \varepsilon$, де $\varepsilon = \text{const}$) реалізації атаки необхідно зашифрувати майже всі такі тексти (а саме, порядку $2^n \varepsilon$ текстів).

Таким чином, твердження 2.6 зводить задачу обґрунтування стійкості блокового шифру відносно різницевого криптоаналізу до знаходження верхніх меж параметра (2.12), які надавали би змогу переконуватися у його достатній малості. Хоча остання задача є нетривіальною та далекою від кінцевого вирішення, для багатьох SPN-шифрів, зокрема, таких як Rijndael та "Калина", створено ефективні методи її розв'язання.

Зокрема, відомо [12], що для шифру Rijndael з довжиною блоку $n = 128$ бітів виконується нерівність $D_{\max}(r-1) \leq 1.144 \cdot 2^{-111}$, де $r \geq 5$. Для шифру "Калина" з довжиною блоку n бітів та $r \geq 6$ раундами шифрування справедливе таке співвідношення [9]:

$$D_{\max}(r-1) \le \begin{cases} 2^{-80}, \text{ якщо } n = 128; \\ 2^{-160}, \text{ якщо } n = 256; \\ 2^{-320}, \text{ якщо } n = 512. \end{cases}$$

Наведені оцінки свідчать про те, що обидва блокових шифри є обґрунтовано стійкими (provable secure) відносно різницевого методу криптоаналізу.

§ 2.5. Лінійний метод криптоаналізу

Лінійний метод запропоновано М. Матцуі [13] стосовно алгоритму шифрування DES та розвинено у багатьох подальших публікаціях. Нижче описано лінійну атаку на довільний блоковий шифр, аналогічну за сутністю так званому Алгоритму 1 Матцуі, та отримано нижню оцінку часової складності цієї атаки.

Нехай $\mathcal{B}$ – довільний (не обов'язково ітераційний) блоковий шифр з множиною ключів $K = V_l$ та набором шифрувальних перетворень $F_k : V_n \to V_n$. Для проведення лінійної атаки на цей шифр супротивник вибирає ненульові вектори $\alpha, \beta \in V_n$ та зрівноважену функцію $\psi : K \to \{0,1\}$.

Нехай κ – невідомий ключ цього шифру, вибраний з імовірністю $|K|^{-1}$ з множини K. При проведенні атаки криптоаналітик генерує t незалежних випадкових рівноймовірних відкритих текстів $X_1, ..., X_t$, зашифровує їх на ключі κ та обчислює значення випадкових величин

$$\xi_{i,\kappa} = \alpha X_i \oplus \beta F_\kappa(X_i),\ i \in \overline{1,t}\,. \qquad (2.17)$$

Мета атаки полягає в тому, щоб відновити за послідовністю (2.17) значення $\psi(\kappa)$, тобто перевірити справжність однієї з двох гіпотез $H_0 : \psi(\kappa) = 0$; $H_1 : \psi(\kappa) = 1$.

Нагадаємо, що довільний критерій для перевірки цих гіпотез визначається множиною $A_0 \subseteq V_t$ та полягає в тому, що гіпотеза H_0 приймається тоді й тільки тоді, коли виконується умова $\xi_\kappa^{(t)} \stackrel{\text{def}}{=} (\xi_{1,\kappa},...,\xi_{t,\kappa}) \in A_0$. Середня ймовірність успіху критерію визначається за формулою

$$p_{\text{suc}}(A_0) = 1/2 \cdot \left(\Pr(\xi_\kappa^{(t)} \in A_0 \mid H_0) + \Pr(\xi_\kappa^{(t)} \notin A_0 \mid H_1)\right).$$

2.7. ТВЕРДЖЕННЯ. Для будь-якої множини $A_0 \subseteq V_t$ справедливе співвідношення $p_{\text{suc}}(A_0) \le 1/2 + 2\sqrt{t}\,\lambda^{1/2}$, де

$$\lambda = |K|^{-1} \sum_{k \in K} (2\Pr\{\alpha X \oplus \beta F_k(X) = 0\} - 1)^2\,. \qquad (2.18)$$

Отже, для проведення на шифр $\mathcal{B}$ лінійної атаки з середньою ймовірністю успіху $1/2 + \varepsilon$, де $\varepsilon \in (0, 1/2)$, необхідно виконати не менше ніж $t \ge \dfrac{\varepsilon^2}{4\lambda}$ зашифрувань.

◄ Перш за все, сформулюємо допоміжне твердження, доведене в [14] (лема 15): для будь-яких $p \in [0,1]$, $t \in \mathbf{N}$ справедлива нерівність

$$\max_{A\subseteq V_t}\left|\sum_{a\in A}(p^{wt(a)}(1-p)^{t-wt(a)}-2^{-t})\right|\le 2\sqrt{t}\,|2p-1|, \qquad (2.19)$$

де $wt(a)=a_1+...+a_t$ для будь-якого $a=(a_1,...,a_t)\in V_t$.

Далі, використовуючи зрівноваженість функції ψ та формулу повної ймовірності, отримаємо такі співвідношення:

$$p_{\text{suc}}(A)=1/2\cdot\left(\Pr(\xi_{\kappa}^{(t)}\in A_0\mid\psi(\kappa)=0)+\Pr(\xi_{\kappa}^{(t)}\notin A_0\mid\psi(\kappa)=1)\right)=$$

$$=\Pr(\xi_{\kappa}^{(t)}\in A_0,\psi(\kappa)=0)+\Pr(\xi_{\kappa}^{(t)}\notin A_0,\psi(\kappa)=1)=$$

$$=|K|^{-1}\sum_{\substack{k\in K:\\ \psi(k)=0}}\Pr(\xi_k^{(t)}\in A_0)+|K|^{-1}\sum_{\substack{k\in K:\\ \psi(k)=1}}(1-\Pr(\xi_k^{(t)}\in A_0))=$$

$$=1/2\ +|K|^{-1}\sum_{\substack{k\in K:\\ \psi(k)=0}}\Pr(\xi_k^{(t)}\in A_0)-|K|^{-1}\sum_{\substack{k\in K:\\ \psi(k)=1}}\Pr(\xi_k^{(t)}\in A_0).$$

Отже,

$$2p_{\text{suc}}(A)-1=\left(\frac{|K|}{2}\right)^{-1}\sum_{\substack{k\in K:\\ \psi(k)=0}}\Pr(\xi_k^{(t)}\in A_0)\ -\left(\frac{|K|}{2}\right)^{-1}\sum_{\substack{k\in K:\\ \psi(k)=1}}\Pr(\xi_k^{(t)}\in A_0).$$

Для будь-якого $k\in K$ позначимо

$$p_k=\Pr\{\alpha X\oplus\beta F_k(X)=1\},\ \lambda_k=(2p_k-1)^2.$$

Внаслідок незалежності випадкових величин $\xi_{1,k},...,\xi_{t,k}$ виконуються рівності

$$\Pr(\xi_k^{(t)} \in A_0) = \sum_{a=(a_1,...,a_t)\in A_0} \Pr(\xi_{k,1} = a_1,...,\xi_{k,t} = a_t) =$$

$$= \sum_{a=(a_1,...,a_t)\in A_0} \Pr(\xi_{k,1} = a_1)\cdots \Pr(\xi_{k,t} = a_t) =$$

$$= \sum_{a=(a_1,...,a_t)\in A_0} p_k^{a_1}(1-p_k)^{1-a_1}\cdots p_k^{a_t}(1-p_k)^{1-a_t} = \sum_{a\in A_0} p_k^{wt(a)}(1-p_k)^{t-wt(a)},$$

з яких випливає, що

$$2p_{\text{suc}}(A)-1 = \left(\frac{|K|}{2}\right)^{-1} \sum_{\substack{k\in K:\\ \psi(k)=0}} \sum_{a\in A_0} (p_k^{wt(a)}(1-p_k)^{t-wt(a)} - 2^{-t}) -$$

$$-\left(\frac{|K|}{2}\right)^{-1} \sum_{\substack{k\in K:\\ \psi(k)=1}} \sum_{a\in A_0} (p_k^{wt(a)}(1-p_k)^{t-wt(a)} - 2^{-t}).$$

Отже, на підставі формули (2.19) мають місце нерівності

$$|2p_{\text{suc}}(A)-1| \le \left(\frac{|K|}{2}\right)^{-1} \sum_{\substack{k\in K:\\ \psi(k)=0}} \left| \sum_{a\in A_0} (p_k^{wt(a)}(1-p_k)^{t-wt(a)} - 2^{-t}) \right| +$$

$$+\left(\frac{|K|}{2}\right)^{-1}\sum_{\substack{k\in K:\\ \psi(k)=1}}\left|\sum_{a\in A_0}(p_k^{wt(a)}(1-p_k)^{t-wt(a)}-2^{-t})\right|\le$$

$$\le\left(\frac{|K|}{2}\right)^{-1}\sum_{\substack{k\in K:\\ \psi(k)=0}}2\sqrt{t}\,|2p_k-1|+\left(\frac{|K|}{2}\right)^{-1}\sum_{\substack{k\in K:\\ \psi(k)=1}}2\sqrt{t}\,|2p_k-1|=$$

$$=4\sqrt{t}\,|K|^{-1}\sum_{k\in K}|2p_k-1|=4\sqrt{t}\,|K|^{-1}\sum_{k\in K}\lambda_k^{1/2}\le 4\sqrt{t}\left(|K|^{-1}\sum_{k\in K}\lambda_k\right)^{1/2},$$

де остання нерівність випливає з опуклості вгору функції $\sqrt{x}$, $x\ge 0$.

Таким чином, $p_{\mathrm{suc}}(A_0)\le 1/2+2\sqrt{t}\,\lambda^{1/2}$, де λ визначається за формулою (2.18), що й треба було довести. ►

Позначимо $\lambda_{\max}$ максимальне значення параметра (2.18) за всіма ненульовими векторами $a,b\in V_n$. З твердження 2.7 випливає, що шифр $\mathcal{B}$ є стійким відносно розглянутої лінійної атаки, якщо число $\lambda_{\max}$ має порядок 2^{-n}. Більш того, це твердження зводить задачу обґрунтування стійкості блокового шифру відносно лінійного методу криптоаналізу до знаходження верхніх меж параметра $\lambda_{\max}$, які надавали би змогу переконуватися у його малості. Як і у випадку різницевого криптоаналізу, остання задача є нетривіальною, проте для SPN-шифрів, таких як Rijndael та "Калина", створено ефективні методи її розв'язання. Зокрема, відомо [12], що для шифру Rijndael з довжиною блоку $n=128$ бітів та $r\ge 4$ раундами

шифрування $\lambda_{\max} \le 1.075 \cdot 2^{-106}$, в той час як для алгоритму "Калина" з довжиною блоку n та $r \ge 7$ раундами виконуються такі нерівності [9]:

$$\lambda_{\max} \le \begin{cases} 9^{16} \cdot 2^{-128} \approx 1.65 \cdot 2^{-78}, \text{ якщо } n = 128; \\ 9^{32} \cdot 2^{-256} \approx 1.35 \cdot 2^{-155}, \text{ якщо } n = 256; \\ 9^{64} \cdot 2^{-512} \approx 1.83 \cdot 2^{-310}, \text{ якщо } n = 512. \end{cases}$$

Наведені оцінки свідчать про обґрунтовану стійкість зазначених шифрів відносно лінійного методу криптоаналізу.

Зауважимо, що поряд з лінійним та різницевим відомо чимало інших статистичних методів криптоаналізу блокових шифрів. Узагальнення тверджень 2.6 та 2.7 на випадок зазначених методів міститься в [15, 16].

Завдання для самоконтролю

1. Розглянемо модифіковану версію SPN-шифру, в якій замість послідовного застосування до вхідного повідомлення в кожному раунді операції додавання раундового ключа, нелінійного перетворення та лінійного перетворення спочатку до відкритого тексту додаються усі раундові ключі, потім застосовуються усі лінійні, а потім – усі нелінійні перетворення. Оцініть стійкість такої конструкції.

2. Побудуйте атаку на 2-раундовий SPN-шифр з довжиною блоку n бітів та незалежними випадковими рівноймовірними раундовими ключами $k_1, k_2 \in V_n$, яка має часову складність $O(2^n)$ та використовує пам'ять обсягом $O(2^n)$ бітів.

3. Доведіть, що для розшифрування повідомлення (y_1, y_2), де $y_1, y_2 \in V_m$, за допомогою r-раундового шифру Фейстеля з довжиною блоку $2m$ бітів на ключі $(k_1,...,k_r)$ достатньо зашифрувати повідомлення (y_2, y_1) на ключі $(k_r,...,k_1)$ та поміняти місцями "половинки" отриманого шифротексту.

4. Знайдіть шифротекст, який отримується при зашифруванні відкритого тексту (x_1, x_2) за допомогою багатораундового шифру Фейстеля, раундова функція якого в кожному раунді є

а) константою 0;

б) тотожним відображенням.

5. Використовуючи символи операцій S, R, M, K, опишіть формально правила зашифрування та розшифрування повідомлень за допомогою алгоритму Rijndael з числом раундів $n_r = 4$.

6. Переконайтесь, що Rijndael є $(n_r + 1)$-раундовий SPN-шифром, який описується співвідношеннями (2.1), (2.2) та (2.3). Наведіть явні вирази лінійних перетворень, що використовуються в окремих раундах цього шифру.

7. Поясніть, чому в останньому раунді кожного з шифрів Rijndael та "Калина" не використовується жодних перетворень, окрім додавання раундового ключа.

8. Опишіть формально правила зашифрування та розшифрування повідомлень за допомогою алгоритму "Калина" з числом раундів $n_r = 3$.

9. Доведіть, що підстановка Ніберг та вузол заміни шифру Rijndael мають однакові максимальні елементи таблиці різниць та, відповідно, таблиці лінійних апроксимацій.

10. Припустимо, що існує атака на блоковий шифр з довжиною ключа n бітів, яка відновлює цей ключ, використовуючи n підібраних відкритих текстів зі складністю, помітно меншою за 2^n. Доведіть, що такий шифр не є стійким у сенсі означення 2.5.

11. Нехай F є випадковою рівноймовірною підстановкою на множині V_n. Доведіть, що при випадковому незалежному від F рівноймовірному виборі вектора X ймовірність події $\{F(X \oplus \alpha) \oplus F(x) = \beta\}$ дорівнює $(2^n - 1)^{-1}$ для будь-яких $\alpha, \beta \in V_n \setminus \{0\}$.

12. Розглянемо 1-раундовий SPN-шифр з двійковим ключовим сумато-ром та раундовою функцією вигляду (2.3). Покажіть, що його стійкість відносно різницевої (відповідно, лінійної) атаки визначається максимальними елементами таблиць різниць (відповідно, лінійних апроксимацій) його вузлів заміни.

13. Доведіть, що для підстановки Ніберг σ для будь-яких ненульових векторів $\alpha, \beta \in V_n$ число розв'язків рівняння $\sigma(x \oplus \alpha) \oplus \sigma(x) = \beta$ не перевищує 4. За яких умов досягається ця оцінка?

14. Нехай $L_1, L_2 : V_n \to V_n$ – оборотні лінійні перетворення, $F : V_n \to V_n$ – підстановка. Доведіть, що максимальні елементи таблиці різниць (відповідно, лінійних апроксимацій) підстановок F та $L_1 \circ F \circ L_2$ збігаються.

15. Нехай $\mathcal{B}$ – r-раундовий блоковий шифр з довжиною блоку n бітів. Розглянемо такий статистичний критерій для перевірки гіпотез H_0 і H_1, визначених в означенні 2.5: вибирається r-раундовий диференціал (α, β) шифру $\mathcal{B}$ з максимальною ймовірністю $D_{\max}(r)$; потім на вхід оракула Ф подається t незалежних випадкових рівноймовірних відкритих

текстів $X_1,...,X_t$ та перевіряється, чи збігається з вектором β хоча б одне значення $\Phi(X_i \oplus \alpha) \oplus \Phi(X_i)$, $i \in \overline{1,t}$. Якщо так, то приймається гіпотеза H_0; інакше приймається гіпотеза H_1. Доведіть, що середня ймовірність помилки цього критерію є не менше ніж $1/2 \cdot (1 - tD_{\max}(r))$.

3. ОСНОВНІ КОМПОНЕНТИ ТА ПРИНЦИПИ ПОБУДОВИ ПОТОКОВИХ ШИФРІВ

§ 3.1. Скінченні автомати

У цьому розділі вивчаються потокові шифри, що будуються на основі генераторів псевдовипадкових послідовностей (які називають також генераторами гами). Стандартною математичною моделлю, що описує функціонування таких генераторів, є скінченний автономний автомат.

Наведемо означення поняття автомата.

3.1. ОЗНАЧЕННЯ. Нехай X, S, Y – множини, а $h: S \times X \to S$ і $f: S \times X \to Y$ – функції. Тоді впорядкована п'ятірка (X, S, Y, h, f) називається *автоматом Мілі* (або просто *автоматом*) з множиною станів S, вхідним алфавітом X, вихідним алфавітом Y, функцією переходів h та функцією виходів f. Автомат називається *скінченним*, якщо кожна множина X, S, Y є скінченною.

Надалі розглядаються тільки скінченні автомати.

Кожен автомат $A = (X, S, Y, h, f)$ функціонує в дискретні моменти часу $i = 0, 1, 2, \ldots$, які називаються *тактами*. Він починає роботу з *початкового стану* $s_0 \in S$, і якщо на його вхід подається послідовність $x_0, x_1, \ldots$, де $x_i \in X$ для кожного $i = 0, 1, 2, \ldots$, то автомат A формує *внутрішню послідовність* (або *послідовність станів*) $s_{i+1} = h(s_i, x_i)$ та *вихідну послідовність* $y_i = f(s_i, x_i)$, $i = 0, 1, 2, \ldots$.

Проілюструємо процес роботи скінченного автомата у перших двох тактах. Нехай він знаходиться у початковому стані s_0, і в нульовому такті

на його вхід подається знак x_0. Тоді автомат переходить в наступний стан $s_1 = h(s_0, x_0)$ та формує знак вихідної послідовності $y_0 = f(s_0, x_0)$. Тепер, в першому такті, автомат знаходиться в стані s_1 та отримує на вхід наступний знак x_1. Тоді він переходить у стан $s_2 = h(s_1, x_1)$ і формує знак вихідної послідовності $y_1 = f(s_1, x_1)$.

Умовну схему роботи автомата в i-ому такті показано на рис. 3.1.

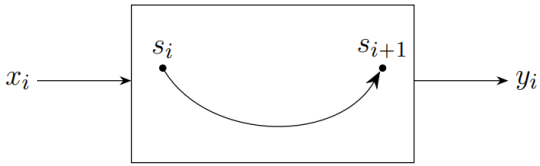

Рис. 3.1. Скінченний автомат в i-ому такті

Розглянемо основні види скінченних автоматів.

1. Автомат A називається *автоматом Мура*, якщо функція виходів f не залежить від змінної x. Таким чином, залежність $f(s, x)$ від x є фіктивною, і вихід автомата визначається тільки його станом.

2. Автомат A називається *автономним*, якщо обидві функції f та h не залежить від змінної x. Тоді немає сенсу розглядати вхідний алфавіт, а функції f та h можна вважати заданими на множині станів:

$$\forall x \in X, s \in S : f(s, x) = f(s), h(s, x) = h(s).$$

В цьому випадку автомат визначається як набір з чотирьох об'єктів $A = (S, Y, h, f)$, де $h : S \to S$, $f : S \to Y$. Таким автомат починає роботу з

деякого початкового стану і формує вихідну послідовність, яка цілком залежить тільки від цього стану.

3. Автомат A називається *автоматом без пам'яті*, якщо $|S|=1$. В цьому випадку можна виключити з розгляду множину S та не розглядати також функцію h, яка є константою. В результаті автомат зводиться лише до функції $f: X \to Y$. Отже, автомат без пам'яті фактично являє собою відображення однієї скінченної множини в іншу.

4. Автомат A називається *автоматом без виходу*, якщо $|Y|=1$. Такий автомат не виробляє вихідні знаки, а вхідні використовуються тільки для оновлення станів. При цьому можна не розглядати функцію f, яка вироджується у константу. Таким чином, автомат без виходу є просто функцією переходів $h: S \times X \to S$.

3.2. ПРИКЛАД. Будь-яка дискретна функція $f: X \to Y$ є автоматом без пам'яті. При цьому обчислення значень такої функції відбувається потактно за правилом $y_i = f(x_i),\ i = 0,1,2,\ldots$.

Блоковий шифр можна розглядати як автомат без виходу. Дійсно, такий шифр являє собою набір підстановок ($f_k: V_n \to V_n : k \in K$), де K позначає множину ключів шифру, $V_n = \{0,1\}^n$. Опишемо цей шифр скінченним автоматом без виходу, вважаючи

$$S = V_n,\ X = K,\ h(x,k) = f_k(x),\ x \in S,\ k \in X$$

(отже, в ролі вхідного символу використовується ключ, а в ролі стану – повідомлення, яке перетворюється за допомогою цього ключа; рис. 3.2).

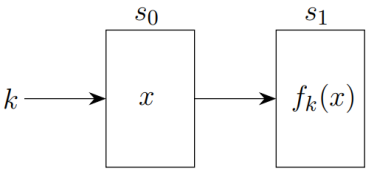

Рис. 3.2. Блоковий шифр як скінченний автомат

Якщо шифр є ітераційним і в ролі ключа k використовується послідовність раундових ключів $k=(k_1,...,k_r)$, то ці ключі застосовуються один за одним до проміжних повідомлень з множини V_n, які розглядаються як стани автомата. В цьому випадку відкритий текст відіграє роль початкового стану автомата, який перетворює цей стан в послідовність проміжних повідомлень-станів за допомогою раундових ключів.

Таке представлення блокового шифру надає змогу будувати та використовувати для подальшого аналізу теоретико-автоматні моделі блокових шифрів.

§ 3.2. Граф автомата. Необоротність автоматів за Гаффманом

Кожний автомат може бути представлений у вигляді певного графа.

3.3. ОЗНАЧЕННЯ. *Графом автомата* $A=(X,S,Y,h,f)$ називається позначений орієнтований граф $G_A=(V,E)$, множина V вершин якого збігається з множиною станів S автомата A, а множина E ребер складається з усіх впорядкованих пар (s,s') таких, що існує елемент $x\in X$, для якого виконується рівність $h(s,x)=s'$. Це ребро позначається символом (x,y), де x зазначено вище, а $y=f(s,x)$.

Зауважимо, що за означенням з кожної вершини s графу G_A виходить точно $|X|$ ребер, позначених символами $(x, f(s,x))$, де $x \in X$.

3.4. ПРИКЛАД. Нехай $A_1 = (X, S, Y, h, f)$, де

$$X = S = Y = \{0,1\},\ \ h(s,x) = x,\ \ f(s,x) = s \oplus x,\ \ \ s, x \in \{0,1\};$$

граф цього автомата зображено на рис. 3.3 (зліва).

Нехай, далі, $A_2 = (X, S, Y, h, f)$, де

$$X = S = Y = \{0,1\},\ \ h(s,x) = x,\ \ f(s,x) = sx,\ \ \ s, x \in \{0,1\}.$$

граф цього автомата зображено на рис. 3.3 (справа).

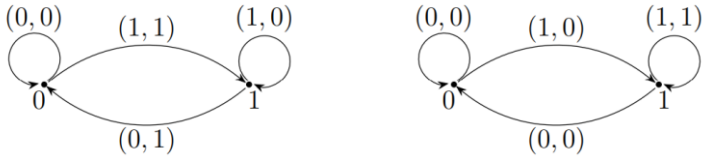

Рис. 3.3. Графи автоматів A_1 та A_2

Розглянемо властивість скінченного автомата, сформульовану Гаффманом [17].

3.5. ОЗНАЧЕННЯ. Автомат $A = (X, S, Y, h, f)$ називається *необоротним за Гаффманом* (або *автоматом з втратою інформації*), якщо для деякої пари станів $s, s' \in S$ у графі G_A між цими станами існують шляхи з

позначками $(x_0, y_0),...,(x_{k-1}, y_{k-1})$ та $(x_0', y_0),...,(x'_{k-1}, y_{k-1})$ відповідно такі, що $x_0,...,x_{k-1}$ та $x_0',...,x'_{k-1}$ – два різні набори вхідних символів, $k \geq 1$.

Інакше кажучи, автомат є необоротним за Гаффманом, якщо в його графі існують шляхи, зображені на рис. 3.4 (зауважимо, що в кожному зі шляхів стани можуть повторюватись, наприклад, шлях може включати лупи).

Нехай про автомат A відомі такі дані:

– стан s_0, з кого він почав працювати;

– стан s_k, в якому він закінчив працювати, $k \geq 1$;

– вихідна послідовність $y_0,..., y_{k-1}$, отримана в результаті переходу зі стану s_0 у стан s_k.

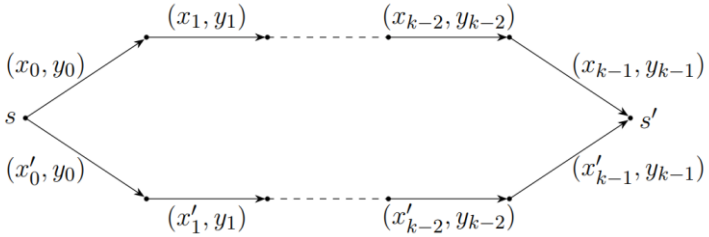

Рис. 3.4. Шляхи у графі G_A, які свідчать про необоротність автомата за Гаффманом

Тоді якщо автомат A є необоротним за Гаффманом, то, взагалі кажучи, за цими даними неможливо однозначно відновити відповідну вхідну послідовність $x_0,...,x_{k-1}$ (див. рис. 3.4). Навпаки, для оборотного за Гаффманом автомата за будь-якою вихідною послідовністю та парою ста-

нів (початковим і фінальним) завжди можна однозначно відновити відповідну вхідну послідовність.

3.6. ПРИКЛАД. Розглянемо граф G_{A_2} з прикладу 3.4 та два різні шляхи у цьому графі:

$$0 \xrightarrow{(1,0)} 1 \xrightarrow{(0,0)} 0,$$

$$0 \xrightarrow{(0,0)} 0 \xrightarrow{(0,0)} 0.$$

Послідовність вхідних символів першого шляху має вигляд $1,0$, а другого шляху – $0,0$, і ці послідовності є різними. При цьому послідовність вихідних символів як першого, так і другого шляху має вигляд $0,0$. Отже, автомат A_2 є необоротним за Гаффманом. Зауважимо, що наведені шляхи мають довжину 2. При цьому побудувати коротші шляхи у графі, які б свідчили про необоротність цього автомата, неможливо.

Таким чином, якщо автомат A_2 почав роботу зі стану 0, пропрацював два такти, зупинився також у стані 0 та згенерував вихідну послідовність $0,0$, то неможливо встановити однозначно, яка послідовність була подана на вхід – $0,0$ або $1,0$.

3.7. ПРИКЛАД. Розглянемо автомат A_1 з прикладу 3.4 та переконаємось, що він є оборотним за Гаффманом. У графі G_{A_1} розглянемо довільний шлях, який починається зі стану s_0, завершується в стані s_k та складається з ребер, позначених парами $(x_i, y_i), i \in \overline{0,k-1}, k \geq 1$. Використовуючи співвідношення $s_{i+1} = h(s_i, x_i) = x_i,\ y_i = f(s_i, x_i) = s_i \oplus x_i, i \in \overline{0,k-1}$, можна скласти таку систему лінійних рівнянь:

$$\begin{cases} s_0 \oplus x_0 = y_0, \\ \dots \\ s_{k-1} \oplus x_{k-1} = y_{k-1}, \\ s_1 = x_0, \\ \dots \\ s_k = x_{k-1}. \end{cases}$$

Розв'язуючи цю систему відносно змінних x_i, $i \in \overline{0, k-1}$, отримаємо, що

$$x_0 = s_0 \oplus y_0,$$

$$x_1 = s_1 \oplus y_1 = x_0 \oplus y_1 = s_0 \oplus y_0 \oplus y_1,$$

$$\dots \quad \dots \quad \dots \quad \dots$$

$$x_{k-1} = s_{k-1} \oplus y_{k-1} = x_{k-2} \oplus y_{k-1} = s_0 \oplus y_0 \oplus \dots \oplus y_{k-1}.$$

Таким чином, наведена система рівнянь має єдиний розв'язок $(x_0, x_1, \dots, x_{k-1})$ і автомат A_1 є оборотним за Гаффманом.

З криптографічної точки зору необоротність за Гаффманом є бажаною властивістю автомата, оскільки вона гарантує неможливість однозначного відновлення його входу за виходом. Дослідимо докладніше міру такої неоднозначності. Для цього введемо одне додаткове поняття.

3.8. ОЗНАЧЕННЯ. Нехай $A = (X, S, Y, h, f)$ – скінченний автомат, k – натуральне число. Тоді відображення

$$s_0, x_0, x_1, \dots x_{k-1} \mapsto y_0, y_1, \dots y_{k-1},$$

де $s_0 \in S$, $x_i \in X$, $y_i = f(s_i, x_i)$, $s_{i+1} = h(s_i, x_i)$ для кожного $i \in \overline{0, k-1}$, називається *автоматним відображенням, обмеженим на довжині* k, що відповідає автомату A.

Позначимо це відображення символом $F_k : S \times X^k \to Y^k$. Кажучи неформально, воно переводить вхідну послідовність $x_0, x_1, \ldots, x_{k-1}$ у вихідну послідовність $y_0, y_1, \ldots, y_{k-1}$ за умови, що автомат починає працювати зі стану s_0.

Позначимо для зручності $\bar{x} = (x_0, \ldots, x_{k-1})$ та $\bar{y} = (y_0, \ldots, y_{k-1})$. Тоді значення автоматного відображення F_k на вхідному наборі $(s_0, \bar{x})$ обчислюється таким чином:

$$F_k(s_0, \bar{x}) = \bar{y}.$$

Якщо потрібно знайти всі можливі набори $(s_0, \bar{x})$, які відповідають певній вихідній послідовності $\bar{y}$, то розглядається її прообраз при відображенні F_k:

$$F_k^{-1}(\bar{y}) = \{(s_0, \bar{x}) \in S \times X^k \mid F_k(s_0, \bar{x}) = \bar{y}\}.$$

Позначимо $\eta_k(\bar{y}) = |F_k^{-1}(\bar{y})|$ потужність цього прообразу, яка збігається з числом розв'язків $(s_0, \bar{x})$ системи рівнянь

$$\begin{cases} f(s_0, x_0) = y_0, \\ \quad \ldots \\ f(s_{k-1}, x_{k-1}) = y_{k-1}, \\ s_1 = h(s_0, x_0), \\ \quad \ldots \\ s_k = h(s_{k-1}, x_{k-1}). \end{cases} \tag{3.1}$$

Доведемо таке твердження.

3.9. ТВЕРДЖЕННЯ. Нехай $A=(X,S,Y,h,f)$ – скінченний автомат. Якщо він є оборотним за Гаффманом, то для кожного $\bar{y}\in Y^k$ система рівнянь (3.1) має не більше $|S|^2$ розв'язків.

Окрім того, за умови $|X|>|Y|$ автомат A є необоротним за Гаффманом.

◄ Нехай автомат A є оборотним за Гаффманом. Тоді для будь-яких фіксованих значень змінних s_0 та s_k система рівнянь (3.1) має не більше одного розв'язку. Дійсно, число таких розв'язків дорівнює числу шляхів у графі автомата A, що мають позначки над ребрами $(x_0,y_0),...,(x_{k-1},y_{k-1})$, починаються у вершині s_0 та закінчуються у вершині s_k, а їхня кількість не перевищує 1 на підставі означення 3.5. Таким чином, загальна кількість розв'язків системи (3.1) не перевищує числа усіх пар $(s_0,s_k)\in S\times S$, тобто $|S|^2$, що й треба було довести.

Припустимо зараз, що $|X|>|Y|$ та доведемо, що автомат A не є оборотним за Гаффманом. Обчислимо середнє значення числа прообразів вихідних послідовностей при відображенні F_k, тобто суму

$$\frac{1}{|Y|^k}\sum_{\bar{y}\in Y^k}\eta_k(\bar{y}).$$

Справедлива рівність $S\times X^k=\bigcup_{\bar{y}\in Y^k}F_k^{-1}(\bar{y})$, причому множини $F_k^{-1}(\bar{y})$ в об'єднанні попарно не перетинаються (рис. 3.5).

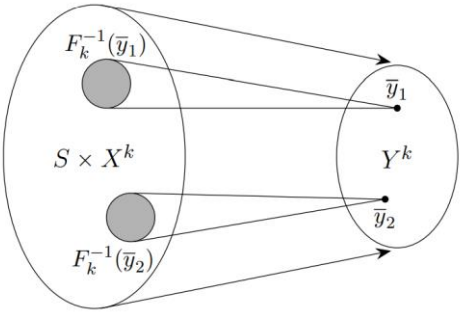

Рис. 3.5. Прообрази елементів $\bar{y}_1$ та $\bar{y}_2$ при відображенні F_k не перетинаються

Звідси випливає, що

$$\bigcup_{\bar{y}\in Y^k} F_k^{-1}(\bar{y}) = \sum_{\bar{y}\in Y^k} |\, F_k^{-1}(\bar{y})\,| = \sum_{\bar{y}\in Y^k} \eta_k(\bar{y}) = |\, S\,| \cdot |\, X\,|^k$$

і, отже,

$$\frac{1}{|\, Y\,|^k} \sum_{\bar{y}\in Y^k} \eta_k(\bar{y}) = \frac{1}{|\, Y\,|^k} \cdot |\, S\,| \cdot |\, X\,|^k = |\, S\,| \cdot \left(\frac{|\, X\,|}{|\, Y\,|}\right)^k .$$

З нерівності $|\, X\,| > |\, Y\,|$ випливає, що при $k \to \infty$ середнє значення числа прообразів прямує до нескінченності:

$$\frac{1}{|\, Y\,|^k} \sum_{\bar{y}\in Y^k} \eta_k(\bar{y}) \to \infty .$$

З іншого боку, якщо автомат A є оборотним за Гаффманом, то за доведеним для кожного $\bar{y} \in Y^k$ справедлива нерівність $\eta_k(\bar{y}) \le |\, S\,|^2$. Таким чи-

ном, за умови $|X|>|Y|$ автомат A є необоротним за Гаффманом, що й треба було довести. ►

§ 3.3. Генератори гами

3.10. ОЗНАЧЕННЯ. *Генератором гами* (або *генератором псевдовипадкових послідовностей*) називаються скінченний автономний автомат $\Gamma = (S, Y, h, f)$, де S – множина станів генератора, Y – вихідний алфавіт, $h: S \to S$ – функція переходів, а $f: S \to Y$ – функція виходів генератора гами.

За початковим станом s_0 генератор Γ виробляє послідовності $s_{i+1} = h(s_i)$ та $\gamma_i = f(s_i), i = 0,1,2,...,$ остання з яких називається *гамою*. Позначаючи h^i i-й степінь функції h відносно операції композиції відображень, отримаємо, що початковий стан генератора гами задовольняє систему рівнянь

$$f(h^i(s_0)) = \gamma_i, i = 0,1,2,...,$$

яка називається *системою рівнянь гамоутворення* генератора Γ.

Генератор гами можна розглядати як сім'ю певних відображень.

3.11. ОЗНАЧЕННЯ. Нехай $\Gamma = (S, Y, h, f)$ – генератор гами, L – натуральне число. Тоді відображення $s_0 \mapsto \gamma_0, \gamma_1, ..., \gamma_{L-1}$, де $s_0 \in S$, $\gamma_i = f(s_i), s_{i+1} = h(s_i)$ для кожного $i \in \overline{0, L-1}$, називається *гамоутворювальним відображенням, обмеженим на довжині* L, яке відповідає генератору гами Γ.

Позначимо це відображення символом $\Gamma_L : S \to Y^L$.

З кожним генератором можна пов'язати набір гамоутворювальних відображень, параметризованих натуральними числами $L = 1, 2, \ldots$. Значенням кожного такого відображення є відрізок гами певної довжини, вироблений за початковим станом генератора.

Характеристичною властивістю гамоутворюючого відображення є *перетворення початку в початок*. А саме, для будь-яких натуральних чисел L_1 та L_2, де $L_1 < L_2$, і довільного початкового стану s_0 генератора гами Γ виконується рівність

$$\Gamma_{L_2}(s_0) = \Gamma_{L_1}(s_0) \cdot B,$$

де B – деяке слово довжини $L_2 - L_1$ над вихідним алфавітом Y, а символ $\cdot$ позначає конкатенацію слів (тобто послідовностей знаків гами).

Ця властивість випливає безпосередньо з означення гамоутворювального відображення. Таким чином, при обчисленні значень цих відображень початки слів зберігаються. Не дивлячись на тривіальність зазначеної властивості, вона іноді використовується при побудові атак на генератори гами.

З криптографічної точки зори основною вимогою до якісного генератора гами є *псевдовипадковість*. Для того, щоб навести формальне означення цього поняття, розглянемо таку *гру між Дослідником та Криптоаналітиком*.

1. Дослідник випадково рівноймовірно генерує початковий стан s_0 генератора гами $\Gamma = (S, Y, h, f)$. Після цього він з ймовірністю $1/2$ вибирає або відрізок гами $\gamma = \gamma_0, \ldots, \gamma_{L-1}$, вироблений генератором за початко-

вим станом s_0, або випадкову рівноймовірну послідовність довжини L над алфавітом Y.

2. Дослідник передає Криптоаналітику послідовність $y = y_0,...,y_{L-1}$, отриману в результаті вибору, зробленого на кроці 1.

3. Криптоаналітик, використовуючи будь-який статистичний критерій, розв'язує задачу перевірки гіпотез H_0 та H_1, що визначаються таким чином: $H_0 : y = \gamma$; $H_1 :$ y є суто випадковою послідовністю.

3.12. ОЗНАЧЕННЯ. Нехай $T > 0$, $0 < \varepsilon < 1/2$. Генератор гами Γ називається (T, L, ε)-*псевдовипадковим*, якщо будь-який критерій для розрізнення зазначених вище гіпотез H_0 та H_1 за вихідною послідовністю довжини L із середньою ймовірністю помилки не вище ε, виконує принаймні T умовних операцій.

Іншими словами, генератор гами є (T, L, ε)-псевдовипадковим, якщо не існує способу відрізнити його вихідну послідовність довжини L, отриману при випадковому рівноймовірному початковому стані, від суто випадкової послідовності такої ж довжини над алфавітом Y з середньою ймовірністю помилки не вище за ε, використовуючи менше ніж T операцій.

Псевдовипадковість генератора гами (для певних значень параметрів L, T, ε) свідчить про його криптографічну стійкість. Наприклад, якщо довжина початкового стану генератора дорівнює $\log|S| = 128$ бітам, то такий генератор можна вважати стійким за умови його (T, L, ε)-псевдовипадковості при $L = 2^{80}$, $\varepsilon = 1/2 - 2^{-20}$, $T = 2^{128}$.

Означення 3.12 є загальновизнаним, але наразі не існує методів для доведення псевдовипадковості генераторів гами. Більш того, існування

псевдовипадкових генераторів близько пов'язано з проблемою існування важкооборотних функцій, яка є на сьогодні відкритою.

В деяких випадках можна показати, що генератор гами не є псевдовипадковим. Зокрема, такою є ситуація, коли за гамою можна відновити початковий стан генератора. Точніше, як показує наступне твердження, за умови існування ефективного алгоритму відновлення початкового стану можна ефективно відрізнити гаму, вироблену генератором, від суто випадкової послідовності.

3.13. ТВЕРДЖЕННЯ. Нехай $\Gamma = (S, Y, h, f)$ – генератор гами, де $S = V_N, Y = V_2$. Нехай, далі, існує (ймовірнісний) алгоритм A, який за відрізком гами $\Gamma_L(s_0)$ довжини $L > N$ відновлює початковий стан s_0 генератора з ймовірністю помилки ε, використовуючи T операцій. Тоді існує статистичний критерій B, який розрізнює гіпотези H_0 та H_1 в описаній вище грі між Дослідником та Криптоаналітиком із середньою ймовірністю помилки $p_{err} \le 1/2 \cdot (\varepsilon + 2^{N-L})$, використовуючи $T + \tau_L$ операцій, де τ_L – складність обчислення відрізка гами довжини L за початковим станом генератора.

◄ Нагадаємо, що під час гри Дослідник випадково рівноймовірно генерує початковий стан s_0 генератора гами та передає Криптоаналітику послідовність y, яка з ймовірністю $1/2$ збігається з відрізком гами $\Gamma_L(s_0)$ і з такою ж ймовірністю є випадковою рівноймовірною послідовністю довжини L над алфавітом Y.

Визначимо статистичний критерій B таким чином. Застосовуючи до послідовності y алгоритм A, отримаємо певний стан s_0^* генератора Γ,

за яким обчислити відрізок гами $\Gamma_L(s_0^*)$. Якщо $y = \Gamma_L(s_0^*)$, приймемо гіпотезу H_0; інакше – приймемо гіпотезу H_1.

Зрозуміло, що число операцій, потрібних для виконання критерію B (без урахування складності порівняння послідовностей y та $\Gamma_L(s_0^*)$) дорівнює $T + \tau_L$. Тому для завершення доведення залишається переконатися у справедливості нерівності $p_{err} \le 1/2 \cdot (\varepsilon + 2^{N-L})$.

За означенням середньої ймовірності помилки

$$p_{err} = 1/2 \cdot (\Pr(H_1 \mid H_0) + \Pr(H_0 \mid H_1)). \qquad (3.2)$$

Нехай справджується гіпотеза H_0, тобто $y = \Gamma_L(s_0)$, і критерій B припускається помилки. Тоді $\Gamma_L(s_0) \ne \Gamma_L(s_0^*)$ і, отже, $s_0 \ne s_0^*$, тобто алгоритм A припускається помилки. Оскільки ймовірність останньої події дорівнює ε, то ймовірність помилки критерію B, за умови справжності гіпотези H_0, є $\Pr(H_1 \mid H_0) \le \varepsilon$.

Нехай зараз справджується гіпотеза H_1, тобто y є суто випадковою послідовністю довжини L над алфавітом Y, і критерій B припускається помилки. Тоді існує початковий стан s генератора гами (а саме, $s = s_0^*$) такий, що $y = \Gamma_L(s)$, причому ймовірність останньої події (для будь-якого фіксованого $s \in S$) дорівнює 2^{-L}. Звідси, враховуючи рівність $|S| = 2^N$, отримаємо $\Pr(H_1 \mid H_0) \le 2^{N-L}$.

Підставляючи наведені оцінки ймовірностей $\Pr(H_1 \mid H_0)$ та $\Pr(H_0 \mid H_1)$ у формулу (3.2), отримаємо потрібну нерівність $p_{err} \le 1/2 \cdot (\varepsilon + 2^{N-L})$. ►

§ 3.4. Генератори гами на базі лінійних регістрів зсуву

Традиційний метод синтезу генераторів гами полягає в побудові генератора у вигляді послідовного з'єднання двох автоматів: *генератора попередньої гами* та *блоку ускладнення*. В ролі генераторів попередніх гам використовуються переважно лінійні регістри зсуву (ЛРЗ), які, за умови примітивності їхніх поліномів зворотного зв'язку, надають змогу отримувати псевдовипадкові послідовності з гарними статистичними та структурними властивостями. Призначення блоку ускладнення полягає у запобіганні простоти аналітичної (лінійної) залежності, що пов'язує знаки вихідної послідовності ЛРЗ з його початковим станом.

Нехай F – поле з q елементів, $f(x) = x^m - c_{m-1}x^{m-1} - ... - c_0x^0$ – поліном степеня $m \geq 2$ над цим полем, де $c_0 \neq 0$.

3.14. ОЗНАЧЕННЯ. *Лінійний регістр зсуву* довжини m над полем F з *поліномом зворотного зв'язку* $f(x)$ визначається як автономний автомат з множиною станів F^m та функцією переходів

$$h(z_{m-1},..., z_0) = (z_{m-1},..., z_0)S_f, (z_{m-1},..., z_0) \in F^m,$$

де

$$S_f = \begin{pmatrix} c_{m-1} & 1 & 0 & \cdots & 0 \\ c_{m-2} & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ c_1 & 0 & 0 & \cdots & 1 \\ c_0 & 0 & 0 & \cdots & 0 \end{pmatrix}. \qquad (3.3)$$

Комірки ЛРЗ і координати вектора, який зберігається у регістрі в i-му такті, нумеруються як зазначено на рис. 3.6. Цей регістр виробляє за

початковим станом $(x_{m-1},...,x_0) \in F^m$ *лінійну рекурентну послідовність* (або *лінійну рекурентну*) $x_0, x_1,...$ таку, що

$$(x_{i+m},...,x_{i+1}) = (x_{i+m-1},...,x_i)S_f, \ i \in 0,1,.... \tag{3.4}$$

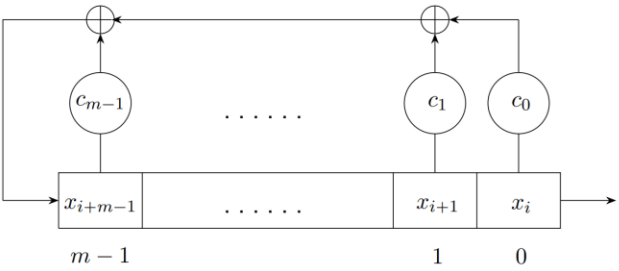

Рис. 3.6. Лінійний регістр зсуву

Наступне твердження надає явний вираз стану лінійного регістру зсуву в i -му такті через його початковий стан.

3.15. ТВЕРДЖЕННЯ. Для будь-якого $i \in 0,1,...$ виконується рівність

$$(x_{i+m-1},...,x_i) = (x_{m-1},...,x_0)S_f^i. \tag{3.5}$$

◄ Формула (3.5) випливає безпосередньо з формули (3.4) та доводиться за допомогою індукції по i . ►

Дослідимо докладніше властивості лінійних регістрів зсуву.

Нагадаємо, що послідовність $a = (a_i : i = 0,1,...)$ елементів довільної множини називається *періодичною*, якщо існують цілі числа $i_0 \geq 0$ і $T \geq 1$ такі, що $a_{i+T} = a_i$ для кожного $+i \geq i_0$. Найменше число T з такою влас-

тивістю називається *періодом* послідовності a та позначається $T(a)$. Послідовність a називається *чисто періодичною*, якщо $i_0 = 0$.

Неважко переконатися в тому (див. задачу 10), що вихідна послідовність будь-якого генератора гами є періодичною. Оскільки повторне використання шифрувальної гами зменшує стійкість шифрування (і тому є неприпустимим), то якісні генератори повинні виробляти послідовності великого періоду, значення якого напевно виключає повторення гами.

Однією з гарних властивостей ЛРЗ є можливість швидкого отримання попередньої гами, що має гарантовано великий період.

3.16. ОЗНАЧЕННЯ. Поліном $f(x)$ степеня m над полем F порядку q називається *примітивним* (або *поліномом максимального періоду*), якщо

1) він є незвідним (тобто не розкладається на співмножники, кожен з яких має степінь менше ніж m) над цим полем;

2) найменше натуральне t, для якого $f(x)$ ділить поліном $x^t - 1$, дорівнює $q^m - 1$.

Наступне твердження (яке наводиться без доведення) надає критерій максимальності періоду лінійної рекуренти, яка виробляється за допомогою ЛРЗ на рис. 3.6.

3.17. ТВЕРДЖЕННЯ. Період вихідної послідовності будь-якого ЛРЗ довжини m над полем F порядку q не перевищує $q^m - 1$. При цьому період дорівнює $q^m - 1$ тоді й тільки тоді, коли послідовність є ненульовою, а поліном зворотного зв'язку ЛРЗ – примітивним над полем F. ►

На практиці лінійні регістри зсуву, що використовуються в ролі генераторів попередніх гам, мають примітивні поліноми зворотного зв'язку.

Іншою гарною властивістю таких ЛРЗ є “майже рівномірність” розподілу частот появи наборів знаків їхніх вихідних послідовностей на повному періоді.

3.18. ТВЕРДЖЕННЯ. Нехай $x_0, x_1, \ldots$ є лінійною рекурентою максимального періоду, яка виробляється лінійним регістром зсуву довжини m над полем F порядку q. Тоді для будь-яких чисел $k \in \overline{1,m}$, $0 \le i_1 < \ldots < i_k \le m-1$ та довільного вектора $(a_1,\ldots,a_k) \in F^k$ число значень $i \in \overline{0, q^m - 2}$ таких, що $x_{i+i_1} = a_1, \ldots, x_{i+i_k} = a_k$, дорівнює q^{m-k} за умови, що a є ненульовим вектором, та $q^{m-k} - 1$ – у протилежному випадку.

◄ Запишемо вектори $(x_i, x_{i+1}, \ldots, x_{i+m-1})$, де $i \in \overline{0, q^m - 2}$, один під одним в таблицю, яку доповнимо нульовим вектором довжини m над полем F. Ця таблиця має розмір $q^m \times m$ і складається з різних рядків, оскільки $x_0, x_1, \ldots$ є лінійною рекурентою максимального періоду. Отже, вектори, що містяться в таблиці, утворюють множину F^m. Звідси випливає, що в будь-яких k стовпцях цієї таблиці кожен вектор $a = (a_1,\ldots,a_k) \in F^k$ зустрічається однакову кількість разів, яка дорівнює q^{m-k}. Отже, якщо a є ненульовим вектором, то існує саме стільки значень $i \in \overline{0, q^m - 2}$ з властивістю $x_{i+i_1} = a_1, \ldots, x_{i+i_k} = a_k$, а якщо $a = 0$, то на одне значення менше. ►

Наведене твердження показує, що лінійні рекуренти максимального періоду непогано імітують суто випадкові послідовності елементів поля F у сенсі рівноймовірності частот появи наборів знаків на повному періоді.

Таким чином, обираючи поліном зворотного зв'язку ЛРЗ примітивним, можна гарантувати як достатню величину періоду, так і гарні статистичні властивості вихідних послідовностей. Поряд з тим, аналітичний опис лінійних рекурент є надто простим: для визначення початкового стану ЛРЗ за довільним відрізком його вихідної послідовності достатньо розв'язати систему лінійних рівнянь. Тому для створення якісних генераторів гами на базі ЛРЗ необхідно використовувати елементи ускладнення, що базуються на нелінійних перетвореннях.

На сьогодні відомо чимало різноманітних способів ускладнення ЛРЗ, з яких традиційно виділяють три базові конструкції:

– генератори із застосуванням фільтрувальних функцій (*фільтрувальні генератори гами*);

– генератори із застосуванням комбінувальних функцій (*комбінувальні генератори гами*);

– генератори із застосуванням нерівномірності руху ЛРЗ (*генератори гами з нерівномірним рухом*);

На рис. 3.7 показано криптосхеми фільтрувального та комбінувального генераторів гами. Зазначені генератори є класичними та застосовуються у багатьох конструкціях сучасних потокових шифрів.

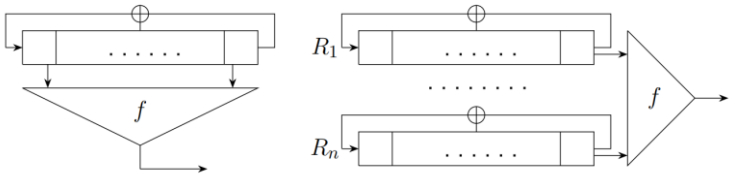

Рис. 3.7. Фільтрувальний (зліва) та комбінувальний генератори гами

Одним із загальних способів підвищення криптографічної стійкості генераторів гами є ускладнення законів їх функціонування шляхом введення нерівномірності руху ЛРЗ, що входять до складу таких генераторів. Зазвичай ефект нерівномірності руху досягається одним із двох можливих способів: на основі зовнішнього управління рухом лінійних регістрів зсуву або шляхом самоуправління, тобто встановлення детермінованої залежності величини зсуву ЛРЗ генератора в кожному такті від його поточного стану.

Наведемо означення генератора гами із зовнішнім управлінням рухом.

Нехай $\Gamma = (S, Y, h, f)$ – генератор гами, (U, p_U) – дискретне джерело без пам'яті, де $U \subseteq \{0, 1, ...\}$, p_U – розподіл ймовірностей на множині U. Це джерело виробляє послідовність незалежних випадкових величин $\varepsilon(0), \varepsilon(1),...,$ кожна з яких розподілена на множині U за законом $\Pr(\varepsilon(i) = a) = p_U(a), a \in U, i \in 0, 1, ...$.

Нагадаємо, що внутрішня послідовність генератора Γ, яка відповідає його початковому стану s_0, визначається за формулою

$$s_{i+1} = h(s_i), \quad i = 0, 1, 2, ...$$

Розглянемо випадкові величини $\delta(0) \equiv 0, \delta(i) = \varepsilon(0) + \ldots + \varepsilon(i-1)$, де $i = 1, 2, ...$, та визначимо послідовність $\gamma_0, \gamma_1, ...$ знаків алфавіту Y за формулою

$$\gamma_i = f(s_{\delta(i)}), \ i = 0, 1, ...$$

Зазначимо, що $\gamma_0, \gamma_1, \ldots$ є випадковою послідовністю, яка залежить від послідовності $\delta(0), \delta(1), \ldots$ та початкового стану s_0 генератора гами Γ. Здебільшого вважають, що s_0 є випадковим елементом, який не залежить від послідовності $\delta(0), \delta(1), \ldots$ та має рівномірний розподіл ймовірностей на множині S.

3.19. ОЗНАЧЕННЯ. Генератор, який функціонує за описаним вище правилом (поряд із джерелом U), називається *генератором гами із зовнішнім управлінням рухом* або U*-рухом*. Говорять про *обмежений* U*-рух,* якщо $|U| < \infty$, та *необмежений* U*-рух* у протилежному випадку.

Зазвичай на практиці в ролі джерела (U, p_U) виступає деякий автономний автомат, що виробляє псевдовипадкову послідовність $\varepsilon(0), \varepsilon(1), \ldots$ невід'ємних цілих чисел. Такий автомат інколи називають *блоком управління рухом* генератора гами Γ.

§ 3.5. Синхронні потокові шифри

3.20. ОЗНАЧЕННЯ. *Синхронний* (*адитивний двійковий*) *потоковий шифр* визначається за допомогою таких об'єктів.

1. Генератора гами $\Gamma = (S, Y, h, f)$, де $S = V_N$ для деякого натурального N та (зазвичай) $Y = V_2$.

2. Алгоритму формування початкового стану генератора за ключем і вектором ініціалізації

$$F : V_{l_0} \times V_{l_1} \to V_N,$$

де V_{l_0} – множина ключів (l_0 – довжина ключа), V_{l_1} – множина векторів ініціалізації (l_1 – довжина вектора ініціалізації). Цей алгоритм за ключем $k \in V_{l_0}$ та вектором ініціалізації $c \in V_{l_1}$ обчислює початковий стан генератора $s_0 = F(k,c)$, що є двійковим вектором довжини N.

3. Правила накладання гами, яке зазвичай визначається за формулою

$$y_i = x_i \oplus \gamma_i, \ i = 0, 1, ...,$$

де y_i та x_i – відповідно знаки шифротексту та відкритого тексту в i-му такті, $x_i, y_i \in V_2$.

Після формування початкового стану $s_0 = F(k,c)$ функціонування генератора описується за допомогою співвідношень $s_{i+1} = h(s_i)$, $\gamma_i = f(s_i), i = 0, 1, ...$ (рис. 3.8).

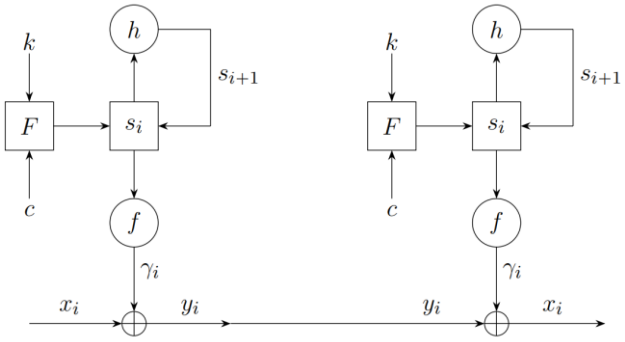

Рис. 3.8. Схематичне зображення процедури шифрування з використанням синхронного потокового шифру

Надалі термін потоковий шифр означає синхронний потоковий шифр. Зауважимо, що при побудові таких шифрів треба обов'язково визначати алгоритм формування початкового стану генератора гами, від якого, зокрема, залежить стійкість шифру. Саме у наявності такого алгоритму полягає суттєва відмінність між синхронним потоковим шифром та генератором гами.

Зауважимо також, що вектор ініціалізації є загальновідомим параметром і використовується для того, щоб змінювати стан генератора гами, не змінюючи при цьому ключ. Це надає змогу уникати багаторазового використання гами, в результаті чого знижується стійкість шифрування. Якщо в ролі F використовується лінійне відображення, то це є слабкістю з погляду стійкості (відомим шифром з лінійним відображенням F є алгоритм A5/1).

Сформулюємо означення поняття стійкого потокового шифру.

Для будь-якого $k \in V_{l_0}$ задамо відображення $F_k : V_{l_1} \to V_N$, вважаючи $F_k(c) = F(k,c), c \in V_{l_1}$. Позначимо також $\Gamma_L : V_N \to V_L$ гамоутворювальне відображення, обмежене на довжині L, що відповідає генератору Γ (див. означення 3.11), та визначимо відображення $\Phi_k = \Gamma_L \circ F_k$. Тоді синхронний потоковий шифр реалізує набір відображень ($\Phi_k : k \in V_{l_0}$) множини V_{l_1} векторів ініціалізації в множину V_L відрізків гами (рис. 3.9).

Розглянемо таку *гру між Дослідником та Криптоаналітиком*.

Дослідник випадково рівноймовірно вибирає ключ k з множини V_{l_0} та надає Криптоаналітику доступ до оракула Φ, який з ймовірністю $1/2$ збігається з відображенням Φ_k (гіпотеза H_0) та з такою ж ймовірністю –

із суто випадковим відображенням множини V_{l_1} в множину V_L (гіпотеза H_1).

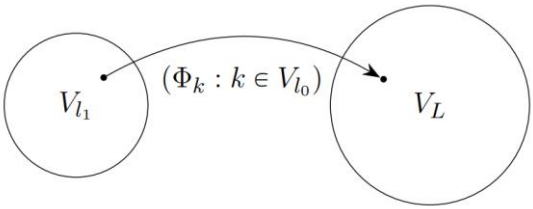

Рис. 3.9. Синхронний потоковий шифр
як набір відображень ($\Phi_k : k \in V_{l_0}$)

Криптоаналітик може звертатися до оракула Φ, обчислюючи значення $\Phi(c_1),\ldots,\Phi(c_t)$ для будь-яких векторів $c_1,\ldots,c_t \in V_{l_1}$ і повинен визначити, яка з гіпотез H_0 або H_1 є справжньою.

3.21. ОЗНАЧЕННЯ. Нехай $T > 0$, $0 < \varepsilon < 1/2$. Тоді синхронний потоковий шифр називається (T,t,ε)-*стійким*, якщо будь-який статистичний критерій для розрізнення двох зазначених вище гіпотез, що використовує t (довільних) векторів ініціалізації $c_1,\ldots,c_t \in V_{l_1}$ та має середню ймовірність помилки не вище ε, виконує принаймні T (умовних) операцій.

Зауважимо, що означення 3.21 є аналогічним означенню 2.5 стійкого блокового шифру. Воно сформувалося наприкінці нульових років цього століття в процесі проведення конкурсу Estream. Під час попереднього конкурсу Nessie, який відбувся у 2000 році, навіть не визначали різницю між потоковими шифрами та генераторами гами. При цьому всі шифри-

кандидати на тому конкурсі були зламані й переможця визначити не вдалось.

Як і для генераторів гами, наразі немає “беззаперечних” доведень стійкості потокових шифрів. Наявні доведення базуються на припущеннях про те, що певні математичні задачі є обчислювально складними. Наприклад, для шифру QUAD в роботі [18] отримано доведення стійкості з використанням припущення, що задача розв’язання випадково згенерованої системи квадратичних рівнянь над скінченним полем є обчислювально складною.

§ 3.6. SNOW 2.0-подібні шифри

Розглянемо клас потокових шифрів, які будуються аналогічно алгоритму шифрування SNOW 2.0 [19]. Зауважимо, що на сьогодні SNOW 2.0 є одним з найбільш швидких програмно орієнтованих потокових шифрів, який обрано як прототип для національного стандарту потокового шифрування – алгоритму “Струмок” [20].

На множині V_m двійкових векторів довжини $m \geq 2$ задамо структуру поля F_{2^m} (порядку 2^m), узгоджену з операцією $\oplus$ покоординатного булевого додавання двійкових векторів. Ототожнимо елементи цієї множини з m-розрядними цілими числами, вважаючи, що вектору $x = (x_1, x_2, \ldots, x_m) \in V_m$ відповідає число $x_1 + 2x_2 + \cdots + 2^{m-1}x_m$, та позначимо символом $+$ операцію додавання цих чисел за модулем 2^m.

Вхідними даними для побудови *SNOW 2.0-подібного потокового шифру з множиною ключів* V_{l_0} *та множиною векторів ініціалізації* V_{l_1} є

такі об'єкти:

– примітивний над полем F_{2^m} поліном $g(z) = z^n \oplus c_{n-1}z^{n-1} \oplus ... \oplus c_0$ степеня $n \geq 3$;

– натуральні числа l, μ, де $\mu \leq n-1$;

– ін'єктивне афінне відображення $L : V_{l_0} \times V_{l_1} \to V_m{}^n$;

– підстановка $\sigma : V_m \to V_m$.

Задамо перетворення h та H множини $V_m{}^n \times V_m{}^2$, вважаючи

$$h((x_{n-1}, x_{n-2}, ..., x_0), u, v) = ((x_n, x_{n-1}, ..., x_1), u', v')), \quad (3.6)$$

$$H((x_{n-1}, x_{n-2}, ..., x_0), u, v) = ((x_n \oplus w,\ x_{n-1}, ..., x_1), u', v')), \quad (3.7)$$

де $x_n = c_{n-1}x_{n-1} \oplus ... \oplus c_0 x_0$, $w = (x_{n-1} + u) \oplus v$, $u' = x_\mu + v$, $v' = \sigma(u)$.

Зауважимо, що внаслідок нерівності $c_0 \neq 0$, яка випливає з умови примітивності полінома $g(z)$, перетворення (3.6) і (3.7) є підстановками на множині $V_m{}^n \times V_m{}^2$.

Згідно із загальним означенням 3.20, SNOW 2.0-подібний шифр складається з алгоритму генерації гами та алгоритму формування початкового стану генератора за ключем і вектором ініціалізації.

Генератор гами (рис. 3.10) являє собою скінченний автономний автомат A з множиною внутрішніх станів $V_m{}^n \times V_m{}^2$, функцією переходів (3.6) та функцією виходів

$$f((x_{n-1}, x_{n-2}, ..., x_0), u, v) = x_0 \oplus (x_{n-1} + u) \oplus v. \quad (3.8)$$

Алгоритм формування початкового стану генератора залежить від параметра l і складається з двох етапів:

1) формування за ключем $k \in V_{l_0}$ та вектором ініціалізації $c \in V_{l_1}$ стану $\theta_0 = (L(k,c), 0, 0)$ автомата A;

2) обчислення початкового стану генератора гами за формулою

$$s_0 = h(H^l(\theta_0)), \tag{3.9}$$

де H^l позначає l-й степінь відображення H відносно операції композиції.

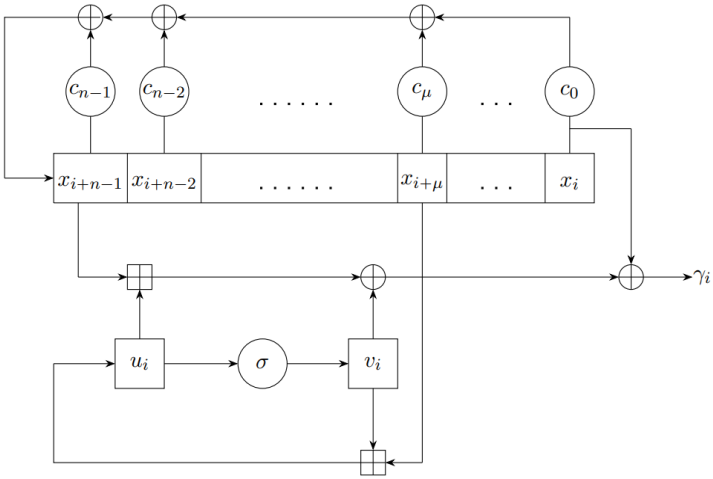

Рис. 3.10. Схема генератора гами SNOW 2.0-подібного шифру

Отже, на першому етапі за допомогою відображення L обчислюється вектор $L(k,c)$ довжини n над множиною V_m, який записується у на-

копичувач (рис. 3.10). Зазначений вектор, поряд з нульовими значеннями змінних u і v, утворює стан θ_0 автомата A. На другому етапі, згідно з формулою (3.9), обчислюється початковий стан

$$s_0 = ((x_{n-1}, x_{n-2}, \dots, x_0), u_0, v_0) .$$

Далі автомат функціонує за законом $s_{i+1} = h(s_i)$, $\gamma_i = f(s_i)$, $i = 0, 1, \dots$, проходячи послідовність станів $s_i = ((x_{i+n-1}, x_{i+n-2}, \dots, x_i), u_i, v_i)$ та формуючи вихідну послідовність (шифрувальну гаму) γ_i, $i = 0, 1, \dots$. Таким чином, стан генератора в i-му такті визначається за формулою

$$s_i = h^{i+1}(H^l(\theta_0)), \ i = 0, 1, \dots,$$

а знак вихідної послідовності – за формулою

$$\gamma_i = x_i \oplus (x_{i+n-1} + u_i) \oplus v_i , \ i = 0, 1, \dots .$$

Зауважимо, що змінними параметрами, від яких залежить визначений потоковий шифр, є примітивний над полем F_{2^m} поліном $g(z)$, числа l та μ, ін'єктивне афінне відображення L та підстановка σ.

3.22. ПРИКЛАД. У шифрі SNOW 2.0 використовуються такі параметри: $m = 32$, $n = 16$, $l = 32$, $\mu = 5$, $g(z) = z^{16} \oplus \alpha^{-1} z^{11} \oplus z^2 \oplus \alpha$, де α є певним примітивним елементом поля $F_{2^{32}}$. При цьому довжина вектора ініціалізації дорівнює $l_1 = 128$ бітів, а довжина ключа може приймати одне з двох значень: $l_0 = 128$ бітів або $l_0 = 256$ бітів. Підстановка σ задається

аналогічно раундовій функції блокового шифру Rijndael (див. § 2.2), а відображення L визначається таким чином:

1) якщо $l_0 = 128$ бітів, то

$$L(k_3, k_2, k_1, k_0, c_3, c_2, c_1, c_0) =$$

$$= (k_3^{c_0}, k_2, k_1, k_0^{c_1},\ \overline{k_3}, \overline{k_2}^{c_2}, \overline{k_1}^{c_3}, \overline{k_0},\ k_3, k_2, k_1, k_0,\ \overline{k_3}, \overline{k_2}, \overline{k_1}, \overline{k_0}),$$

де $k_i, c_i \in V_{32}$, $k^c = k \oplus c$, а $\overline{k}$ позначає вектор, який отримується шляхом інвертування усіх координат двійкового вектора k;

2) якщо $l_0 = 256$ бітів, то

$$L(k_7, k_6, \ldots, k_0, c_3, c_2, c_1, c_0) =$$

$$= (k_7^{c_0}, k_6, k_5, k_4^{c_1}, k_3, k_2^{c_2}, k_1^{c_3}, k_0, \overline{k_7}, \overline{k_6}, \ldots, \overline{k_0}),$$

де $k_i, c_i \in V_{32}$, а символи k^c, $\overline{k}$ мають той самий сенс, що і вище.

3.23. ПРИКЛАД. У шифрі "Струмок" використовуються такі параметри: $m = 64$, $n = 16$, $l = 32$, $\mu = 13$, $g(z) = z^{16} \oplus z^{13} \oplus \alpha^{-1} z^{11} \oplus \alpha$, де α є певним примітивним елементом поля $F_{2^{64}}$. При цьому довжина вектора ініціалізації дорівнює $l_1 = 256$ бітів, а довжина ключа може приймати одне з двох значень: $l_0 = 256$ бітів або $l_0 = 512$ бітів. Підстановка σ задається аналогічно раундовій функції шифру "Калина" (див. § 2.2), а відображення L визначається таким чином:

1) якщо $l_0 = 256$ бітів, то

$$L(k_3, k_2, k_1, k_0, c_3, c_2, c_1, c_0) =$$

$$= (k_3^{c_0}, k_2, k_1^{c_1}, k_0^{c_2},\ k_3,\ k_2^{c_3}, \overline{k_1}, \overline{k_0},\ k_3, k_2, \overline{k_1}, k_0,\ k_3, \overline{k_2}, k_1, \overline{k_0})\,;$$

2) якщо $l_0 = 512$ бітів, то

$$L(k_7, k_6, k_5, k_4, k_3, k_2, k_1, k_0, c_3, c_2, c_1, c_0) =$$

$$= (k_7^{c_0}, k_6, k_5, k_4^{c_1},\ k_3,\ k_2^{c_2}, k_1, \overline{k_0},\ k_4^{c_3}, \overline{k_6}, k_5, \overline{k_7},\ k_3, k_2, \overline{k_1}, k_0)\,,$$

де $k_i, c_i \in V_{64}$, а символи k^c, $\overline{k}$ мають той самий сенс, що й у прикладі 3.22.

Наведене означення SNOW 2.0-подібних потокових шифрів використовується при аналізі їхньої стійкості відносно низки сучасних атак [1, 21, 22, 23].

Завдання для самоконтролю

1. Побудуйте граф скінченного автомата та визначте, чи є цей автомат оборотним за Гаффманом, якщо

а) $X = S = Y = \{0,1\}$, $h(s,x) = sx \oplus x \oplus 1$, $f(s,x) = sx$;

б) $X = Y = \{0,1\}$, $S = \{0,1,2,3\}$, $h(0,0) = h(2,0) = 0$, $h(0,1) = h(2,1) = 1$, $h(1,0) = h(3,0) = 2$, $h(1,1) = h(3,1) = 3$, $f(s,x) = 0$ для усіх $s \in S$, $x \in X$, окрім $f(3,1) = 1$.

2. Нехай функція виходів f автомата A є такою, що для довільних $s \in S$ та $y \in Y$ існує єдиний елемент $x \in X$ з властивістю $f(s,x) = y$. Чи є такий автомат оборотним за Гаффманом? Чи виконується обернене твердження?

3. Побудуйте граф лінійного регістру зсуву довжини n над полем з двох елементів з поліномом зворотного зв'язку $f(x)$, якщо

а) $n = 3$, $f(x) = x^3 \oplus x \oplus 1$;

б) $n = 3$, $f(x) = x^3 \oplus x^2 \oplus 1$;

в) $n = 4$, $f(x) = x^4 \oplus x \oplus 1$;

б) $n = 4$, $f(x) = x^4 \oplus x^2 \oplus 1$.

Визначте, якими є довжини періодів вихідних послідовностей цього регістру.

4. Нехай $A = (X, S, Y, h, f)$, де $X = S = Y = \{0,1\}$, $f(s,x) = s \oplus x$, $h(s,x) = x$. Позначимо $\Phi(k)$ число розв'язків системи рівнянь (3.1) при $y_0 = ... = y_{k-1} = 0$. Знайдіть значення $\Phi(1)$, $\Phi(2)$ та доведіть, що $\Phi(k) = \Phi(k-1) \oplus \Phi(k-2)$ при $k \geq 3$.

5. Нехай Γ – генератор гами з множиною станів V_n та вихідним алфавітом $\{0,1\}$, який виробляє за початковим станом s_0 вихідну послідовність $\Gamma_L(s_0)$ довжини L. Покажіть, що існує статистичний критерій, який дозволяє відрізнити цю послідовність, отриману за випадковим рівноймовірним початковим станом, від суто випадкової двійкової послідов-

ності довжини L із середньою ймовірністю помилки p_e, використовуючи T двійкових операцій, якщо

а) $L = N+1$, $\Gamma_{N+1}(s_0) = (s_0, s)$, де s – сума за модулем 2 координат вектора s_0, $p_e = 1/4$, $T = N$;

б) $L = 2N$, $\Gamma_{2N}(s_0) = (s_0, s_0)$, $p_e = 2^{-N-1}$, $T = N$.

6. Розглянемо генератор гами Γ, який з початкового стану переходить у наступний стан, а далі звичайним чином виробляє гаму. Відновіть початковий стан генератора за відрізком гами γ, якщо:

а) Γ є фільтрувальним генератором, що складається з ЛРЗ довжини 3 з поліномом зворотного зв'язку $p(x) = x^3 \oplus x \oplus 1$ та функції ускладнення $f(z_0, z_1, z_2) = z_0 \oplus z_1 z_2$ (див. рис. 3.11, зліва), а $\gamma = 0, 1, 1$;

б) Γ є комбінувальним генератором гами, що складається з двох ЛРЗ довжини 3 з поліномами зворотного зв'язку $p_1(x) = x^3 \oplus x \oplus 1$ та $p_2(x) = x^3 \oplus x^2 \oplus 1$ відповідно та комбінувальної функції $f(z_1, z_2) = z_1 z_2$, а $\gamma = 1, 0, 1, 0, 0, 0$;

в) Γ є регістром зсуву довжини 3 з нелінійною функцією зворотного зв'язку $\phi(z_0, z_1, z_2) = z_0 \oplus z_1 z_2$ та функцією виходів $f(z_0, z_1, z_2) = z_0$ (див. рис. 3.11, справа), а $\gamma = 1, 0, 1$;

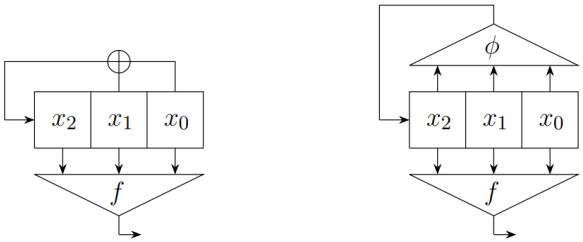

Рис. 3.11. Схеми генераторів гами до пунктів а), в) задачі 6

7. Розглянемо генератор гами з нерівномірним рухом, що складається з двох ЛРЗ з поліномами зворотного зв'язку $p_1(x) = x^3 \oplus x \oplus 1$ та $p_2(x) = x^3 \oplus x^2 \oplus 1$ відповідно (рис. 3.12). В першому регістрі виділеною є комірка з номером 0, а в другому – комірка з номером 1. Зсув регістрів відбувається за таким правилом: якщо значення бітів у виділених комірках збігаються, то обидва регістри зсуваються, інакше зсувається лише перший регістр. Відомо, що вихідною послідовністю генератора є $\gamma = 1, 1, 1, 1, 1$.

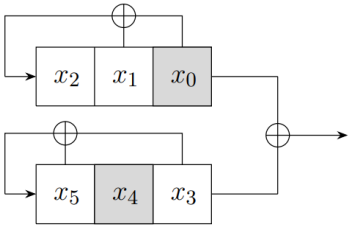

Рис. 3.12. Схема генератора гами до задачі 7

Побудуйте та розв'яжіть систему рівнянь гамоутворення цього генератора гами.

8. Нехай $x_0, x_1, \ldots$ – послідовність, що виробляється лінійним регістром зсуву з початковим станом s_0 та поліномом зворотного зв'язку $f(z)$ над полем з q елементів. Знайдіть знак x_m цієї послідовності, якщо

а) $q = 2$, $f(z) = z^3 + z + 1$, $s_0 = (0, 1, 1)$, $m = 1000$;

б) $q = 3$, $f(z) = z^3 + 2z + 1$, $s_0 = (2, 1, 0)$, $m = 1000$;

в) $q = 5$, $f(z) = z^3 + z + 1$, $s_0 = (1, 3, 4)$, $m = 100$;

в) $q = 7$, $f(z) = z^3 + 2z + 1$, $s_0 = (1, 6, 2)$, $m = 100$.

9. Побудуйте схему фільтрувального генератора гами над полем з двох елементів, якщо поліном зворотного зв'язку ЛРЗ та функція ускладнення генератора мають відповідно такий вигляд:

а) $f(z) = z^{10} \oplus z^4 \oplus 1$, $F(x_0,...,x_9) = x_1x_2 \oplus x_6 \oplus x_3$;

б) $f(z) = z^{11} \oplus z^2 \oplus 1$, $F(x_0,...,x_{10}) = x_3x_4 \oplus x_{10} \oplus x_5$;

в) $f(z) = z^{15} \oplus z^5 \oplus 1$, $F(x_0,...,x_{14}) = x_1x_2x_3 \oplus x_6x_{12} \oplus x_8$.

10. Доведіть, що внутрішня та вихідна послідовності генератора гами з множиною станів S є періодичними та мають періоди не вище за $|S|$.

11. Доведіть, що внутрішня послідовність генератора гами з бієктивною функцією переходів є чисто періодичною.

12. Доведіть, що поліном зворотного зв'язку довільного лінійного регістру зсуву довжини n можна відновити за $2n$ послідовними знаками його вихідної послідовності шляхом розв'язання системи з n лінійних рівнянь від n невідомих.

13. Доведіть, що ненульова вихідна послідовність двійкового фільтрувального генератора гами, побудованого на базі лінійного регістру зсуву довжини n з примітивними поліномом зворотного зв'язку та зрівноваженою функцією ускладнення має період не менше ніж $2^n - 1$.

14. Для SNOW 2.0-подібного шифру на рис. 3.10 складіть систему рівнянь, що пов'язує значення (3.9) при $l = 0, 1, 2$ з координатами вектора θ_0.

15. Для SNOW 2.0-подібного шифру на рис. 3.10 складіть систему рівнянь, яка пов'язує початковий стан s_0 генератора гами зі знаками $\gamma_0, \gamma_1, \gamma_2$ його вихідної послідовності.

4. МЕТОДИ КРИПТОАНАЛІЗУ ПОТОКОВИХ ШИФРІВ

§ 4.1. Атака Беббіджа-Голіча

Розглянемо атаку на довільний генератор гами, яка базується на методі балансування (time-memory-data trade off), запропоновану незалежно С. Беббіджем [24] та Й. Голічем [25] в середині 90-х років минулого століття.

Атака є важливою для обґрунтування загального співвідношення між довжинами ключа та початкового стану генератора гами потокового шифру. При її проведенні вважається, що криптоаналітику відома деяка кількість D вихідних послідовностей генератора, які отримані при різних (невідомих) початкових станах.

Отже, нехай Γ – генератор гами з множиною станів V_n та вихідним алфавітом $\{0,1\}$. Позначимо f відображення, яке ставить у відповідність початковому стану генератора набір, що складається з перших n знаків його вихідної послідовності.

Атака складається з двох етапів, на першому з яких (етапі передобчислень) криптоаналітик генерує деяку кількість M попарно різних початкових станів $s_1,\ldots,s_M$, за якими обчислює набори $f(s_1),\ldots,f(s_M)$ знаків гами. Далі він формує таблицю, яка складається зі слів $f(s_i)$, де $i\in\overline{1,M}$, впорядкованих за другою компонентою. Інакше кажучи, слова в таблиці записуються в порядку неспадання значень $f(s_i)$ відносно лексикографічного впорядкування на множині V_n.

На другому етапі (пошуку) криптоаналітик має доступ до D різних наборів гами $\gamma_1,\ldots,\gamma_D$, вироблених генератором при різних невідомих початкових станах, причому довжина кожного набору є не менше ніж n бітів.

Не обмежуючи загальності міркувань, припустимо, що $\gamma_1,\ldots,\gamma_D \in V_n$. Тоді криптоаналітик відшукує (наприклад, за допомогою алгоритму бінарного пошуку) значення $i \in \overline{1,M}$ таке, що $f(s_i)=\gamma_j$ для деякого $j \in \overline{1,D}$, та знаходить стан s_i генератора, якому відповідає набор γ_j.

Атака завершується успішно, якщо вдається знайти хоча б одну пару ($i \in \overline{1,M}$, $j \in \overline{1,D}$) таку, що $f(s_i)=\gamma_j$ (і припиняється при першому знаходженні такої пари).

Розглянемо параметри, що характеризують ефективність описаної атаки. Введемо такі позначення:

– T – трудомісткість другого етапу атаки;

– D – обсяг доступних даних (слів довжини n);

– M – обсяг пам'яті, що використовується (обсяг пам'яті в бітах дорівнює $2nM$);

– P – час передобчислень (кількість операцій, які виконуються на першому етапі атаки; зрозуміло, що $P=O(M)$);

– $N=2^n$ – кількість різних початкових станів генератора.

Якщо знехтувати часом пошуку в таблиці на другому етапі атаки, тобто взяти в якості елементарної операції однократну перевірку умови: γ_j мститься серед слів $f(s_i)$, $i \in \overline{1,M}$, то отримаємо, що $T=D$. Зауважимо також, що при бінарному пошуку перевірка цієї умови потребує $O(\log M)$ операцій порівняння двійкових слів довжини n. Більше того,

криптоаналітик може на свій розсуд обмежити час пошуку, переглядаючи не всі D, а меншу кількість доступних йому наборів гами.

Таким чином, мають місце такі співвідношення:

$$1 \le T \le D,\ P = O(M). \tag{4.1}$$

З'ясуємо, як вибрати значення M для заданих чисел $N = 2^n$ та $D < N$. Для цього, перш за все, оцінимо ймовірність успіху атаки.

Припустимо, що послідовності $f(s_1),\ldots,f(s_M)$ та $\gamma_1,\ldots,\gamma_D$ формуються випадково й незалежно одна від одної за урновою схемою без повернення кожна. Інакше кажучи, вважатимемо, що для будь-яких $a_1,\ldots,a_M \in V_n$, $b_1,\ldots,b_D \in V_n$ виконується рівність

$$\Pr(f(s_1),\ldots,f(s_M) = a_1,\ldots,a_M, \gamma_1,\ldots,\gamma_D = b_1,\ldots,b_D) = \frac{1}{(N)_M (N)_D},$$

де $(N)_m = N(N-1)\ldots(N-m+1)$ – число розміщень з N по m, $0 \le m \le N$.

Атака завершується успішно, якщо послідовності $f(s_1),\ldots,f(s_M)$ та $\gamma_1,\ldots,\gamma_D$ мають хоча б один спільний член. Ймовірність цієї події дорівнює

$$\pi_n(M,D) = 1 - \frac{(N)_M \cdot (N-M)_D}{(N)_M \cdot (N)_D} =$$

$$= 1 - \left(1 - \frac{M}{N}\right)\left(1 - \frac{M}{N-1}\right)\ldots\left(1 - \frac{M}{N-D-1}\right) >$$

$$>1-\left(1-\frac{M}{N}\right)^{D} \geq 1-e^{-\frac{MD}{N}}, \qquad (4.2)$$

де останнє співвідношення випливає з відомої нерівності

$$1-x \leq e^{-x},\ x \in (0,1).$$

Отже, на підставі (4.2) за умови

$$M = C \cdot \frac{N}{D}, \quad C = \text{const} \geq 1, \qquad (4.3)$$

ймовірність успішного завершення атаки становить

$$\pi_n(M,D) \geq 1-e^{-C} \qquad (4.4)$$

і може бути зроблена як завгодно близькою до 1 шляхом вибору достатньо великого значення C.

Таким чином, на підставі формул (4.1), (4.3) мають місце такі співвідношення, що пов'язують основні характеристики ефективності описаної атаки:

$$M \cdot D \geq N, \quad 1 \leq T \leq D, \quad P = O(M).$$

Зокрема, вважаючи $D = N^{1/2}$, $M = C \cdot N^{1/2}$, де $C \geq 1$, отримаємо, що трудомісткість атаки складає $T = O(N^{1/2})$. При цьому ймовірність її успіху оцінюється знизу за формулою (4.4), обсяг необхідної пам'яті дорівнює

$M = O(N^{1/2})$ (двійкових слів довжини $2n$), а час передобчислень – $P = O(N^{1/2})$. Зауважимо також, що трудомісткість тотального методу (перебору усіх початкових станів генератора гами) має порядок $O(N)$.

З аналізу наведеної атаки можна зробити такий важливий висновок: *для того, щоб синхронний потоковий шифр забезпечував стійкість на рівні* 2^l *необхідно, щоб довжина початкового стану генератора гами цього шифру була не менш ніж* $2l$ *бітів.*

Зокрема, довжина початкового стану потокового шифру має бути принаймні вдвічі більше за довжину його ключа.

§ 4.2. Атака Куртуа-Майєра та алгебраїчна імунність булевих функцій

У 2003 р. Н. Куртуа та В. Майєр [26] запропонували алгебраїчну атаку на фільтрувальні генератори (зокрема, LILI-128 і Toyocrypt), яку згодом було узагальнено та застосовано до інших генераторів гами.

Для викладення атаки введемо декілька допоміжних понять.

Позначимо B_n множину всіх булевих функцій від n змінних. Помітимо, що ця множина утворює *комутативне кільце* відносно природних операцій додавання та множення функцій:

$$(f_1 \oplus f_2)(x) = f_1(x) \oplus f_2(x), \quad (f_1 f_2)(x) = f_1(x) f_2(x)$$

для будь-яких $x \in V_n$, $f_1, f_2 \in B_n$. Нагадаємо, що множина $I \subseteq B_n$ називається *ідеалом*, якщо для будь-яких функцій $f_1, f_2 \in I$, $g \in B_n$ виконують-

ся співвідношення $f_1 \oplus f_2 \in I$, $f_1 g \in I$. *Ідеал, породжений функцією* $f \in B_n$, визначається за формулою $< f > = \{gf : g \in B_n\}$.

4.1. ОЗНАЧЕННЯ. *Анулятором* функції $f \in B_n$ називається множина $\mathrm{Ann}(f) = \{g \in B_n : gf = 0\}$.

Безпосередньо з означення 4.1 випливає такий результат.

4.2. ТВЕРДЖЕННЯ. Множина $\mathrm{Ann}(f)$ є ідеалом кільця B_n, породженим функцією $f \oplus 1$.►

4.3. ОЗНАЧЕННЯ. *Мінімальним степенем* $\min \deg I$ ненульового ідеалу I кільця B_n називається мінімум степенів ненульових функцій, які йому належать.

Розглянемо зараз генератор, функціонування якого описується системою рівнянь

$$f(xL_i) = \gamma_i, i = 0, 1, \ldots, \tag{4.5}$$

де $x = (x_1, \ldots, x_n) \in V_n$ – невідомий початковий стан генератора, f – відома булева функція від n змінних, L_i – відома матриця розміру $n \times n$ над полем з двох елементів, $i = 0, 1, \ldots$ (Як приклади генераторів, що описуються системами рівнянь вигляду (4.5), відзначимо фільтрувальний та комбінувальний генератори гами).

Припустимо, що виконується хоча б одна з двох умов:

1) існує ненульова функція $g \in \mathrm{Ann}(f)$ така, що $\deg g < \deg f$;

2) існує ненульова функція $h \in \mathrm{Ann}(f \oplus 1)$ така, що $\deg h < \deg f$.

Тоді у випадку $\gamma_i = 1$ за умови 1) маємо

$$0 = g(xL_i) f(xL_i) = g(xL_i),$$

а у випадку $\gamma_i = 0$ за умови 2) маємо

$$0 = h(xL_i)(f(xL_i) \oplus 1) = h(xL_i).$$

Таким чином, за системою рівнянь (4.5) побудуємо нову систему, що складається з рівнянь меншого степеня, розв'язуючи яку, відновимо початковий стан генератора гами.

Оцінимо часову складність цієї атаки, вважаючи, що для розв'язання отриманої системи рівнянь використовується *метод введення нових змінних*.

Нагадаємо, що при застосуванні цього методу треба представити кожну функцію в лівій частині системи рівнянь поліномом Жегалкіна та замінити кожен моном x^{α} у виразі цього полінома на нову змінну y_{α}, $\alpha \in V_n \setminus \{0\}$. Отриману таким чином систему лінійних рівнянь (відносно нових змінних) можна розв'язати за допомогою відомих методів (наприклад, методу Гаусса) та відновити значення змінних $x_i = y_i$, $i \in \overline{1,n}$.

Нехай $\min\{\deg g, \deg h\} = d$. Тоді в результаті описаної заміни змінних отримаємо систему лінійних рівнянь від

$$N_d = \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{d}$$

невідомих. Складність розв'язання цієї системи методом Гаусса становить $O(tN_d^2)$ двійкових операцій, де $t \geq N_d$ позначає кількість рівнянь у систе-

мі. Таким чином, виграш у часовій складності атаки Куртуа-Майєра в порівнянні з тривіальною атакою, що полягає у розв'язанні вхідної системи (4.5) методом введення нових змінних, є величиною порядку $\left(N_D / N_d\right)^3$, де $D = \deg f$.

Описана атака являє собою підставу для введення такого важливого поняття.

4.4. ОЗНАЧЕННЯ. Число

$$\mathrm{AI}(f) = \min\{\min \deg \mathrm{Ann}(f), \min \deg \mathrm{Ann}(f \oplus 1)\}$$

називається *алгебраїчною імунністю булевої функції* f.

4.5. ПРИКЛАД. У потоковому шифрі Toyocrypt використовується фільтрувальний генератор гами з функцією ускладнення $f \in B_{128}$, де $\deg f = 63$. При цьому $\mathrm{AI}(f) = 3$, що надає змогу зламати цей шифр за допомогою атаки Куртуа-Майєра.

У шифрі LILI-128 використовується схема з нерівномірним рухом, у якій один фільтрувальний генератор гами керує рухом іншого. Функція ускладнення другого генератора залежить від 10 змінних та має степінь 6. При цьому її алгебраїчна імунність дорівнює 4, що приводить до алгебраїчної атаки на шифр, помітно ефективнішої за тривіальну.

Доведемо твердження, яке надає змогу оцінювати (а в деяких випадках – обчислювати точно) мінімальний степінь ідеалу, породженого булевою функцією. Попередньо введемо декілька позначень.

Для будь-якого натурального d позначимо

$$m(n,d) = \sum_{i=0}^{d} \binom{n}{i}.$$

Для заданої (відмінної від константи 1) функції $f \in B_n$ розглянемо матрицю $M_{f,d}$, рядки якої занумеровані векторами $x \in V_n$ такими, що $f(x) = 1$ (їхня кількість дорівнює вазі $\| f \|$ функції f), а стовпці – мономами степенів $0, 1, \ldots, d$ (їхня кількість дорівнює $m(n,d)$); на перетині рядка та стовпця запишемо значення монома у точці x.

4.6. ЛЕМА. Справедливе таке співвідношення:

$$\text{mindeg } \text{Ann}(f) \geq d+1 \Leftrightarrow \text{rank}(M_{f,d}) = m(n,d).$$

◄ Згідно з означенням матриці $M_{f,d}$ ненульова функція $g(x) = \bigoplus\limits_{\substack{\alpha \in V_n: \\ wt(\alpha) \leq d}} c_\alpha x^\alpha$ належить ідеалу $\text{Ann}(f)$ тоді й тільки тоді, коли вектор $(c_\alpha : \alpha \in V_n, wt(\alpha) \leq d)$ є ненульовим розв'язком системи лінійних рівнянь $M_{f,d} z^{\downarrow} = 0^{\downarrow}$. Отже,

$$\text{mindeg } \text{Ann}(f) \geq d+1 \Leftrightarrow (\forall g \in \text{Ann}(f) \setminus \{0\} : \deg g \geq d+1) \Leftrightarrow$$

$$\Leftrightarrow (\text{система рівнянь } M_{f,d} z^{\downarrow} = 0^{\downarrow} \text{ не має ненульових розв'язків}) \Leftrightarrow$$

$$\Leftrightarrow \text{rank}(M_{f,d}) = m(n,d). \blacktriangleright$$

4.7. ТВЕРДЖЕННЯ. Нехай d є найбільшим натуральним числом, що задовольняє нерівність $m(n,d) \le \| f \|$. Тоді $\text{mindeg Ann}(f) \le d+1$. При цьому $\text{mindeg Ann}(f) = d+1 \Leftrightarrow \text{rank}(M_{f,d}) = m(n,d)$.

◄ З означення параметра d випливає, що $m(n,d+1) > \| f \|$. Отже, $\text{rank}(M_{f,d+1}) \le \min\{\| f \|, m(n,d+1)\} < m(n,d+1)$ і на підставі леми 4.6 $\text{mindeg Ann}(f) < d+2$. Таким чином, $\text{mindeg Ann}(f) \le d+1$, що й треба було довести. Остання частина твердження випливає безпосередньо з леми 4.6. ►

Отже, згідно з твердженням 4.7 для оцінювання мінімального степеня ідеалу $\text{Ann}(f)$ достатньо:

1) знайти найбільше натуральне d, для якого $m(n,d) \le \| f \|$;

2) побудувати матрицю $M_{f,d}$ та обчислити її ранг (наприклад, за допомогою алгоритму Гаусса).

Якщо $\text{rank}(M_{f,d}) = m(n,d)$, то $\text{mindeg Ann}(f) = d+1$; в іншому випадку $\text{mindeg Ann}(f) \le d$.

4.8. ПРИКЛАД. Нехай $f(x_1, x_2, x_3) = x_1x_2 \oplus x_1 \oplus x_2 \oplus x_3 \oplus 1$. Тоді $\| f \| = 4$ і найбільше натуральне d таке, що $m(3,d) \le \| f \|$, дорівнює 1. Побудуємо матрицю $M_{f,1}$:

$$M_{f,1} = \begin{pmatrix} 1|_{(0,0,0)} & x_1|_{(0,0,0)} & x_2|_{(0,0,0)} & x_3|_{(0,0,0)} \\ 1|_{(0,1,1)} & x_1|_{(0,1,1)} & x_2|_{(0,1,1)} & x_3|_{(0,1,1)} \\ 1|_{(1,0,1)} & x_1|_{(1,0,1)} & x_2|_{(1,0,1)} & x_3|_{(1,0,1)} \\ 1|_{(1,1,1)} & x_1|_{(1,1,1)} & x_2|_{(1,1,1)} & x_3|_{(1,1,1)} \end{pmatrix} = \begin{pmatrix} 1000 \\ 1011 \\ 1101 \\ 1111 \end{pmatrix}.$$

Використовуючи алгоритм Гаусса, знайдемо $\operatorname{rank}(M_{f,d}) = 4$. Отже, $\operatorname{mindeg} \operatorname{Ann}(f) = 2$.

На завершення отримаємо верхню оцінку алгебраїчної імунності.

4.9. ТВЕРДЖЕННЯ. Для будь-якої функції $f \in B_n$ виконується нерівність

$$\operatorname{AI}(f) \le \left\lceil \frac{n}{2} \right\rceil.$$

◄ З функцій f та $f \oplus 1$ виберемо ту, вага якої не перевищує 2^{n-1}. Не обмежуючи загальності, вважатимемо, що це є функція f.

Позначимо $d = \left\lceil \frac{n}{2} \right\rceil$ та розглянемо матрицю $M = M_{f,d}$, яка має $\| f \|$ рядків та $m(n,d) = \sum_{i=0}^{\left\lceil \frac{n}{2} \right\rceil} \binom{n}{i} > 2^{n-1} \ge \| f \|$ стовпців. Оскільки стовпців більше ніж рядків, то система лінійних рівнянь $Mz^{\downarrow} = 0^{\downarrow}$ має ненульовий розв'язок, який визначає вектор коефіцієнтів полінома Жегалкіна функції $g \in B_n$ степеня $\deg g \le \left\lceil \frac{n}{2} \right\rceil$. Ця функція обертається в нуль на усіх векторах $x \in V_n$ таких, що $f(x) = 1$, тобто задовольняє умову $g \in \operatorname{Ann}(f)$. ►

§ 4.3. Кореляційна атака Зігенталера

Атака Зігенталера [27] є історично першою кореляційною атакою, опублікованою у відкритих джерелах. Вона спрямована на відновлення

початкового стану комбінувального генератора гами за його вихідною послідовністю і базується на припущенні, що комбінувальну функцію генератора можна наблизити функцією від меншої кількості змінних.

Розглянемо комбінувальний генератор гами, який складається з n лінійних регістрів зсуву довжини $L_1, \ldots, L_n$ відповідно (рис. 4.1).

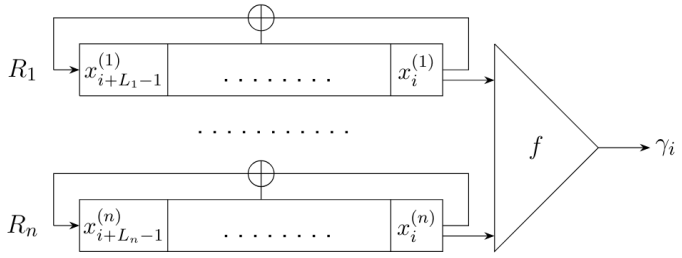

Рис. 4.1. Комбінувальний генератор гами

Вважається, що поліноми зворотного зв'язку лінійних регістрів є примітивними, а комбінувальна функція $f : V_n \to \{0, 1\}$ – зрівноваженою. Знак гами, що виробляється в i-му такті, обчислюється за формулою

$$\gamma_i = f(x_i^{(1)}, \ldots, x_i^{(n)}), \tag{4.6}$$

де $x_i^{(j)}$ – i-й знак лінійної рекуренти, яка виробляється j-м регістром, $i = 0, 1, \ldots$, $j \in \overline{1, n}$.

Як зазначено вище, атака Зігенталера спрямована на те, щоб відновити початковий стан генератора гами за послідовністю (4.6). При цьому вважається, що кількість знаків послідовності, доступних для аналізу, є потенційно необмеженою.

Основне припущення, необхідне для проведення атаки, полягає в тому, що існує булева функція g від $k < n$ змінних та числа $1 \le i_1 < \ldots < i_k \le n$ такі, що

$$\Pr(f(X_1,\ldots,X_n) \neq g(X_{i_1},\ldots,X_{i_k})) = p \le 1/2 \cdot (1-\varepsilon), \qquad (4.7)$$

де $\varepsilon > 0$, а $(X_1,\ldots,X_n)$ – випадковий рівноймовірний двійковий вектор довжини n.

Надалі, не обмежуючи загальності, вважатимемо, що $(i_1,\ldots,i_k) = (1,\ldots,k)$. За вхідним генератором гами побудуємо новий, який складається з перших k регістрів вхідного генератора та комбінувальної функції g (рис. 4.2). Назвемо новий генератор гами *статистичним аналогом* вхідного.

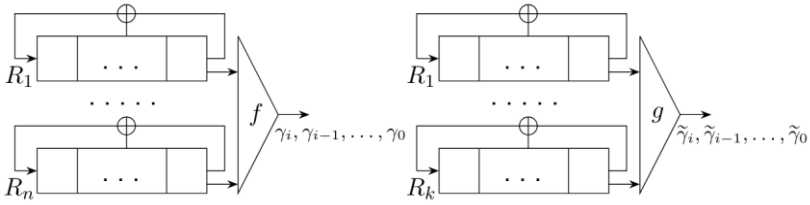

Рис. 4.2. Вхідний генератор гами та його статистичний аналог

Основна ідея атаки полягає в тому, щоб розв’язувати задачу відновлення початкового стану нового, простіше збудованого генератора гами, вважаючи, що послідовність $\gamma_0, \gamma_1, \ldots$ вигляду (4.6) отримується в резуль-

тації спотворення вихідної послідовності $\tilde{\gamma}_0, \tilde{\gamma}_1, \ldots$ нового генератора гами так, що (згідно з формулою (4.7))

$$\Pr(\tilde{\gamma}_i \neq \gamma_i) = p \leq 1/2 \cdot (1-\varepsilon),\ i = 0, 1, \ldots$$

Іншими словами, замість вхідної (умовно складної) задачі пропонується розв'язувати нову (більш просту) задачу, але для неточно визначених, спотворених вхідних даних. Зазначена ідея є дуже поширеною в криптоаналізі.

Опишемо алгоритм відновлення початкового стану генератора гами, який по суті реалізує метод максимуму правдоподібності.

1. Переберемо усі початкові стани $x^{(1)}, \ldots, x^{(k)}$ лінійних регістрів зсуву з номерами $1, \ldots, k$ відповідно, обчислюючи значення

$$\xi(x^{(1)}, \ldots, x^{(k)}) = \sum_{i=0}^{T-1} (g(x_i^{(1)}, \ldots, x_i^{(k)}) \oplus \gamma_i), \qquad (4.8)$$

де T – довжина фрагменту гами, доступного для аналізу, $x_i^{(j)}$ – i-й знак рекуренти, що виробляється j-м регістром при початковому стані $x^{(j)}$, $i \in \overline{0, T-1},\ j \in \overline{1, k}$.

2. Вважатимемо істинним набір $(\hat{x}^{(1)}, \ldots, \hat{x}^{(k)})$ початкових станів, який задовольняє умову

$$\xi(\hat{x}^{(1)}, \ldots, \hat{x}^{(k)}) = \min_{x^{(1)}, \ldots, x^{(k)}} \xi(x^{(1)}, \ldots, x^{(k)}).$$

3. Знаючи початкові стани регістрів з номерами $1,\ldots,k$, відновимо початкові стани решти лінійних регістрів зсуву шляхом повного перебору.

Зауважимо, що сума в правій частині формули (4.8) дорівнює кількості позицій, в яких вихідна послідовність нового генератора гами відрізняється від наявної гами, виробленої вхідним генератором. Тому (згідно з методом максимуму правдоподібності) істинним вважається набір початкових станів регістрів зсуву, на якому досягається мінімум цієї кількості.

Зрозуміло, що часова складність наведеної атаки становить

$$O(T \cdot 2^{L1+\ldots+Lk} + (L_1 + \ldots + L_n) \cdot 2^{Lk+1+\ldots+Ln}), \qquad (4.9)$$

операцій, в той час, як складність повного перебору дорівнює $O((L_1 + \ldots + L_n) \cdot 2^{L_1+\ldots+L_n})$ (за умови, що відстань єдиності вхідного генератора гами є величиною порядку $L_1 + \ldots + L_n$).

Отримаємо оцінку обсягу матеріалу T, для якого наведена атака надає можливість відновлювати початковий стан генератора із заданою достовірністю. З цією метою зробимо такі ймовірнісні припущення.

По-перше, позначимо $(\breve{x}^{(1)},\ldots,\breve{x}^{(n)})$ істинний набір початкових станів усіх лінійних регістрів зсуву генератора та вважатимемо, що знаки $\breve{x}_i^{(j)}$ лінійних рекурент, які виробляються за цими початковими станами, є незалежними випадковими величинами, розподіленими за законом

$$\Pr(\breve{x}_i^{(j)} = 0) = \Pr(\breve{x}_i^{(j)} = 1) = 1/2, \ i \in \overline{0, T-1}, \ j \in \overline{1, n}.$$

По-друге, вважатимемо, що для будь-якого хибного набору $(\tilde{x}^{(1)},\ldots,\tilde{x}^{(k)}) \neq (\breve{x}^{(1)},\ldots,\breve{x}^{(k)})$ початкових станів перших k регістрів знаки $\tilde{x}_i^{(j)}$, $i \in \overline{0,T-1}$, $j \in \overline{1,k}$, є незалежними випадковими величинами з рівномірним розподілом на множині $\{0,1\}$, які не залежать від знаків $\breve{x}_i^{(j)}$ для усіх $i \in \overline{0,T-1}$, $j \in \overline{1,n}$.

З першого припущення та формул (4.6), (4.7) випливає, що при $(x^{(1)},\ldots,x^{(k)}) = (\breve{x}^{(1)},\ldots,\breve{x}^{(k)})$ значення $\xi(x^{(1)},\ldots,x^{(k)})$ вигляду (4.8) збігається з кількістю успіхів у схемі Бернуллі з числом випробувань T та ймовірністю успіху $p \le 1/2 \cdot (1-\varepsilon)$. Якщо ж $(x^{(1)},\ldots,x^{(k)}) \neq (\breve{x}^{(1)},\ldots,\breve{x}^{(k)})$, то на підставі другого припущення $\xi(x^{(1)},\ldots,x^{(k)})$ є кількістю успіхів у схемі Бернуллі з таким самим числом випробувань та ймовірністю успіху $1/2$.

Для доведення наступного результату скористаємося такої лемою.

4.10. ЛЕМА (*оцінки ймовірностей великих відхилень у схемі Бернуллі*). Нехай ξ – кількість успіхів у схемі Бернуллі з числом випробувань T та ймовірністю успіху p. Тоді для будь-якого $\theta > 0$ виконуються нерівності

$$\Pr\{\xi - Tp \ge T\theta\} \le \exp\{-2T\theta^2\},\ \Pr\{\xi - Tp \le -T\theta\} \le \exp\{-2T\theta^2\}.$$

4.11. ЛЕМА. За умови наведених вище припущень для ймовірності помилкового відновлення початкових станів перших k регістрів зсуву на кроці 2 атаки Зігенталера виконується така нерівність:

$$p_{err} = \Pr\left((\hat{x}^{(1)},\ldots,\hat{x}^{(k)}) \neq (\breve{x}^{(1)},\ldots,\breve{x}^{(k)})\right) \le 2^{L_1+\ldots+L_k} \exp\{-1/8 \cdot T\varepsilon^2\}.$$

◄ З умови $(\hat{x}^{(1)},\ldots,\hat{x}^{(k)}) \neq (\breve{x}^{(1)},\ldots,\breve{x}^{(k)})$ випливає, що існує набір $(x^{(1)},\ldots,x^{(k)})$ такий, що $\xi(x^{(1)},\ldots,x^{(k)}) < \xi(\breve{x}^{(1)},\ldots,\breve{x}^{(k)})$. Отже, для будь-якого $C > 0$ виконуються співвідношення

$$\{(\hat{x}^{(1)},\ldots,\hat{x}^{(k)}) \neq (\breve{x}^{(1)},\ldots,\breve{x}^{(k)})\} \subseteq$$

$$\subseteq \{\xi(\breve{x}^{(1)},\ldots,\breve{x}^{(k)}) \geq C\} \cup \bigcup_{(x^{(1)},\ldots,x^{(k)}) \neq (\breve{x}^{(1)},\ldots,\breve{x}^{(k)})} \{\xi(x^{(1)},\ldots,x^{(k)}) < C\},$$

з яких випливає, що

$$p_{err} \leq \Pr\{\xi(\breve{x}^{(1)},\ldots,\breve{x}^{(k)}) \geq C\} + \sum_{(x^{(1)},\ldots,x^{(k)}) \neq (\breve{x}^{(1)},\ldots,\breve{x}^{(k)})} \Pr\{\xi(x^{(1)},\ldots,x^{(k)}) < C\} \leq$$

$$\leq \Pr\{\xi(\breve{x}^{(1)},\ldots,\breve{x}^{(k)}) \geq C\} +$$

$$+ (2^{L_1+\ldots+L_k} - 1) \max_{(x^{(1)},\ldots,x^{(k)}) \neq (\breve{x}^{(1)},\ldots,\breve{x}^{(k)})} \{\Pr\{\xi(x^{(1)},\ldots,x^{(k)}) < C\}\}. \qquad (4.10)$$

Покладемо

$$C = 1/4 \cdot T(2-\varepsilon).$$

Як зазначено вище, величина $\xi(\breve{x}^{(1)},\ldots,\breve{x}^{(k)})$ збігається з кількістю успіхів у схемі Бернуллі з числом випробувань T та ймовірністю успіху $p \leq 1/2 \cdot (1-\varepsilon)$. Звідси, використовуючи лему 4.10, отримаємо, що

$$\Pr\{\xi(\bar{x}^{(1)},\ldots,\bar{x}^{(k)}) \geq C\} = \Pr\{\xi(\bar{x}^{(1)},\ldots,\bar{x}^{(k)}) - Tp \geq C - Tp\} \leq$$

$$\leq \Pr\{\xi(\bar{x}^{(1)},\ldots,\bar{x}^{(k)}) - Tp \geq C - 1/2 \cdot T(1-\varepsilon)\} =$$

$$= \Pr\{\xi(\bar{x}^{(1)},\ldots,\bar{x}^{(k)}) - Tp \geq 1/4 \cdot T\varepsilon\} \leq \exp\{-1/8 \cdot T\varepsilon^2\}. \qquad (4.11)$$

Далі, для будь-якого $(x^{(1)},\ldots,x^{(k)}) \neq (\bar{x}^{(1)},\ldots,\bar{x}^{(k)})$ величина $\xi(x^{(1)},\ldots,x^{(k)})$ є кількістю успіхів у схемі Бернуллі з числом випробувань T та ймовірністю успіху $1/2$. Отже, на підставі леми 4.10

$$\Pr\{\xi(x^{(1)},\ldots,x^{(k)}) < C\} = \Pr\{\xi(x^{(1)},\ldots,x^{(k)}) - 1/2 \cdot T < C - 1/2 \cdot T\} =$$

$$= \Pr\{\xi(x^{(1)},\ldots,x^{(k)}) - 1/2 \cdot T < -1/4 \cdot T\varepsilon\} \leq \exp\{-1/8 \cdot T\varepsilon^2\}. \qquad (4.12)$$

Підставляючи оцінки (4.11), (4.12) у формулу (4.10), отримаємо потрібну нерівність $p_{err} \leq 2^{L_1+\ldots+L_k} \exp\{-1/8 \cdot T\varepsilon^2\}$. ►

Безпосередньо з леми 4.11 випливає таке твердження.

4.12. ТВЕРДЖЕННЯ. Нехай виконуються зазначені вище припущення, $\delta \in (0,1)$ і

$$T = \left\lceil 8 \cdot \varepsilon^{-2} \ln(2^{L_1+\ldots+L_k} \delta^{-1}) \right\rceil.$$

Тоді атака Зігенталера відновлює початковий стан генератора гами на рис. 4.1 з ймовірністю не менше $1-\delta$ та часовою складністю, що визначається за формулою (4.9).

Таким чином, для забезпечення стійкості комбінувального генератора гами відносно наведеної атаки потрібно вибирати його комбінувальну функцію так, щоб для неї не існувало високоймовірних наближень від достатньо малої кількості змінних. Такі функції отримали назву кореляційно-імунних (див. задачі 6, 7).

Зауважимо також, що в оригінальній роботі Зігенталера [27] розглядається випадок, в якому комбінувальна функція генератора наближується функцією від однієї змінної (тобто $k=1$). При цьому атака будується на основі відомого шифротексту за умови, що відкритий текст являє собою послідовність незалежних випадкових величин з відомим нерівномірним законом розподілу. Аналіз ефективності атаки в цьому випадку проводиться аналогічно тому як це зроблено вище.

§ 4.4. Перетворення Фур'є псевдобулевих функцій

Апарат дискретного перетворення Фур'є займає центральне місце серед аналітичних методів сучасної симетричної криптографії. Достатньо зазначити, що в термінах перетворення Фур'є (або його різновиду – перетворення Уолша-Адамара) визначається низка важливих криптографічних параметрів булевих функцій, а без знання основ аналізу Фур'є неможливо просунутись у вивченні кореляційних атак на потокові шифри.

Нижче викладено основні відомості про перетворення Фур'є псевдобулевих функцій.

Позначимо $\mathbf{R}^{2^n}$ векторний простір усіх функцій, заданих на множині V_n, які приймають значення в полі дійсних чисел. Довільну функцію $f \in \mathbf{R}^{2^n}$ будемо називати *псевдобулевою* і ототожнювати її з вектор-

стовпцем її значень: $f = (f(x) : x \in V_n)^T$ (вважаючи, що аргументи функції перелічені в лексикографічному порядку).

Векторний простір псевдобулевих функцій від n змінних є евклідовим простором відносно *скалярного добутку*

$$\langle f, g \rangle = \sum_{x \in V_n} f(x) g(x),\ f, g \in \mathbf{R}^{2^n},$$

що надає змогу надалі використовувати результати, які стосуються цих просторів та їхніх лінійних перетворень. Зокрема, для будь-якої функції $f \in \mathbf{R}^{2^n}$ можна визначити її *норму*:

$$\| f \|_2 = \sqrt{\langle f, f \rangle}.$$

При цьому для довільних функцій $f, g \in \mathbf{R}^{2^n}$ виконується *нерівність Коші-Буняковського* (або *нерівність Шварца*):

$$\left| \langle f, g \rangle \right| \le \| f \|_2 \| g \|_2 .$$

Ключову роль в означенні перетворення Фур'є псевдобулевих функцій відіграє наступне поняття.

4.13. ОЗНАЧЕННЯ. *Матрицею Адамара* (типу Сільвестра) порядку 2^n називається квадратна матриця

$$H_n = ((-1)^{\alpha\beta})_{\alpha,\beta \in V_n},$$

де $\alpha\beta = \bigoplus_{i=1}^{n} \alpha_i \beta_i$ – булев скалярний добуток двійкових векторів $\alpha = (\alpha_1, \ldots, \alpha_n)$ та $\beta = (\beta_1, \ldots, \beta_n)$.

Наступне твердження містить основну властивість матриць Адамара.

4.14. ТВЕРДЖЕННЯ. Матриця H_n є оборотною, причому

$$H_n^{-1} = 2^{-n} H_n .$$

◄ Достатньо переконатися в тому, що для будь-яких $\alpha, \beta \in V_n$ виконується рівність

$$2^{-n} \sum_{x \in V_n} (-1)^{\alpha x} \cdot (-1)^{\beta x} = \delta_{\alpha,\beta} , \qquad (4.13)$$

де $\delta_{\alpha,\beta}$ – символ Кронекера:

$$\delta_{\alpha,\beta} = \begin{cases} 1, & \text{якщо } \alpha = \beta; \\ 0, & \text{якщо } \alpha \neq \beta. \end{cases}$$

Але це випливає безпосередньо з того, що лінійна булева функція $(\alpha \oplus \beta)x$, $x \in V_n$ є зрівноваженою за умови $\alpha \neq \beta$ та дорівнює 0 у протилежному випадку. ►

Співвідношення (4.13) (за всіма $\alpha, \beta \in V_n$) називаються *співвідношеннями ортогональності* та означають, що *матриця* $2^{-\frac{n}{2}} H_n$ *є ортогональною.* (Нагадаємо, що квадратна матриця U над полем **R** називається ор-

тогональною, якщо обернена до неї матриця збігається з транспонованою: $U^{-1} = U^T$).

За допомогою матриці Адамара H_n визначається перетворення Фур'є псевдобулевих функцій.

4.15. ОЗНАЧЕННЯ. *Перетворенням Фур'є* функції $f \in \mathbf{R}^{2^n}$ називається функція $C_f = H_n f$ (нагадаємо, що функції f та C_f ототожнюються з вектор-стовпцями їхніх значень). При цьому *коефіцієнтом Фур'є* функції f, який відповідає вектору $\alpha \in V_n$, називається число

$$C_f(\alpha) = \sum_{x \in V_n} f(x)(-1)^{\alpha x}. \qquad (4.14)$$

Таким чином, перетворення Фур'є ставить у відповідність кожній функції f нову функцію C_f, значення якої на векторі $\alpha \in V_n$ визначається за формулою (4.14).

Розглянемо основні властивості перетворення Фур'є, які випливають з його означення та ортогональності матриці Адамара.

1. Перетворення Фур'є є лінійним перетворенням векторного простору $\mathbf{R}^{2^n}$.

2. Справедлива *формула обернення для перетворення Фур'є*:

$$f = 2^{-n} H_n C_f,$$

яку можна записати також у координатній формі:

$$f(x) = 2^{-n} \sum_{\alpha \in V_n} C_f(\alpha)(-1)^{\alpha x},\ x \in V_n .$$

Отже, функція f однозначно визначається своїми коефіцієнтами Фур'є.

3. Нагадаємо, що будь-яка ортогональна матриця U порядку 2^n зберігає скалярний добуток векторів, тобто задовольняє умову $\langle Uf, Ug \rangle = \langle f, g \rangle$ для будь-яких $f, g \in \mathbf{R}^{2^n}$. Застосовуючи цей факт до матриці $2^{-\frac{n}{2}} H_n$, отримаємо таку рівність:

$$\langle f, g \rangle = 2^{-n} \langle H_n f, H_n g \rangle$$

або в координатній формі

$$\sum_{x \in V_n} f(x) g(x) = 2^{-n} \sum_{\alpha \in V_n} C_f(\alpha) C_g(\alpha) . \qquad (4.15)$$

Таким чином, скалярний добуток псевдобулевих функцій збігається з точністю до коефіцієнта 2^{-n} зі скалярним добутком їхніх перетворень Фур'є.

4. Вважаючи в формулі (4.15) $f = g$, отримаємо *рівність Парсеваля*:

$$\| f \|_2^2 = \sum_{x \in V_n} f(x)^2 = 2^{-n} \sum_{\alpha \in V_n} C_f(\alpha)^2 .$$

Отже, квадрат норми псевдобулевої функції дорівнює середньому арифметичному значенню квадратів її коефіцієнтів Фур'є.

§ 4.5. Алгоритм швидкого перетворення Адамара

Задача обчислення коефіцієнтів Фур'є псевдобулевої функції є дуже розповсюдженою у криптографічних (та інших) застосуваннях. Тому постає питання про ефективні алгоритми розв'язання цієї задачі.

Нехай $\alpha \in \mathbf{R}^{2^n}$ – довільний вектор-стовпець довжини 2^n, H_n – матриця Адамара порядку 2^n. Тоді для знаходження вектора

$$b = H_n a \tag{4.16}$$

за допомогою звичайного алгоритму множення матриць потрібно виконати порядку 2^{2n} додавань або віднімань дійсних чисел. Окрім того, потрібно виділити порядку 2^{2n} бітів пам'яті для зберігання матриці H_n.

Проте існує більш ефективний алгоритм, який не потребує додаткової пам'яті та надає змогу обчислювати вектор (4.16), використовуючи лише $2^n n$ операцій додавання чи віднімання.

В основі зазначеного алгоритму лежить наступне твердження, яке доводиться шляхом безпосередньої перевірки.

4.16. ТВЕРДЖЕННЯ. Матриці Адамара задовольняють рекурентне співвідношення

$$H_n = \begin{pmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{pmatrix}, \; n = 2, 3, \ldots,$$

де

$$H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Алгоритм швидкого перетворення Адамара являє собою рекурсивну $A(n)$, яка визначається таким чином.

Процедура $A(n)$**.**

Вхід: вектор-стовпець $a = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$ довжини 2^n, де $a_0, a_1 \in \mathbf{R}^{2^{n-1}}$.

Результат: вектор-стовпець $b = H_n a$.

Якщо $n = 1$, обчислити

$$b_0 = a_0 + a_1,\ b_1 = a_0 - a_1,\ b = \begin{pmatrix} b_0 \\ b_1 \end{pmatrix}. \qquad (4.17)$$

Якщо $n \geq 2$, обчислити вектори b_0 та b_1, застосовуючи процедуру $A(n-1)$ до векторів $a_0 + a_1$ та $a_0 - a_1$ відповідно; покласти $b = \begin{pmatrix} b_0 \\ b_1 \end{pmatrix}$.

Коректність алгоритму випливає безпосередньо зі співвідношень

$$H_n a = \begin{pmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} = \begin{pmatrix} H_{n-1}(a_0 + a_1) \\ H_{n-1}(a_0 - a_1) \end{pmatrix}.$$

Позначимо $t(n)$ кількість додавань або віднімань дійсних чисел, що виконуються при обчисленні вектора b вигляду (4.16) за допомогою наведеного алгоритму.

4.17. ТВЕРДЖЕННЯ. Для будь-якого натурального n справедлива рівність

$$t(n) = 2^n n.$$

◄ Отримаємо рекурентне співвідношення для чисел $t(n),\ n=1,2,\ldots$.

З рівностей (4.17) випливає, що

$$t(1)=2\,. \tag{4.18}$$

Далі, при $n\geq 2$ для обчислення вектора b за допомогою процедури $A(n)$ необхідно виконати 2^n операцій додавання (віднімання) для обчислення векторів $a_0+a_1,\ a_0-a_1$ та ще $2t(n-1)$ таких операцій при застосуванні до отриманих векторів процедури $A(n-1)$. Таким чином,

$$t(n)=2^n+2t(n-1),\ \ n=2,3,\ldots\,. \tag{4.19}$$

Покладемо $\tau(n)=2^{-n}t(n),\ n=1,2,\ldots$. На підставі формул (4.18), (4.19) мають місце рівності

$$\tau(1)=1,\ \tau(n)=1+\tau(n-1),\ n=2,3,\ldots\,,$$

з яких випливає, що $\tau(n)=n$ для будь-якого натурального n. Отже,

$$t(n)=2^n\tau(n)=2^n n\,,$$

що й треба було довести. ►

§ 4.6. Перетворення Уолша-Адамара та афінні наближення булевих функцій

Розглянемо окремий випадок перетворення Фур'є, що використовується для аналізу кореляційних властивостей булевих функцій.

4.18. ОЗНАЧЕННЯ. *Перетворенням Уолша-Адамара* функції $f : V_n \to \{0,1\}$ називається перетворення Фур'є псевдобулевої функції $(-1)^f$:

$$\hat{f}(\alpha) = \sum_{x \in V_n} (-1)^{f(x) \oplus \alpha x}, \alpha \in V_n .$$

При цьому число $\hat{f}(\alpha)$ називається *коефіцієнтом Уолша-Адамара* функції f, який відповідає вектору α.

Оскільки перетворення Уолша-Адамара є окремим випадком перетворення Фур'є, то результати, отримані для останнього, виконуються і для перетворення Уолша-Адамара. Зокрема, функція $f : V_n \to \{0,1\}$ однозначно відновлюється за її коефіцієнтами Уолша-Адамара. При цьому справедлива рівність

$$(-1)^{f(x)} = 2^{-n} \sum_{\alpha \in V_n} \hat{f}(\alpha)(-1)^{\alpha x}, x \in V_n .$$

Крім того, для будь-яких функцій $f, g : V_n \to \{0,1\}$ виконується співвідношення

$$2^n \sum_{x \in V_n} (-1)^{f(x) \oplus g(x)} = \sum_{\alpha \in V_n} \hat{f}(\alpha)\hat{g}(\alpha),$$

з якого (при $f = g$) випливає *рівність Парсеваля*:

$$\sum_{\alpha \in V_n} \hat{f}(\alpha)^2 = 2^{2n}. \tag{4.20}$$

Таким чином, сума квадратів коефіцієнтів Уолша-Адамара булевої функції від n змінних дорівнює 2^{2n}.

Зазвичай кореляційні атаки на потокові шифри базуються на можливості наближення нелінійних функцій ускладнення, що використовуються у конструкціях цих шифрів, простіше збудованими, перш за все, афінними функціями.

4.19. ОЗНАЧЕННЯ. Функція $g : V_n \to \{0,1\}$ називається *наближенням* (або *статистичним аналогом*) функції $f : V_n \to \{0,1\}$, якщо виконується нерівність $\Pr(f(X) = g(X)) > 1/2$, де X – випадковий рівноймовірних вектор довжини n.

Як показує наступне твердження, коефіцієнти Уолша-Адамара надають можливість оцінювати якість афінних наближень булевих функцій та знаходити їхні афінні статистичні аналоги.

4.20. ТВЕРДЖЕННЯ. Для будь-яких $f : V_n \to \{0,1\}$, $\alpha \in V_n$, $c \in \{0,1\}$ виконується рівність

$$\Pr(f(X) = \alpha X \oplus c) = 1/2 \cdot (1 + (-1)^c 2^{-n} \hat{f}(\alpha)). \tag{4.21}$$

◄ Достатньо довести формулу (4.21) при $c = 0$. Дійсно, мають місце такі співвідношення:

$$\hat{f}(\alpha) = \sum_{x \in V_n} (-1)^{f(x) \oplus \alpha x} = \left| \{ x \in V_n : f(x) = \alpha x \} \right| - \left| \{ x \in V_n : f(x) \neq \alpha x \} \right| =$$

$$= 2 \cdot \left| \{ x \in V_n : f(x) = \alpha x \} \right| - 2^n = 2^{n+1} \Pr(f(X) = \alpha X) - 2^n ,$$

що й треба було довести. ►

З твердження 4.20 випливає, що функція $l_{\alpha,c}(x) = \alpha x \oplus c,\ x \in V_n$ є статистичним аналогом функції f тоді й тільки тоді, коли $(-1)^c \hat{f}(\alpha) > 0$. Зокрема, за умови $\hat{f}(\alpha) \neq 0$ функція f має статистичним аналогом точно одну з двох функцій $l_{\alpha,0}$ та $l_{\alpha,1}$. При цьому на підставі рівності Парсеваля (див. формулу (4.20)) афінні статистичні аналоги існують для будь-якої булевої функції.

Розглянемо зараз такий важливий криптографічний параметр булевої функції як її нелінійність.

Нагадаємо (див. означення 2.8), що нелінійність функції $f : V_n \to \{0,1\}$ визначається як відстань Ґеммінга від неї до множини афінних функцій: $N_f = \min\{ d(f, l_{\alpha,c}) : \alpha \in V_n, c \in \{0,1\} \}$.

4.21. ТВЕРДЖЕННЯ. Для нелінійності функції $f : V_n \to \{0,1\}$ виконується рівність

$$N_f = 2^{n-1} (1 - 2^{-n} \max_{\alpha \in V_n} | \hat{f}(\alpha) |) .$$

◄ На підставі твердження 4.20

$$d(f, l_{\alpha,c}) = 2^n \Pr(f(X) \neq l_{\alpha,c}(X)) = 2^{n-1}(1-(-1)^c 2^{-n} \hat{f}(\alpha)).$$

Отже,

$$\min_{\substack{\alpha \in V_n, \\ c \in \{0,1\}}} d(f, l_{\alpha,c}) = \min_{\substack{\alpha \in V_n, \\ c \in \{0,1\}}} 2^{n-1}(1-(-1)^c 2^{-n} \hat{f}(\alpha)) =$$

$$= \min_{\alpha \in V_n} 2^{n-1}(1-2^{-n} \mid \hat{f}(\alpha) \mid) = 2^{n-1}(1-2^{-n} \max_{\alpha \in V_n} \mid \hat{f}(\alpha) \mid). \blacktriangleright$$

4.22. ТВЕРДЖЕННЯ. Нелінійність функції $f: V_n \to \{0,1\}$ задовольняє нерівність

$$N_f \leq 2^{n-1} - 2^{\frac{n}{2}-1}, \tag{4.22}$$

яка перетворюється на рівність тоді й тільки тоді, коли $| \hat{f}(\alpha) | = 2^{\frac{n}{2}}$ для кожного $\alpha \in V_n$.

◄ Використовуючи рівність Парсеваля, отримаємо, що

$$2^{2n} = \sum_{\alpha \in V_n} \hat{f}(\alpha)^2 \leq 2^n \max_{\alpha \in V_n} \hat{f}(\alpha)^2. \tag{4.23}$$

Отже, $\max_{\alpha \in V_n} | \hat{f}(\alpha) | \geq 2^{\frac{n}{2}}$. Звідси, на підставі твердження 4.21 випливає нерівність (4.22).

Далі, якщо $|\hat{f}(\alpha)| = 2^{\frac{n}{2}}$ для кожного $\alpha \in V_n$, то зазначена нерівність досягається. Навпаки, якщо $N_f = 2^{n-1} - 2^{\frac{n}{2}-1}$, то внаслідок твердження 4.21 $\max\limits_{\alpha \in V_n} |\hat{f}(\alpha)| = 2^{\frac{n}{2}}$, звідси випливає, що нерівність (4.23) перетворюється на рівність. Отже,

$$|\hat{f}(\alpha)| = \max_{\alpha \in V_n} |\hat{f}(\alpha)| = 2^{\frac{n}{2}}$$

для кожного $\alpha \in V_n$. ►

4.23. ОЗНАЧЕННЯ. Функція $f : V_n \to \{0,1\}$ називається *бент-функцією*, якщо вона має найбільшу можливу нелінійність, тобто задовольняє умову $|\hat{f}(\alpha)| = 2^{\frac{n}{2}}$ для кожного $\alpha \in V_n$.

Зрозуміло, що бент-функції від n змінних існують тільки для парних значень n. Найвідомішим прикладом бент-функції є функція $xy = \bigoplus\limits_{i=1}^{n} x_i y_i$, де $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in V_n$.

§ 4.7. Кореляційна атака на спрощену версію SNOW 2.0-подібного потокового шифру

Розглянемо SNOW 2.0-подібний шифр, схему якого зображено на рис. 3.10. Усі відомі кореляційні атаки на такі шифри спрямовані на від-

новлення початкового стану ЛРЗ на рис. 3.10 за шифрувальною гамою і базуються на тому, що сума знаків гами в будь-яких суміжних тактах є результатом спотворення знаку лінійної рекуренти, знання якої надає змогу одразу ж відновити цей стан.

Для викладення сутності зазначених атак розглянемо спрощену версію шифру, яка відрізняється від оригіналу застосуванням операції $\oplus$ замість операції $+$ у схемі на рис. 3.10. В цьому випадку рівняння, що описують функціонування генератора гами, спрощуються і приймають такий вигляд: $\gamma_i = x_i \oplus x_{i+n-1} \oplus u_i \oplus v_i$, $u_{i+1} = x_{i+\mu} \oplus v_i$, $v_{i+1} = \sigma(u_i)$, $i = 0, 1, \ldots$.

Звідси випливає, що

$$(x_i \oplus x_{i+1} \oplus x_{i+\mu} \oplus x_{i+n-1} \oplus x_{i+n}) \oplus (u_i \oplus \sigma(u_i)) = \gamma_i \oplus \gamma_{i+1}, i = 0, 1, \ldots. \quad (4.24)$$

Вважаючи, що змінні $u_0, u_1, \ldots$ у формулі (4.24) є незалежними випадковими величинами з рівномірним розподілом на множині V_m та виражаючи знаки $x_i, x_{i+1}, x_{i+\mu}, x_{i+n}$ лінійної рекуренти $x_0, x_1, \ldots$ через початковий стан $(x_0, x_1, \ldots, x_{n-1})$ ЛРЗ на рис. 3.10 (наприклад, за допомогою твердження 3.15), отримаємо систему лінійних рівнянь зі спотвореними правими частинами над полем F_{2^m}, де спотворення дорівнюють $\xi_i = u_i \oplus \sigma(u_i)$, $i = 0, 1, \ldots$. Метою кореляційної атаки, що розглядається, є відновлення вектора $(x_0, x_1, \ldots, x_{n-1})$ за відомою гамою $\gamma_0, \gamma_1, \ldots$ шляхом розв'язання отриманої системи рівнянь.

Для цього зафіксуємо довільний базис поля F_{2^m} над полем F_2 та замінимо отриману систему на рівносильну систему спотворених лінійних рівнянь над полем F_2, використовуючи представлення коефіцієнтів та не-

відомих вхідної системи в цьому базисі. А саме, помітимо, що добуток ax_i елементів a та x_i поля F_{2^m} є лінійним перетворенням набору $\hat{x}_i$ координат елемента x_i у вибраному базисі. Отже, набір координат цього добутку можна представити у вигляді $\hat{x}_i A$, де A – певна $m \times m$-матрицю над полем F_2, яка залежить від елемента a (див. задачу 19). Таким чином, кожне рівняння вхідної системи вигляду $a_0 x_0 \oplus \ldots \oplus a_{n-1} x_{n-1} \oplus \xi = b$ можна замінити рівносильним "векторним" рівнянням

$$\hat{x}_0 A_0 \oplus \ldots \oplus \hat{x}_{n-1} A_{n-1} \oplus \hat{\xi} = \hat{b} \tag{4.25}$$

над полем F_2. Нарешті, для отримання кінцевої системи булевих рівнянь виберемо ненульовий вектор-стовпець $\alpha \in V_m$ та помножимо його справа на кожне рівняння вигляду (4.25).

Кінцеву систему рівнянь можна записати у вигляді

$$a_i x \oplus \eta_i = (\gamma_i \oplus \gamma_{i+1})\alpha\,,\ i = 0, 1, \ldots. \tag{4.26}$$

де a_i – відомі двійкові вектори довжини mn, x – двійковий вектор-стовпець такої ж довжини, що складається з наборів координат невідомих $x_0, x_1, \ldots, x_{n-1}$, $\eta_i = \xi_i \alpha$ – випадкові величини, розподілені за законом

$$\Pr(\eta_i = 0) = 1 - \Pr(\eta_i = 1) = \Pr(u_i \alpha = \sigma(u_i)\alpha)\,,\ i = 0, 1, \ldots. \tag{4.27}$$

Складність розв'язання системи рівнянь (4.26) (будь-яким відомим методом) залежить від параметра $\lambda_\alpha = (2\Pr(X\alpha = \sigma(X)\alpha) - 1)^2$, який хара-

ктеризує близькість розподілу (4.27) до рівномірного розподілу ймовірностей на множині $\{0,1\}$. (При цьому, здебільшого, складність стрімко зростає зі зменшенням значення λ_α).

Розглянемо функцію $f(x) = \sigma(x)\alpha$, $x \in V_m$. Застосовуючи до неї формулу (4.21), отримаємо, що $\lambda_\alpha = 2^{-m} | \hat{f}(\alpha)|^2$, де $\hat{f}(\alpha)$ – коефіцієнт Уолша-Адамара функції f. Звідси на підставі твердження 4.21 та означення 2.15 випливає, що

$$\lambda_\alpha \le 2^{-m} \max_{\beta \in V_n} | \hat{f}(\beta)|^2 = 1 - 2^{-(m-1)} N_f \le 1 - 2^{-(m-1)} N_\sigma$$

де N_f та N_σ позначають нелінійність функції f та підстановки σ відповідно.

Таким чином, складність розглянутої кореляційної атаки залежить від нелінійності цієї підстановки: *чим більше значення N_σ, тим менше значення λ_α, тобто сильніше спотворення у рівняннях системи (4.26), а, отже, тим більше часу потрібно для її розв'язання.*

Отриманий результат показує, що для забезпечення належної стійкості спрощеної версії SNOW 2.0-подібного шифру відносно розглянутої кореляційної атаки слід вибирати таку підстановку σ, яка має достатньо високу нелінійність.

Подальші відомості з аналізу стійкості SNOW 2.0-подібних шифрів відносно кореляційних атак можна знайти в [21, 22, 28].

Завдання для самоконтролю

1. Поясніть, чому в алгоритмах SNOW 2.0 та "Струмок" використовуються лінійні регістри зсуву, довжини яких удвічі більше за довжини ключів шифрування.

2. Оцініть часову складність атаки Куртуа-Майєра на фільтрувальний генератор гами, побудований на основі ЛРЗ довжини n з функцією ускладнення f, якщо

а) $f(x_1, x_2, x_3) = x_1 \oplus x_2 x_3$;

б) $f(x_1, x_2, x_3) = x_2 \oplus x_1 x_2 \oplus x_1 x_3$;

в) $f(x_1, x_2, x_3, x_4) = x_1 \oplus x_1 x_2 x_3 \oplus x_2 x_3 x_4$;

г) $f(x_1, x_2, x_3, x_4) = x_1 \oplus x_2 \oplus x_3 \oplus x_1 x_4 \oplus x_1 x_2 x_3$.

3. Нехай $f \in B_n$, $\mathrm{AI}(f) = d$ та g – афінна булева функція від n змінних. Доведіть, що $d - 1 \le \mathrm{AI}(f \oplus g) \le d + 1$.

4. Нехай $f, g \in B_n$. Доведіть, що $\mathrm{AI}(f \oplus g) \le \mathrm{AI}(f) + \mathrm{AI}(g)$.

5. Нехай n – непарне число та $\mathrm{AI}(f) = \left\lceil \frac{n}{2} \right\rceil$. Доведіть, що f є зрівноваженою функцією.

6. Нехай $(X_1, \ldots, X_n)$ – випадковий рівноймовірний двійковий вектор, f – булева функція від n змінних, $k \in \overline{1, n-1}$. Функція f називається *кореляційно-імунною порядку* k, якщо для будь-якого набору $1 \le i_1 < \ldots < i_k \le n$ випадкові величини $f(X_1, \ldots, X_n)$ та $(X_{i_1}, \ldots, X_{i_k})$ є незалежними. Переконайтесь, що атака Зігенталера, яка базується на співвідношенні (4.7), є незастосовною до генератора гами з кореляційно-імунною порядку k комбінувальною функцією.

7. Доведіть, що зрівноважена булева функція є кореляційно-імунною порядку k тоді й тільки тоді, коли всі функції, отримані шляхом фіксації довільних k її змінних довільними константами, є також зрівноваженими.

8. Оцініть кількість знаків гами, потрібної для успішного застосування атаки Зігенталера на комбінувальний генератор, який задовольняє умову (4.7) при $n = 32$, $k = 2$, $L_1 = L_2 = 512$, $\varepsilon = 2^{-20}$.

9. Знайдіть коефіцієнти Фур'є таких булевих функцій:

а) $x_1 \oplus x_2 \oplus \cdots \oplus x_n$;

б) $x_1 x_2 \oplus x_3 \oplus \cdots \oplus x_n$.

10. Знайдіть перетворення Фур'є та Уолша-Адамара булевої функції $h(x_1, x_2, x_3, x_4) = x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_2 x_3$.

11. Знайдіть перетворення Фур'є булевої функції, яка задається таким співвідношенням: $f(x_1, x_2, x_3, x_4, x_5) = 1 \Leftrightarrow 2 \le x_1 + x_2 + x_3 + x_4 + x_5 \le 3$.

12. Знайдіть коефіцієнти Фур'є булевої функції $f(x_1, x_2, x_3)$ з вектором значень

а) $(1\,0\,1\,1\,0\,0\,1\,0)^T$;

б) $(0\,0\,1\,1\,0\,1\,1\,1)^T$;

в) $(1\,1\,0\,1\,0\,1\,1\,0)^T$;

г) $(1\,1\,1\,0\,0\,1\,0\,1)^T$.

13. Розглянемо комбінувальний генератор гами з комбінувальною функцією

$$f(x_1, x_2, x_3, x_4) = x_1 x_2 x_4 \oplus x_1 x_2 x_3 \oplus x_2 x_3 \oplus x_3 x_4 \oplus x_1 \oplus x_3 \oplus 1.$$

Розрахуйте ймовірність появи 1 на виході цього генератора за умови, що змінні x_1, x_2, x_3, x_4 є незалежними випадковими величинами, розподіленими за законом $\Pr\{x_i = 1\} = 1 - \Pr\{x_i = 0\} = 1/4$, $i = \overline{1,4}$.

14. Знайдіть коефіцієнт Фур'є $C_f(\alpha)$ псевдобулевої функції $f(x_1, \ldots, x_n) = (1 + x_1) \cdots (1 + x_n)$ при $\alpha = (1, 1, \ldots, 1)$.

15. Нехай f – булева функція від n змінних, $\varepsilon \in (0, 1)$. Доведіть, що кількість векторів $\alpha \in V_n$ таких, що $\hat{f}(\alpha) \geq 2^n \varepsilon$, не перевищує ε^{-2}.

16. Нехай f – бент-функція від $n \geq 4$ змінних. Доведіть, що $\mathrm{AI}(f) \geq 2$.

17. Знайдіть афінні статистичні аналоги функцій, зазначених в задачі 12. Якими є нелінійності цих функцій?

18. Знайдіть який-небудь найімовірніший афінний статистичний аналог булевої функції $x_1 x_2 \oplus x_3 \oplus \cdots \oplus x_n$.

19. Нехай $F_{2^m} = F_2[z]/(g(z))$, де $g(z)$ – незвідний унітарний поліном степеня m над полем F_2. Доведіть, що вектор коефіцієнтів добутку елементів $a(z) = a_0 \oplus a_1 z \oplus \cdots \oplus a_{m-1} z^{m-1}$ та $b(z) = b_0 \oplus b_1 z \oplus \cdots \oplus b_{m-1} z^{m-1}$ поля F_{2^m} дорівнює добутку вектора $(a_0, a_1, \ldots, a_{m-1})$ на матрицю, i-й рядок якої є вектором коефіцієнтів полінома $b(z) z^i \bmod g(z)$, $i \in \overline{0, m-1}$.

20. Підстановка $\sigma : V_m \to V_m$ називається *ортоморфізмом*, якщо відображення $u \mapsto u \oplus \sigma(u)$, $u \in V_m$ також є підстановкою. Доведіть, що при $m = 2l$ ортоморфізмом є підстановка

$$\sigma(u_1, u_2) = (u_1 \oplus \varphi(u_2), u_2 \oplus \varphi(u_1 \oplus \varphi(u_2))), \; u_1, u_2 \in V_l,$$

яка реалізується двохраундовою мережею Фейстеля. Переконайтесь, що у випадку, коли σ є ортоморфізмом, кореляційна атака на спрощену версію SNOW 2.0-подібного шифру є незастосовною.

ПЕРЕЛІК ПОСИЛАНЬ

1. Олексійчук А. М. Методи криптоаналізу потокових шифрів [Електронний ресурс] : навч. посіб. для здобувачів ступеня магістра за освітньою програмою «Математичні методи криптографічного захисту інформації» спеціальності 113 Прикладна математика / А. М. Олексійчук, О. В. Курінний; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 995.3 Кбайт). – Київ : КПІ ім. Ігоря Сікорського, 2023. – 172 с. – Режим доступу: https://ela.kpi.ua/handle/123456789/52404 (дата звернення: 24.10.2024). – Назва з екрана.

2. Shannon C. E. Communication Theory of Secrecy Systems [Electronic resource] / C. E. Shannon // Bell System Technical Journal. – 1949. – Vol. 28, № 4. – P. 656–715. – Mode of access: https://doi.org/10.1002/j.1538-7305.1949.tb00928.x (date of access: 24.10.2024). – Title from screen.

3. Nyberg K. Differentially uniform mappings for cryptography [Electronic resource] / Kaisa Nyberg // Advances in Cryptology – EUROCRYPT ’93. – Berlin, Heidelberg. – P. 55–64. – Mode of access: https://doi.org/10.1007/3-540-48285-7_6 (date of access: 24.10.2024). – Title from screen.

4. Daemen J. AES Proposal: Rijndael [Electronic resource] / Joan Daemen, Vincent Rijmen. – 1999. – Mode of access: https://www.researchgate.net/publication/2237728_AES_proposal_rijndael (date of access: 24.10.2024). – Title from screen.

5. Bogdanov A. Biclique Cryptanalysis of the Full AES [Electronic resource] / Andrey Bogdanov, Dmitry Khovratovich, Christian Rechberger // Lecture Notes in Computer Science. – Berlin, Heidelberg, 2011. – P. 344–371. – Mode of access: https://doi.org/10.1007/978-3-642-25385-0_19 (date of access: 24.10.2024). – Title from screen.

6. Huang J. Transposition of AES Key Schedule [Electronic resource] / Jialin Huang, Xuejia Lai // Cryptology ePrint Archive, report 2012/260. – Mode of access: https://ia.cr/2012/260 (date of access: 24.10.2024). – Title from screen.

7. Murphy S. Essential Algebraic Structure within the AES [Electronic resource] / Sean Murphy, Matthew J. B. Robshaw // Advances in Cryptology – CRYPTO 2002. – Berlin, Heidelberg, 2002. – P. 1–16. – Mode of access: https://doi.org/10.1007/3-540-45708-9_1 (date of access: 24.10.2024). – Title from screen.

8. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. – [Чинний від 2015-07-01]. – Вид. офіц. – Київ : Мінекономрозвитку України, 2016.

9. Cryptographic Properties of a New National Encryption Standard of Ukraine [Electronic resource] / A. N. Alekseychuk [et al.] // Cybernetics and Systems Analysis. – 2016. – Vol. 52, № 3. – P. 351–364. – Mode of access: https://doi.org/10.1007/s10559-016-9835-0 (date of access: 24.10.2024). – Title from screen.

10. Ferguson N. Practical cryptography / Niels Ferguson, Bruce Schneier. – New York : John Wiley & Sons, 2003. – 410 p.

11. Biham E. Differential cryptanalysis of DES-like cryptosystems [Electronic resource] / Eli Biham, Adi Shamir // Journal of Cryptology. – 1991. – Vol. 4, №. 1. – P. 3–72. – Mode of access: https://doi.org/10.1007/BF00630563 (date of access: 24.10.2024). – Title from screen.

12. Improving the Upper Bound on the Maximum Differential and the Maximum Linear Hull Probability for SPN Structures and AES [Electronic resource] / Sangwoo Park [et al.] // Fast Software Encryption. – Berlin, Heidel-

berg, 2003. – P. 247–260. – Mode of access: https://doi.org/10.1007/978-3-540-39887-5_19 (date of access: 24.10.2024). – Title from screen.

13. Matsui M. Linear Cryptanalysis Method for DES Cipher [Electronic resource] / Mitsuru Matsui // Advances in Cryptology – EUROCRYPT '93. – Berlin, Heidelberg, 1994. – P. 386–397. – Mode of access: https://doi.org/10.1007/3-540-48285-7_33 (date of access: 24.10.2024). – Title from screen.

14. Vaudenay S. Decorrelation: A Theory for Block Cipher Security [Electronic resource] / Serge Vaudenay // Journal of Cryptology. – 2003. – Vol. 16, № 4. – P. 249–286. – Mode of access: https://doi.org/10.1007/s00145-003-0220-6 (date of access: 24.10.2024). – Title from screen.

15. Олексійчук, А. М. Показники та оцінки стійкості блокових шифрів відносно статистичних атак першого порядку / Антон Олексійчук, Артур Шевцов // Реєстрація, зберігання і обробка даних. – 2006. – Т. 8, № 4. – С. 53–63.

16. Alekseychuk A. N. Non-Asymptotic lower bounds for the data complexity of statistical attacks on symmetric cryptosystems [Electronic resource] / A.N. Alekseychuk // Cybernetics and Systems Analysis. – 2018. – Vol. 54, № 1. – P. 83–93. – Mode of access: https://doi.org/10.1007/s10559-018-0009-0 (date of access: 24.10.2024). – Title from screen.

17. Huffman D. Canonical forms for information-lossless finite-state logical machines [Electronic resource] / D. Huffman // IEEE Transactions on Information Theory. – 1959. – Vol. 5, № 5. – P. 41–59. – Mode of access: https://doi.org/10.1109/tit.1959.1057537 (date of access: 24.10.2024). – Title from screen.

18. Berbain C. On the Security of IV Dependent Stream Ciphers [Electronic resource] / Côme Berbain, Henri Gilbert // Fast Software Encryption. – Berlin, Heidelberg. – P. 254–273. – Mode of access:

https://doi.org/10.1007/978-3-540-74619-5_17 (date of access: 24.10.2024). – Title from screen.

19. Ekdahl P. A New Version of the Stream Cipher SNOW [Electronic resource] / Patrik Ekdahl, Thomas Johansson // Selected Areas in Cryptography. – Berlin, Heidelberg, 2003. – P. 47–61. – Mode of access: https://doi.org/10.1007/3-540-36492-7_5 (date of access: 24.10.2024). – Title from screen.

20. ДСТУ 8845:2019. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного потокового перетворення. – [Чинний від 2019-10-01]. – Вид. офіц. – Київ : ДП «УкрНДНЦ», 2019.

21. Alekseychuk A.N. Upper bounds on the imbalance of discrete functions implemented by sequences of finite automata [Electronic resource] / A. N. Alekseychuk, S. M. Koniushok, M. V. Poremskyi // Cybernetics and Systems Analysis. – 2019. – Vol. 55, № 5. – P. 752–759. – Mode of access: https://doi.org/10.1007/s10559-019-00185-w (date of access: 24.10.2024). – Title from screen.

22. Alekseychuk, A.N. A Method of evaluating the security of Snow 2.0-like ciphers against correlation attacks over the finite extensions of two element field [Electronic resource] / A. N. Alekseychuk, S. M. Koniushok, M. V. Poremskyi // Cybernetics and Systems Analysis. – 2020. – Vol. 56, № 1. – P. 40–52. – Mode of access: https://doi.org/10.1007/s10559-020-00220-1 (date of access: 24.10.2024). – Title from screen.

23. Олексійчук А. М. Достатня умова стійкості SNOW 2.0-подібних потокових шифрів відносно певних атак зі зв'язаними ключами [Електронний ресурс] / Антон Олексійчук // Захист інформації. – 2016. – Т. 18, № 4. – С. 261–268. – Режим доступу: https://doi.org/10.18372/2410-7840.18.11087 (дата звернення: 24.10.2024). – Назва з екрана.

24. Babbage S. H. Improved «exhaustive search» attacks on stream ciphers [Electronic resource] / S. H. Babbage // European Convention on Security and Detection, Brighton, UK. – 1995. – Mode of access: https://doi.org/10.1049/cp:19950490 (date of access: 24.10.2024). – Title from screen.

25. Golić J. D. Cryptanalysis of Alleged A5 Stream Cipher [Electronic resource] / Jovan Dj Golić // Advances in Cryptology – EUROCRYPT '97. – Berlin, Heidelberg, 1997. – P. 239–255. – Mode of access: https://doi.org/10.1007/3-540-69053-0_17 (date of access: 24.10.2024). – Title from screen.

26. Courtois N. T. Algebraic Attacks on Stream Ciphers with Linear Feedback [Electronic resource] / Nicolas T. Courtois, Willi Meier // Lecture Notes in Computer Science. – Berlin, Heidelberg, 2003. – P. 345–359. – Mode of access: https://doi.org/10.1007/3-540-39200-9_21 (date of access: 24.10.2024). – Title from screen.

27. Siegenthaler. Decrypting a Class of Stream Ciphers Using Ciphertext Only [Electronic resource] / Siegenthaler // IEEE Transactions on Computers. – 1985. – Vol. C-34, № 1. – P. 81–85. – Mode of access: https://doi.org/10.1109/tc.1985.1676518 (date of access: 24.10.2024). – Title from screen.

28. Поремський М. В. Методи обґрунтування стійкості SNOW-2.0-подібних потокових шифрів відносно кореляційних атак над скінченними полями порядку 2^r : дис. ... д-ра філософії: 125 Кібербезпека / Поремський Михайло Васильович. – Київ, 2020. – 153 с.