МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

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

А. М. Олексійчук, О. В. Курінний

МЕТОДИ КРИПТОАНАЛІЗУ ПОТОКОВИХ ШИФРІВ

Навчальний посібник

Рекомендовано Методичною радою КПІ ім. Ігоря Сікорського
як навчальний посібник для здобувачів ступеня магістра
за освітньою програмою «Математичні методи криптографічного
захисту інформації» спеціальності 113 Прикладна математика

Електронне мережне навчальне видання

Київ
КПІ ім. Ігоря Сікорського
2023

Рецензенти

Савчук М. М., доктор фіз.-мат. наук, член-кореспондент НАНУ, доцент, професор кафедри ММЗІ НН ФТІ

Ковальчук Л. В., доктор технічних наук, професор, професор кафедри ММЗІ НН ФТІ

Відповідальний редактор

Яковлєв С. В., кандидат технічних наук, доцент кафедри ММЗІ НН ФТІ

Гриф надано Методичною радою КПІ ім. Ігоря Сікорського (протокол № 4 від 19.01.2023 р.) за поданням Вченої ради Фізико-технічного інституту (протокол № 1 від 16.01.2023 р.)

У посібнику викладено низку сучасних методів криптоаналізу синхронних потокових шифрів, а також основи математичного апарату, на якому ґрунтуються зазначені методи.

Призначено для студентів та аспірантів, які навчаються за освітньою програмою «Математичні методи криптографічного захисту інформації».

Реєстр. № НП 22/23-413. Обсяг 5,47 авт. арк.

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
проспект Перемоги, 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 навчальний посібник створено на основі матеріалів лекцій з навчальної дисципліни «Методи криптоаналізу», яка викладається здобувачам ступеня магістра на кафедрі математичних методів захисту інформації Навчально-наукового фізико-технічного інституту Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».

При відборі матеріалу ставилося за мету викласти базові поняття і результати, а також надати уявлення про різноманіття сучасних методів, які використовуються при дослідженні стійкості синхронних потокових шифрів. Посібник складається з трьох розділів, основними з яких є другий і третій, присвячені, відповідно, алгебраїчним і статистичним методам криптоаналізу, а також основам математичного апарату, на якому ці методи, значною мірою, ґрунтуються.

Відмінною рисою посібника є оригінальність змісту: переважна більшість представлених результатів, методів або криптоаналітичних атак викладена у навчальній літературі вперше. Низку пунктів (зокрема, 2.1 – 2.4, 3.2, 3.10, 3.11) написано на основі наукових результатів, отриманих за участі першого автора посібника.

Наприкінці кожного пункту містяться задачі для самостійного розв'язання, більшість з яких спрямована на розвиток ідей і методів, викладених в основній частині книги.

Опанувавши теоретичний матеріал та розв'язавши більшість задач, читач набуде можливості краще орієнтуватися в сучасній науковій літературі з методів криптоаналізу потокових шифрів.

Автори вдячні колегам з кафедри ММЗІ за увагу, проявлену до попередньої версії цього навчального посібника.

Перелік позначень

$\mathbb{N}$	множина натуральних чисел
$\mathbb{N}_0$	множина $\mathbb{N} \cup \{0\}$
$\mathbb{R}$	множина дійсних чисел
$\square$	закінчення доведення
$X \times Y$	декартів добуток множин X та Y
$f : X \to Y$	відображення f множини X у множину Y
$\lvert X \rvert$	потужність множини X
$\overline{i, j}$	множина $\{i, i+1, \ldots, j\}$, де i, j – невід'ємні цілі числа
$\log x$	логарифм за основою 2
$\ln x$	натуральний логарифм
ЛРЗ	лінійний регістр зсуву
V_n	множина двійкових векторів довжини n
B_n	множина булевих функцій від n змінних
$\oplus$	додавання за модулем 2
$I \lhd B_n$	множина I є ідеалом кільця B_n
$\langle g_1, \ldots, g_m \rangle$	ідеал, породжений множиною $\{g_1, \ldots, g_m\}$
$V(I)$	множина нулів ідеалу I

$J(M)$	ідеал, що складається з усіх булевих функцій, які обертаються в нуль на множині M
$\mathrm{Ann}\,(I)$ $(\mathrm{Ann}\,(f))$	анулятор ідеалу I (функції f)
$\dim(I)$	розмірність ідеалу I
$\lvert\alpha\rvert$	мультистепінь вектора α
$\preceq_{\mathrm{lex}}$	відношення лексикографічного порядку
$\preceq_{\mathrm{drl}}$	відношення степеневого зворотного порядку
$\mathrm{LM}_{\preceq}(f)$	старший моном (член) функції $f \in B_n\backslash\{0\}$ відносно впорядкування $\preceq$
$\alpha \perp \beta$ $(x^\alpha \perp x^\beta)$	вектори (мономи) є диз'юнктними
$\mathrm{Res}(f; f_1, \ldots, f_m)$	залишок від ділення функції $f \in B_n$ на систему функцій $f_1, \ldots, f_m \in B_n\backslash\{0\}$
$\deg f$	степінь полінома Жегалкіна функції f
$\mathrm{mindeg}\, I$	мінімальний степінь ідеалу I
$\mathrm{rank}\,(M)$	ранг матриці M
$\mathrm{AI}\,(f)$	алгебраїчна імунність функції f
$\mathrm{AI}'\,(s)$	алгебраїчна імунність вектор-функції s
$\mathbb{F}_q$	скінченне поле порядку q
$\overset{r}{+}$	додавання за модулем 2^r
$\mathfrak{B}$	базис скінченного поля
$\lvert\lvert f\rvert\rvert$, $\mathrm{wt}(f)$	вага двійкового вектора (або булевої функції) f
$\lvert\lvert f\rvert\rvert_2$	евклідова норма функції f
$\langle f, g\rangle$	скалярний добуток функцій f і g
H_n	матриця Адамара порядку 2^n

$\delta_{\alpha,\beta}$	символ Кронекера
$C_f(\alpha)$	коефіцієнт Фур'є функції f, який відповідає вектору $\alpha \in V_n$
$\hat{f}(\alpha)$	коефіцієнт Уолша-Адамара функції f, який відповідає вектору $\alpha \in V_n$
N_f	нелінійність функції f
Tr	слід (абсолютний) поля $\mathbb{F}_{2^r}$
$\mathrm{Tr}_{2^t}^{2^r}$	слід поля $\mathbb{F}_{2^r}$ над підполем $\mathbb{F}_{2^t}$
$D_\alpha f(x)$	похідна функції f за напрямом $\alpha \in V_n$

1 Синхронні потокові шифри

Під криптоаналізом зазвичай розуміють методологію отримання обґрунтованих оцінок стійкості криптосистем (шифрів) або криптографічних протоколів. Ця методологія має дві сторони:

– негативну, яка полягає у побудові атак на шифр, тобто зламуванні шифру;

– позитивну, яка полягає в обґрунтуванні стійкості шифру, тобто доведенні того, що на нього нема ефективних атак з певного класу.

Отже, як випливає з самої назви, криптоаналіз являє собою аналіз (а точніше, дослідження) стійкості шифру. Якщо в результаті цього аналізу вдається знайти слабкості, то з'являються атаки на шифр. Якщо ж, навпаки, виявляється, що в певному класі атак нема ефективних, отримують обґрунтування стійкості шифру відносно зазначених атак.

Потокові шифри є історично найвідомішими та найдавнішими криптосистемами. Вони застосовувалися ще до того, як з'явились традиційні блокові шифри на кшталт `DES` або `AES`. На сьогодні потокові шифри використовуються у багатьох інформаційних і телекомунікаційних системах, де висуваються підвищені вимоги до швидкості передачі інформації (зокрема, у системах стільникового або мобільного зв'язку). Зауважимо також, що слід відрізняти потокові шифри від блокових шифрів, які використовуються в потокових режимах. Тому далі розглядатимемо саме спеціально побудовані потокові шифри (dedicated stream ciphers).

Виділяють дві основні переваги потокових шифрів:

– висока швидкість шифрування;

– відсутність розповсюдження помилок.

Остання властивість полягає в наступному: якщо при передачі шифрованого повідомлення каналом зв'язку сталося t помилок, то при розшифруванні цього повідомлення кількість спотворень у відкритому тексті є не більше ніж t.

Зауважимо, що у блокових шифрах, навпаки, помилки розповсюджуються на велику кількість символів, оскільки такі шифри, як правило, забезпечують лавинний ефект. Зазначимо також, що на відміну від блокових шифрів, серед яких найпоширенішими є SP-мережі та мережі Фейстеля, різноманітних конструкцій потокових шифрів існує набагато більше. Це знаходить своє відображення і у методах криптоаналізу потокових шифрів.

Однією з основних складових будь-якого потокового шифру є генератор гами, стандартною математичною моделлю якого є скінченний автомат. Тому цей розділ починається з базових відомостей про скінченні автомати та їхні властивості (такі як необоротність за Гаффманом), що можуть бути застосовані в криптоаналізі. Крім того, розглядаються сучасні означення понять стійкого генератора гами та стійкого потокового шифру.

Завершується розділ докладним аналізом певної атаки на комбінувальні генератори гами з нерівномірним рухом, яка (серед іншого) покликана продемонструвати різноманіття сучасних методів криптоаналізу потокових шифрів.

1.1 Скінченні автомати

Скінченний автомат є стандартною моделлю будь-якого детермінованого пристрою перетворення дискретної інформації. Все, що визначається з використанням детермінованих рекурентних залежностей, можна описати за допомогою автомата.

Перейдемо до означення поняття автомата та опису його функціонування.

Означення 1.1. Нехай X, S, Y – скінченні множини, $h : S \times X \to S$ і $f : S \times X \to Y$ – функції. Тоді впорядкована п'ятірка об'єктів (X, S, Y, h, f) називається *скінченним автоматом* (або *автоматом Мілі*) з множиною станів S, вхідним алфавітом X, вихідним алфавітом Y, функцією переходів h та функцією виходів f.

Автомат $A = (X, S, Y, h, f)$ функціонує в дискретні моменти часу $i = 0, 1, 2, \ldots$, які називаються *тактами*. Починає роботу автомат A з *початкового стану* $s_0 \in S$. Якщо на вхід автомата 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 автомат знаходиться в початковому стані s_0, і (в нульовому такті) на вхід подається знак x_0. Тоді автомат переходить в наступний стан $s_1 = h(s_0, x_0)$ та формує знак вихідної послідовності $y_0 = f(s_0, x_0)$. Зараз, в першому такті, автомат знаходиться в стані s_1 та отримує на вхід наступний знак x_1. Тоді автомат переходить в стан $s_2 = h(s_1, x_1)$ і формує знак вихідної послідовності $y_1 = f(s_1, x_1)$.

Умовна схема роботи автомата в i-ому такті зображена на рис. 1.1.

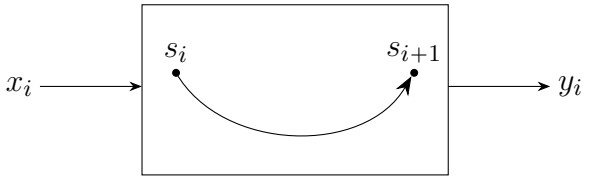

Рис. 1.1: Скінченний автомат в i-ому такті

Розглянемо декілька видів скінченних автоматів.

1. Автомат A називається *автоматом Мура*, якщо функція виходів f не залежить від вхідної 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 залежать 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 $h : S \to S$, $f : S \to Y$. Такий автомат починає роботу з деякого початкового стану і формує вихідну послідовність, яка цілком залежить від нього.

3. Автомат A називається *автоматом без пам'яті*, якщо $|S| = 1$. В цьому випадку можна виключити множину S з розгляду та не розглядати функцію h, яка стає 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 використовую-

ться тільки для оновлення станів. При цьому можна не розглядати функцію f, яка вироджується у константу. Таким чином, автомат без виходу є просто функцією переходів $h : S \times X \to S$.

Розглянемо декілька прикладів скінченних автоматів.

Приклад 1.1. 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; див. рис. 1.2).

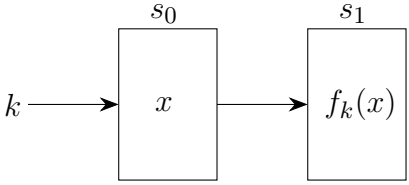

Рис. 1.2: Блоковий шифр як скінченний автомат

Якщо шифр є ітераційним і в ролі ключа k використовується послідовність раундових ключів $k = (k_1, \ldots, k_r)$, то ці ключі застосовуються один за одним до проміжних повідомлень з множини V_n, які розглядаються як стани автомата. В такому разі 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.

1.2 Граф скінченного автомата. Необоротність скінченного автомата за Гаффманом

Кожний скінченний автомат може бути представлений у вигляді певного графа.

Означення 1.2. *Графом скінченного автомата* $A=(X,S,Y,h,f)$ називається позначений орієнтований граф $G_A = (V,E)$, множина V вершин якого співпадає 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 $x \in X$.

Розглянемо декілька прикладів побудови графів скінченних автоматів.

Приклад 1.2. Розглянемо автомат $A_1 = (X,S,Y,h,f)$, 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. 1.3 (зліва).

Розглянемо автомат $A_2 = (X, S, Y, h, f)$, в якому

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

Граф цього автомата зображено на рис. 1.3 (справа).

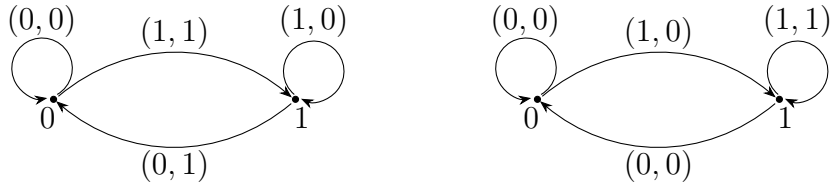

Рис. 1.3: Графи автоматів A_1 та A_2

Розглянемо властивість скінченного автомата, сформульовану Гаффманом [Huff].

Означення 1.3. 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 $(x_0, y_0), \ldots, (x_{k-1}, y_{k-1})$ та $(x'_0, y_0), \ldots, (x'_{k-1}, y_{k-1})$ відповідно такі, що $x_0, \ldots, x_{k-1}$ та $x'_0, \ldots, x'_{k-1}$ – два різні набори вхідних символів, $k \geqslant 1$.

Інакше кажучи, автомат є необоротним за Гаффманом, якщо в його графі існують шляхи, зображені на рис. 1.4. 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 якого він почав працювати;

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

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

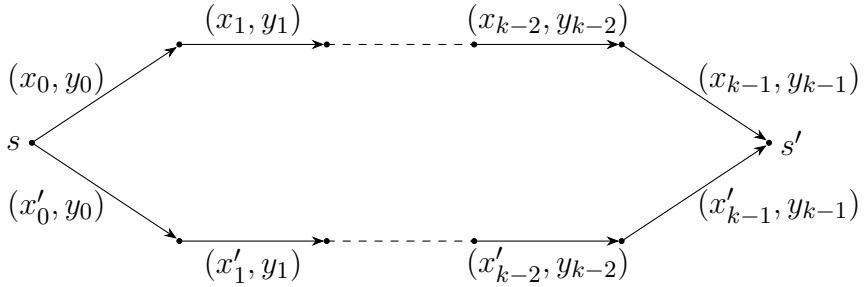

Рис. 1.4: Шляхи у G_A, що свідчать про необоротність автомата за Гаффманом

Тоді якщо автомат A є необоротним за Гаффманом, то, взагалі кажучи, за цими даними неможливо однозначно відновити відповідну вхідну послідовність $x_0, \ldots, x_{k-1}$ (див. рис. 1.4). Навпаки, для оборотного за Гафманом автомата за будь-якою вихідною послідовністю та парою станів (початковим і фінальним) завжди можна однозначно відновити відповідну вхідну послідовність.

Приклад 1.3. Розглянемо граф G_{A_2} з прикладу 1.2 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 $1, 0$.

Приклад 1.4. Розглянемо автомат A_1 з прикладу 1.2 та переконаємося, 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), $i \in \overline{0, k-1}$, $k \geqslant 1$. 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:

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

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

$$\begin{aligned} x_0 &= s_0 \oplus y_0, \\ x_1 &= s_1 \oplus y_1 = x_0 \oplus y_1 = s_0 \oplus y_0 \oplus y_1, \\ &\dots \quad \dots \quad \dots \quad \dots \\ x_{k-1} &= s_{k-1} \oplus y_{k-1} = x_{k-2} \oplus y_{k-1} = s_0 \oplus y_0 \oplus \dots \oplus y_{k-1}. \end{aligned}$$

Таким чином, наведена система рівнянь має єдиний розв'язок $(x_0, x_1, \ldots, x_{k-1})$, 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.

Означення 1.4. Нехай $A = (X, S, Y, h, f)$ – скінченний автомат, k – натуральне число, $k \geqslant 1$. Тоді відображення

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

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

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

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

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

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

$$\begin{cases} f(s_0, x_0) = y_0, \\ \qquad \cdots\cdots \\ f(s_{k-1}, x_{k-1}) = y_{k-1}, \\ s_1 = h(s_0, x_0), \\ \qquad \cdots\cdots \\ s_k = h(s_{k-1}, x_{k-1}). \end{cases} \tag{1.1}$$

Доведемо таке твердження.

Твердження 1.1. *Нехай $A = (X, S, Y, h, f)$ – скінченний автомат. Якщо він є оборотним за Гаффманом, то для кожного $\overline{y} \in Y^k$ система рівнянь (1.1) має не більше $|S|^2$ розв'язків.*

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

Доведення. Нехай автомат A є оборотним за Гаффманом. Тоді для будь-яких фіксованих значень змінних s_0 та s_k система рівнянь (1.1) має не більше одного розв'язку. Дійсно, число таких розв'язків дорівнює числу шляхів у графі автомата A, що мають позначки над ребрами $(x_0, y_0), \ldots, (x_{k-1}, y_{k-1})$, починаються у вершині s_0 та закінчуються у вершині s_k, а їхня кількість не перевищує 1 на підставі означення 1.3. Таким чином, загальна кількість розв'язків системи (1.1) 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

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

Справедлива рівність

$$S \times X^k = \bigcup_{\overline{y} \in Y^k} F_k^{-1}(\overline{y}),$$

причому множини $F_k^{-1}(\overline{y})$ в об'єднанні попарно не перетинаються (див. рис. 1.5).

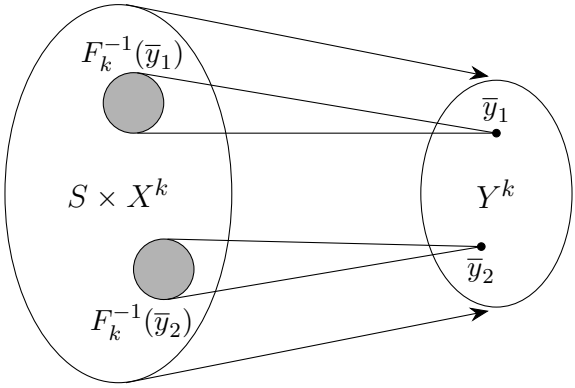

Рис. 1.5: Прообрази елементів $\overline{y}_1$ та $\overline{y}_2$ при відображенні F_k не перетинаються

Звідси випливає, що

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

і, отже,

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

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

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

З іншого боку, якщо автомат A є оборотним за Гаффманом, то за доведеним для кожного $\overline{y} \in Y^k$ справедлива нерівність $\eta_k(\overline{y}) \leqslant |S|^2$. Таким чином, за умови $|X| > |Y|$ автомат A є необоротним за Гаффманом, що й треба було довести. □

1.3 Генератори гами

Означення 1.5. *Генератором гами* (або *генератором псевдовипадкових послідовностей*) називається 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 $\gamma_i = f(s_i)$, $i = 0, 1, 2, \ldots$, 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

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

яка називається *системою рівнянь гамоутворення* генератора Γ.

Генератор гами можна розглядати також як сім'ю певних відображень.

Означення 1.6. Нехай $\Gamma = (S, Y, h, f)$ – генератор гами, L – натуральне число. Тоді відображення

$$s_0 \mapsto \gamma_0, \gamma_1, \ldots, \gamma_{L-1},$$

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 *гамоутворюючим 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 гамоутворюючих відображень, параметризованих натуральними числами $L = 1, 2, \ldots$. Значенням кожного такого відображення є відрізок гами певної довжини, вироблений за початковим станом генератора. Часто в літературі генератори гами визначають саме через такі відображення.

Характеристичною властивістю гамоутворюючого відображення є *перетворення початку в початок*. А саме, для будь-яких натуральних чисел L_1 та L_2, де $L_1 < L_2$, та 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 гамоутворюючого 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 зору, 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 початковим станом s_0, або випадкову рівноймовірну послідовність довжини L над алфавітом Y.

2. Дослідник передає Криптоаналітику послідовність $y = y_0, \ldots, y_{L-1}$, 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:

$$H_0 : \ y = \gamma;$$
$$H_1 : \ y \text{ є суто випадковою.}$$

Означення 1.7. Нехай $T > 0$, $0 < \varepsilon < 1/2$. Генератор гами Γ називається (T, ε)-*псевдовипадковим*, якщо будь-який критерій для розрізнення зазначених вище гіпотез H_0 та H_1, що має середню ймовірність помилки не вище ε, використовує принаймні T (умовних) операцій (нагадаємо, що середня ймовірність помилки критерію визначається за формулою

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

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

Іншими словами, генератор гами є (T, ε)-псевдовипадковим, якщо не існує способу відрізнити його вихідну послідовність (певної, достатньо великої довжини L), отриману при випадковому рівноймовірному початковому стані, від суто випадкової послідовності такої ж довжини над алфавітом Y з середньою ймовірністю помилки не вище 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 складає $\log|S| = 128$ бітів, то такий генератор можна вважати стійким за умови його (T, ε)-псевдовипадковості при $L = 2^{80}$, $\varepsilon = 1/2 - 2^{-20}$, $T = 2^{128}$. (Зауважимо, що такий підхід відображає так звану *конкретну стійкість* криптосистем на відміну від їх асимптотичної стійкості; див., наприклад, п. 3.1 в [KL]).

Означення 1.7 є загальновизнаним, але наразі не існує методів для доведення псевдовипадковості генераторів гами. Окрім того, існування псевдовипадкових генераторів близько пов'язано з проблемою існуванням 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.

Твердження 1.2. *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 дозволяє розрізнити гіпотези H_0 та H_1 в описаній вище грі між Дослідником та Криптоаналітиком із середньою ймовірністю помилки $p_{err} \leqslant 1/2 \cdot (\varepsilon + 2^{N-L})$, використовуючи $T + \tau_L$ операцій, де τ_L – складність обчислення відрізка гами довжини L за початковим станом генератора.

Доведення. Нагадаємо, що під час гри Дослідник випадково рівноймовірно генерує початковий стан s_0 генератора гами та передає Криптоаналітику послідовність y, яка з ймовірністю $1/2$ співпадає 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 $p_{err} \leqslant 1/2 \cdot (\varepsilon + 2^{N-L})$.

За означенням середньої ймовірності помилки

$$p_{err} = 1/2 \cdot (\Pr(H_1|H_0) + \Pr(H_0|H_1)). \tag{1.2}$$

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

Нехай зараз справедлива гіпотеза H_1, тобто y є суто випадковою послідовністю довжини L над алфавітом Y, і критерій B припускається помилки. Тоді існує початковий s стан 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, що $\Pr(H_0|H_1) \leqslant 2^{N-L}$.

Підставляючи наведені оцінки ймовірностей $\Pr(H_1|H_0)$ та $\Pr(H_0|H_1)$ у формулу (1.2), отримаємо потрібну нерівність $p_{err} \leqslant 1/2 \cdot (\varepsilon + 2^{N-L})$.

□

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, як правило, використовуються *лінійні регістри зсуву* (ЛРЗ), які (за умови примітивності їхніх поліномів зворотного зв'язку) дозволяють 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.

З метою уточнення термінології та позначень нагадаємо, що ЛРЗ довжини m над (довільним) полем F визначається за допомогою *полінома зворотного зв'язку* $f(x) = x^m - c_{m-1}x^{m-1} - \ldots - c_0x^0$ над цим полем і являє собою автономний автомат з множиною станів F^m та функцією переходів

$$h(z_{m-1}, \ldots, z_0) = (z_{m-1}, \ldots, z_0)C(f(x)),\ (z_{m-1}, \ldots, z_0) \in F^m,$$

де

$$C(f(x)) = \begin{pmatrix} c_{m-1} & 1 & 0 & \ldots & 0 \\ c_{m-2} & 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ c_1 & 0 & 0 & \ldots & 1 \\ c_0 & 0 & 0 & \ldots & 0 \end{pmatrix}. \qquad (1.3)$$

Комірки ЛРЗ і координати вектора, який зберігається у регістрі в i-му такті, нумеруються як зазначено на рис. 1.6. Такий регістр виробляє за початковим станом $(x_{m-1}, \ldots, x_0) \in F^m$ *лінійну рекурентну послідовність* (або *лінійну рекуренту*) $x_0, x_1, \ldots$ таку, що

$$(x_{i+m-1}, \ldots, x_i) = (x_{m-1}, \ldots, x_0)C(f(x))^i, \ i = 0, 1, \ldots.$$

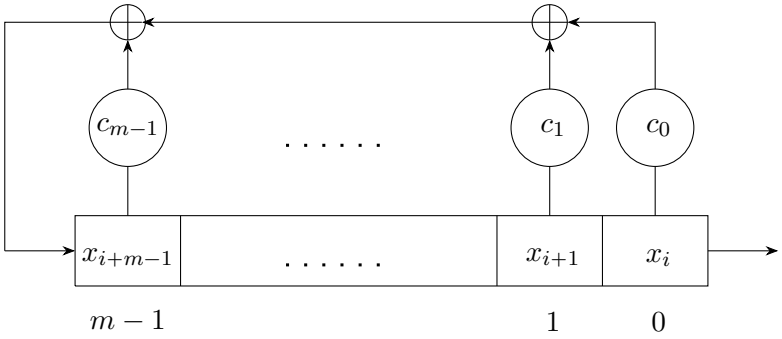

Рис. 1.6: Лінійний регістр зсуву

На сьогодні відомо чимало різноманітних способів побудови генераторів гами, які базуються на різних варіантах ускладнення попередніх гам. Це, зокрема, використання регістрів зсуву з *нелінійним зворотним зв'язком*, *функцій ускладнення*, *нерегулярного проріджування/стискування* (decimation/shrinking), *нерегулярних покрокових функцій* (stepping function), «блоково-подібних» конструкцій, які застосовуються, наприклад, у шифрах `RC4`, `SNOW 2.0` та `SCREAM`, що орієнтовані на швидку програмну реалізацію. Різноманіття конструкцій сучасних потокових шифрів вважається однією з причин менш стабільного стану в галузі їх криптоаналізу, на відміну від блокових шифрів, переважну більшість яких можна віднести до SP-мереж або до шифрів Фейстеля.

Незважаючи на це, у багатьох публікаціях виділяють три загальних методи побудови генераторів гами:

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

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

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

На рис. 1.7 показано криптосхеми фільтрувального та комбінувального генераторів гами. Зазначені генератори є класичними та застосовуються у багатьох конструкціях сучасних потокових шифрів.

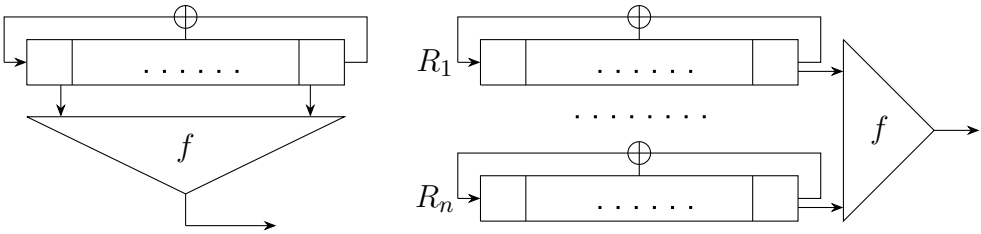

Рис. 1.7: Фільтрувальний (зліва) та комбінувальний генератори гами

Одним із загальних способів підвищення криптографічної стійкості зазначених 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 з зовнішнім управлінням рухом.

Нехай $\Gamma = (S, Y, h, f)$ – генератор гами, $(U,\ p_U)$ – дискретне джерело без пам'яті, де $U \subseteq \mathbb{N}_0 = \{0, 1, 2, \ldots\}$, p_U — розподіл ймовірностей на множині U. Це джерело виробляє послідовність незалежних випадкових величин $\varepsilon(0), \varepsilon(1), \ldots$, кожна з яких розподілена на множині U за законом $\Pr(\varepsilon(i) = a) = p_U(a)$, $a \in U$, $i = 0, 1, \ldots$.

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

$$s_{i+1} = h(s_i), \quad i = 0, 1, 2, \ldots. \tag{1.4}$$

Розглянемо випадкові величини $\delta(0) \equiv 0$, $\delta(i) = \varepsilon(0) + \ldots + \varepsilon(i-1)$, де $i = 1, 2, \ldots$, та визначимо послідовность $\gamma_0, \gamma_1, \gamma_2, \ldots$ знаків алфавіту Y за формулою

$$\gamma_i = f\left(s_{\delta(i)}\right), \quad i = 0, 1, 2, \ldots. \tag{1.5}$$

Зазначимо, що $\gamma_0, \gamma_1, \gamma_2, \ldots$ є випадковою послідовністю, яка залежить від послідовності $\delta(0), \delta(1), \delta(2), \ldots$ та початкового стану s_0 генератора гами Γ. Як правило вважають, що s_0 є випадковим елементом, який не залежить від послідовності $\delta(0), \delta(1), \delta(2), \ldots$ та має рівномірний розподіл ймовірностей на множині S.

Означення 1.8. 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 Г.

На завершення розглянемо більш загальний варіант управління рухом генератора гами, який являє собою каскад паралельного з'єднання n автономних автоматів без виходу та автомата без пам'яті.

Нехай $S = V_{m_1} \times \ldots \times V_{m_n}$, $\Gamma = (S, Y, h, f)$ – автономний автомат з функцією переходів

$$h(z_1, \ldots, z_n) = (h_1(z_1), \ldots, h_n(z_n)),\ z_j \in V_{m_j}, \tag{1.6}$$

де $h_j : V_{m_j} \to V_{m_j}$, $j \in \overline{1,n}$. Нехай, далі,

$$(x_1(i+1), \ldots, x_n(i+1)) = (h_1(x_1(i)), \ldots, h_n(x_n(i))),\ i = 0, 1, \ldots \tag{1.7}$$

внутрішня послідовність автомата Г, що відповідає його початковому стану $(x_1(0), \ldots, x_n(0))$. Припустимо, що $U \subseteq \mathbb{N}_0^n$ та $\varepsilon(i) = (\varepsilon_1(i), \ldots, \varepsilon_n(i))$ є n-вимірним випадковим вектором, що розподілений на множині U за законом p_U, $i = 0, 1, \ldots$. Позначимо, як і раніше

$$\delta(0) \equiv 0,\ \delta(i) = (\delta_1(i), \ldots, \delta_n(i)) =$$
$$= \varepsilon(0) + \ldots + \varepsilon(i-1),\ i = 1, 2, \ldots, \tag{1.8}$$

та визначимо випадкову послідовність

$$\gamma_i = f(x_1(\delta_1(i)), \ldots, x_n(\delta_n(i))), \quad i = 0, 1, \ldots. \tag{1.9}$$

Зауважимо, що співвідношення (1.7), (1.9) являють собою n-вимірне узагальнення співвідношень (1.4), (1.5).

Конкретним прикладом генератора, функціонування якого описується наведеними рівностями (1.7) – (1.9), є комбінувальний генератор гами з нерівномірним рухом. В цьому випадку функція (1.6) визначається за формулою $h(z_1, \ldots, z_n) = (z_1 C_1, \ldots, z_n C_n)$, де z_j позначає поточний стан ЛРЗ R_j, а C_j – матрицю, що задається його поліномом зворотного зв'язку, $j \in \overline{1,n}$. Знак вихідної послідовності даного генератора гами має вигляд (1.9), де функція $f : V_n \to \{0,1\}$ залежить лише від перших координат булевих векторів $x_1(\delta_1(i)), \ldots, x_n(\delta_n(i))$.

1.4 Синхронні потокові шифри

Означення 1.9. *Синхронний (адитивний двійковий) потоковий шифр* – це шифр, що визначається за допомогою таких об'єктів.

1. Генератора гами $\Gamma = (S, Y, h, f)$, де $S = V_N$ для деякого $N \in \mathbb{N}$ та (як правило) $Y = V_2$.

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 $c \in V_{l_1}$ повертає початковий стан генератора $s_0 = F(k, c)$, що є двійковим вектором довжини N.

3. Правилом накладання гами, яке (як правило) визначається за формулою

$$y_i = x_i \oplus \gamma_i, \quad i = 0, 1, 2, \ldots,$$

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 $s_{i+1} = h(s_i)$, $\gamma_i = f(s_i)$, $i = 0, 1, 2, \ldots$ (див. рис. 1.8).

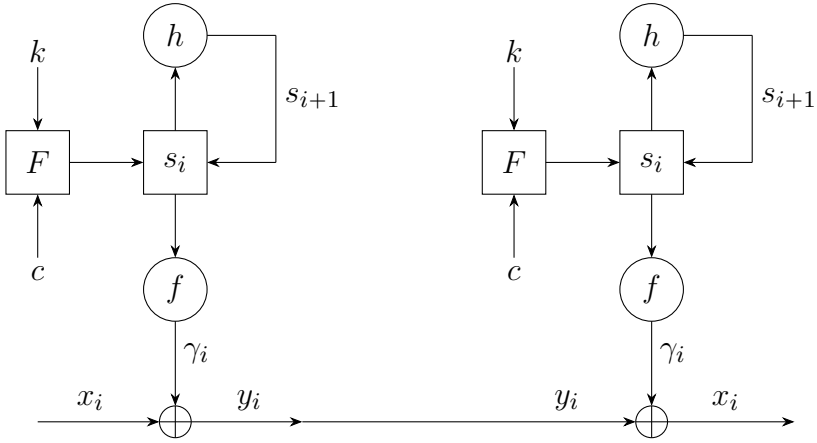

Рис. 1.8: Схематичне зображення процедури шифрування з використанням синхронного потокового шифру

Надалі термін потоковий шифр означає синхронний потоковий шифр. Зауважимо, що при побудові таких шифрів треба обов'язково визначати алгоритм генерації 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 прикладом шифру з лінійним відображенням F є алгоритм шифрування `A5/1`).

Визначимо 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 $\Gamma_L : V_N \to V_L$ гамоутворююче відображення, обмежене на довжині L, що відповідає генератору Γ (див. означення 1.6), та покладемо $\Phi_k = \Gamma_L \circ F_k$. Тоді синхронний потоковий шифр реалізує сім'ю відображень $(\Phi_k : k \in V_{l_0})$ множини V_{l_1} векторів ініціалізації в множину V_L відрізків гами (див. рис. 1.9).

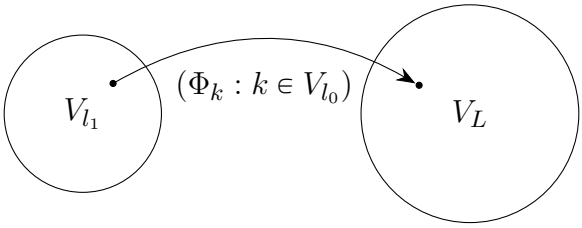

Рис. 1.9: Синхронний потоковий шифр як сім'я відображень $(\Phi_k : k \in V_{l_0})$

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 $1/2$ співпадає 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).

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 істинною.

Означення 1.10. Нехай $T > 0$, $t \in \mathbb{N}$, $0 < \varepsilon < 1/2$. 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 задачу розрізнення гіпотез можна сформулювати у більш звичних термінах розподілів ймовірностей. Припустимо, не обмежуючи суттєво загальності, що усі відображення Φ_k, де $k \in V_{l_0}$, є попарно різними. Розглянемо сукупність відображень множини V_{l_1} в множину V_L, на який задано розподіл ймовірностей. Відомо, що за умови справедливості гіпотези H_1 цей розподіл є рівномірним на всій сукупності відображень, а за умови справедливості гіпотези H_0 є рівномірним на підмножині $\{\Phi_k : k \in V_{l_0}\}$ цієї сукупності. Тоді задача полягає в тому, щоб розрізнити два зазначені розподіли за умови вільного доступу до оракула, який реалізує випадкове відображення, обране (з ймовірністю $1/2$) відповідно до однієї із зазначених гіпотез.

Зауважимо також, що означення 1.10 є аналогічним до означення стійкого блокового шифру. (Нагадаємо, що такий шифр являє собою сім'ю підстановок, параметризованих ключами, і називається стійким, якщо його не можна статистично відрізнити за прийнятний час із достатньо високою ймовірністю від суто випадкової підстановки).

Наведене означення стійкого потокового шифру сформувалося приблизно у 2007 році 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 [BG] отримано доведення стійкості з використанням припущення, що задача розв'язання випадково згенерованої системи квадратичних рівнянь над скінченним полем є обчислювально складною.

1.5 Класифікація атак на синхронні потокові шифри

Сформульоване вище означення стійкого потокового шифру надає можливість навести загальну класифікацію атак на синхронні потокові шифри. Виділяють три ознаки, за якими класифікують ці атаки.

1. *Мета противника.* В залежності від неї можна поділити атаки на розрізнювальні та ті, що спрямовані на відновлення ключа або початкового стану генератора гами.

Якщо противник має на меті відрізнити задане за допомогою оракула відображення Φ_k (для випадково обраного невідомого ключа $k \in V_{l_0}$) від суто випадкового відображення множини V_{l_1} в множину V_L, то така атака називається *розрізнювальною* (або *розпізнавальною*; distinguishing attack). Як варіант, відзначимо розрізнювальну атаку, спрямовану на те, щоб відрізнити гаму, вироблену генератором Г при випадковому рівноймовірному початковому стані, від суто випадкової послідовності відповідної довжини над вихідним алфавітом.

Якщо противник має на меті відновити ключ або початковий стан генератора, то атака такого типу називається *спрямованою на відновлення ключа* (key recover attack) або, відповідно, початкового

стану. Твердження 1.2 показує, що наявність подібної атаки тягне за собою можливість побудувати розрізнювальну атаку (неформально кажучи, якщо можна відновити, то можна також відрізнити).

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

Якщо противнику відомі відкритий та шифрований тексти, він може обчислити гаму. Отже, в цьому випадку можна ставити задачу відновлення початкового стану генератора за відрізком гами (класична задача криптоаналізу потокових шифрів).

При проведенні атак на основі підібраних векторів ініціалізації противник має вільний доступ до оракула Φ та може отримувати послідовності $\Phi(c_1), \ldots, \Phi(c_t)$ для будь-яких векторів ініціалізації $c_1, \ldots, c_t \in V_{l_1}$ (див. означення 1.10). Зауважимо, що кількість t зазначених векторів є одним з параметрів, що характеризують ефективність атаки. Іншим важливим параметром є мінімальна довжина відрізка гами, виробленої при фіксованому ключі, яка потрібна для реалізації атаки.

Таким чином, при створенні синхронного потокового шифру розробник повинен явно визначати такі два параметри:

– довжина відрізка гами, яку дозволяється виробляти при фіксованих значеннях ключа $k \in V_{l_0}$ та вектора ініціалізації $c \in V_{l_1}$;

– кількість векторів ініціалізації, які можна використовувати при фіксованому ключі, тобто *термін дії ключа*.

Якщо розробник не зазначає ці параметри, то при побудові атак противник може вибирати їх значення довільним чином. Зауважимо

також, що будь-яка атака вважається ефективною, якщо її часова складність (при заданій, достатньо малій імовірності помилки) є помітно менше за трудомісткість повного перебору.

3. *Метод криптоаналізу.* В залежності від методів, які використовуються для розв'язання криптоаналітичних задач, виділяють *алгебраїчні*, *статистичні* (*кореляційні*), *змішані* атаки тощо.

Алгебраїчними називають атаки, що базуються на розв'язанні систем алгебраїчних рівнянь, які пов'язують знаки гами, виробленої генератором, з його початковим станом. Статистичні атаки базуються на ймовірнісно-статистичних методах і, як правило, полягають у розв'язанні задач перевірки (двох або декількох) статистичних гіпотез. Змішаними називають атаки, які базуються на сумісному застосуванні різних за сутністю математичних методів. Як приклад, відзначимо атаки типу TMDTO (Time Memory Data Trade Off), які поєднують перебір зі статистичними методами. Зрозуміло, що клас, до якого відносять ту чи іншу атаку за типом методу криптоаналізу, визначається досить умовно.

В залежності від наведених ознак, можна класифікувати практично будь-яку атаку на потоковий шифр.

1.6 Атака на комбінувальний генератор гами з нерівномірним рухом на основі опробування індексів руху ЛРЗ

Розглянемо нетривіальний приклад перебірної атаки на комбінувальний генератор гами з нерівномірним рухом. Ця атака запропонована Е. Зеннером [Zen] і демонструє різноманіття ідей, які використовуються при розробці криптоаналітичних методів. Крім того,

зазначена атака надає змогу сформулювати низку необхідним умов стійкості комбінувальних генераторів гами з нерівномірним рухом.

Зауважимо, що використання нерівномірності руху ЛРЗ в конструкціях генераторів гами, як правило, підвищує їх стійкість відносно багатьох атак. Поряд з тим, широкий клас таких генераторів виявляється вразливим до атаки Зеннера, яка за певних умов має помітно меншу часову складність в порівнянні з повним перебором. При цьому умови застосовності зазначеної атаки допускають просту перевірку на практиці.

Як типовий приклад комбінувального генератора гами з нерівномірним рухом, до якого є застосовною атака Зеннера, розглянемо `A5/1`-подібний генератор, зображений на рис. 1.10.

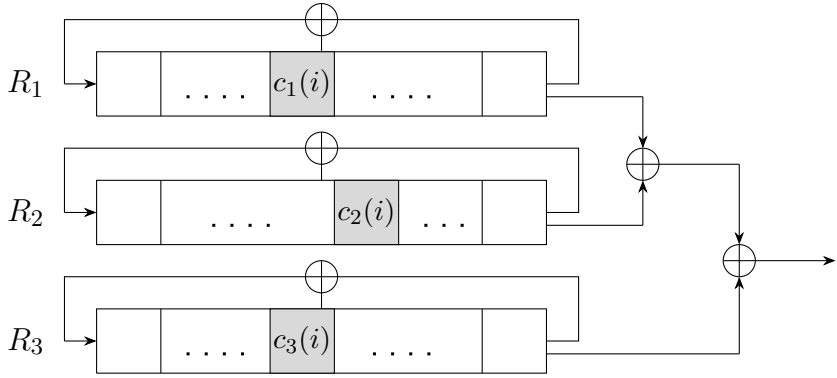

Рис. 1.10: Схема `A5/1`-подібного генератора гами з нерівномірним рухом

Цей генератор складається з таких компонент.

1. Трьох двійкових лінійних регістрів зсуву R_1, R_2, R_3 довжини n_1, n_2, n_3 відповідно (зауважимо, що для шифру `A5/1` $n_1 = 19$, $n_2 = 22$, $n_3 = 23$, а довжина початкового стану генератора становить $n = n_1 + n_2 + n_3 = 64$).

2. Лінійної комбінувальної функції, яка дорівнює сумі виходів усіх трьох ЛРЗ.

3. Закону зсуву регістрів, який являє собою елемент ускладнення та використовується для створення нерівномірності руху ЛРЗ.

Для генератора гами шифру `A5/1` цей закон визначається так, як описано у табл. 1.1. В кожному регістрі є певна *виділена* комірка, яка містить значення, що відповідає за величину зсуву регістрів (для R_1, R_2, R_3 це – комірки з номерами 8, 10, 10 відповідно; при цьому комірки нумеруються справа наліво, починаючи з 0). Позначимо $c_1(i)$, $c_2(i)$ та $c_3(i)$ значення, які зберігаються в i-ому такті у виділених комірках регістрів R_1, R_2 та R_3 відповідно, а $\varepsilon_1(i)$, $\varepsilon_2(i)$ та $\varepsilon_3(i)$ – величини зсувів регістрів R_1, R_2 та R_3 відповідно в цьому такті. Тоді $\varepsilon_1(i)$, $\varepsilon_2(i)$, $\varepsilon_3(i)$ є булевими функціями від змінних $c_1(i)$, $c_2(i)$, $c_3(i)$, вектори значень яких наведено в табл. 1.1, $i = 0, 1, 2, \ldots$.

Як видно з таблиці, закон руху ЛРЗ можна описати таким чином. Ті два регістри, виділені комірки яких містять в даному такті однакові значення, зсуваються на один крок. Якщо при цьому у виділеній комірці третього регістру зберігається інше значення, то він залишається на місці; в іншому випадку цей регістр також зсувається на один крок.

Функціонування генератора гами відбувається звичайним чином. Спочатку шляхом запису в кожен регістр певного двійкового вектора формується початковий стан генератора. Потім підсумовуються значення, що містяться в найменших за номером (найправіших на рис. 1.10) комірках регістрів, в результаті чого обчислюється знак гами. Далі регістри зсуваються відповідно до закону, зазначеного в табл. 1.1, генератор переходить в наступний стан, і процес гамоутворення продовжується.

Наведемо більш точний, формальний опис функціонування генератора гами, потрібний для викладення атаки Зеннера. Для цього

Табл. 1.1: Закон зсуву регістрів R_1, R_2, R_3

$c_1(i)$	$c_2(i)$	$c_3(i)$	$\varepsilon_1(i)$	$\varepsilon_2(i)$	$\varepsilon_3(i)$
0	0	0	1	1	1
0	0	1	1	1	0
0	1	0	1	0	0
0	1	1	0	1	1
1	0	0	0	1	1
1	0	1	1	0	1
1	1	0	1	1	0
1	1	1	1	1	1

введемо такі позначення (нижче змінні i та ν позначають номер такту та номер ЛРЗ і приймають значення $0, 1, \ldots$ та $1, 2, 3$ відповідно):

- $x_\nu(i)$ – двійковий вектор-рядок довжини n_ν, який дорівнює стану ЛРЗ R_ν в i-ому такті;
- γ_i – знак гами в i-ому такті;
- $e_{j,\nu}$ – двійковий вектор-стовпець довжини n_ν, всі координати якого, за виключенням j-ої, дорівнюють 0, $j \in \overline{0, n_\nu - 1}$;
- $h_\nu = e_{n_\nu - 1, \nu}$ – вектор-індикатор точки зйому знаків вихідної послідовності ЛРЗ R_ν;
- c_1, c_2, c_3 – номери виділених комірок ЛРЗ R_1, R_2, R_3 відповідно;
- $g_\nu = e_{n-1-c_\nu, \nu}$ – вектор-індикатор точки зйому керування рухом ЛРЗ R_ν;
- $C_\nu = C(f_\nu(x))$ – матриця, що задається поліномом зворотного зв'язку $f_\nu(x)$ ЛРЗ R_ν (див. формулу (1.3));

– $c(i) = (c_1(i), c_2(i), c_3(i))$ – вектор значень, які містяться в i-ому такті в комірках з номерами c_1, c_2, c_3 ЛРЗ R_1, R_2, R_3 відповідно;

– $\varepsilon(i) = (\varepsilon_1(i), \varepsilon_2(i), \varepsilon_3(i))$ – вектор, ν-та координата якого дорівнює величині зсуву ЛРЗ R_ν в i-ому такті;

– $\delta_\nu(i) = \sum\limits_{j=0}^{i-1} \varepsilon_\nu(j)$ – загальна величина зсуву ЛРЗ R_ν в перших i тактах; $\delta_\nu(0) = 0$.

За допомогою введених позначень процес функціонування генератора гами можна описати такою системою рівнянь:

$$\gamma_i = x_1(i)h_1 \oplus x_2(i)h_2 \oplus x_3(i)h_3,\ c_\nu(i) = x_\nu(i)g_\nu, \qquad (1.10)$$
$$x_\nu(i+1) = x_\nu(i)C_\nu^{\varepsilon_\nu(i)},\ \nu = 1,2,3,\ i = 0,1,\ldots,$$

де значення параметрів $\varepsilon_1(i), \varepsilon_2(i), \varepsilon_3(i)$ визначаються за вектором $c(i) = (c_1(i), c_2(i), c_3(i))$ згідно з табл. 1.1.

Назвемо *індексом руху лінійних регістрів зсуву* в i-му такті довільне можливе значення вектора $\varepsilon(i)$, $i = 0, 1, \ldots$. Помітимо, що, відповідно до табл. 1.1, індекс руху може приймати будь-яке з наступних чотирьох значень:

$$\begin{aligned}
&\varepsilon(i) = (1,1,1) \Leftrightarrow (c_1(i) \oplus c_2(i) = 0, c_1(i) \oplus c_3(i) = 0);\\
&\varepsilon(i) = (0,1,1) \Leftrightarrow (c_1(i) \oplus c_2(i) = 1, c_1(i) \oplus c_3(i) = 1);\\
&\varepsilon(i) = (1,0,1) \Leftrightarrow (c_1(i) \oplus c_2(i) = 1, c_1(i) \oplus c_3(i) = 0);\\
&\varepsilon(i) = (1,1,0) \Leftrightarrow (c_1(i) \oplus c_2(i) = 0, c_1(i) \oplus c_3(i) = 1).
\end{aligned} \qquad (1.11)$$

Перетворимо співвідношення (1.10). Для будь-яких $\nu = 1,2,3$, $i = 0, 1, \ldots$ покладемо

$$g_\nu(i) = C_\nu^{\delta_\nu(i)} g_\nu,\ h_\nu(i) = C_\nu^{\delta_\nu(i)} h_\nu. \tag{1.12}$$

На підставі рівності $x_\nu(i) = x_\nu(0) C_\nu^{\delta_\nu(i)}$ система рівнянь (1.10) може бути записана у вигляді

$$\gamma_i = x_1(0)h_1(i) \oplus x_2(0)h_2(i) \oplus x_3(0)h_3(i),\ c_\nu(i) = x_\nu(0)g_\nu(i),$$

$$\nu = 1, 2, 3,\ i = 0, 1, \ldots; \tag{1.13}$$

при цьому на підставі рівності $\delta_\nu(i) = \delta_\nu(i-1) + \varepsilon_\nu(i-1)$, $i = 1, 2, \ldots$ вектори $g_\nu(i)$, $h_\nu(i)$, які визначаються за формулами (1.12), задовольняють такі рекурентні співвідношення:

$$g_\nu(i) = C_\nu^{\varepsilon_\nu(i-1)} g_\nu(i-1),\ h_\nu(i) = C_\nu^{\varepsilon_\nu(i-1)} h_\nu(i-1),\ i = 1, 2, \ldots, \tag{1.14}$$

$$g_\nu(0) = g_\nu,\ h_\nu(0) = h_\nu,\ \nu = 1, 2, 3. \tag{1.15}$$

Отже, рівності (1.13), (1.14) разом зі співвідношеннями (1.11) утворюють систему рівнянь, яка пов'язує невідомий початковий стан $x(0)$ генератора гами з параметрами $\varepsilon(i)$ та знаками гами γ_i, $i = 0, 1, \ldots$.

Сутність атаки Зеннера полягає в розв'язанні отриманої системи рівнянь шляхом опробування індексів руху ЛРЗ генератора гами.

Виберемо певним чином натуральне число $t \leqslant n = n_1 + n_2 + n_3$. Тоді, фіксуючи у співвідношеннях (1.14) довільними допустимими значеннями параметри $\varepsilon(i-1)$, $i = 1, 2, \ldots, t$, на підставі рівностей (1.11), (1.13) отримаємо систему, яка складається з $3t$ лінійних рівнянь відносно n невідомих координат векторів $x_1(0), x_2(0), x_3(0)$. Таким чином, перебираючи індекси руху $\varepsilon(0), \varepsilon(1), \ldots, \varepsilon(t-1)$, отримаємо деяку множину систем лінійних рівнянь, перевірка сумісності яких та розв'язання (в ідеалі – єдиної) сумісної системи надає можливість відновити шуканий вектор $x(0)$.

Для наочності проілюструємо наведені міркування при $t = 2$. Цьому значенню t відповідають номери тактів $i = 0$ та $i = 1$. При $i = 0$ вектори $g_\nu(0)$ та $h_\nu(0)$, $\nu = 1, 2, 3$, є відомими (див. рівності (1.15)). Отже, перше лінійне рівняння має вигляд

$$\gamma_0 = x_1(0)h_1(0) \oplus x_2(0)h_2(0) \oplus x_3(0)h_3(0). \tag{1.16}$$

Присвоїмо довільне допустиме значення вектору $\varepsilon(0)$, наприклад, $\varepsilon(0) = (0, 1, 1)$. На підставі рівностей (1.11), (1.13) отримаємо два лінійних рівняння відносно невідомих координат векторів $x_1(0), x_2(0), x_3(0)$:

$$x_1(0)g_1(0) \oplus x_2(0)g_2(0) = 1, \quad x_1(0)g_1(0) \oplus x_3(0)g_3(0) = 1. \tag{1.17}$$

Таким чином, при $i = 0$ сформуємо систему, яка складається з трьох лінійних рівнянь (1.16), (1.17). Якщо ця система є сумісною, то перейдемо до наступного кроку, інакше – виберемо нове допустиме значення $\varepsilon(0)$.

У випадку сумісності системи рівнянь (1.16), (1.17) покладемо $i = 1$ та обчислимо вектори $g_\nu(1)$, $h_\nu(1)$, $\nu = 1, 2, 3$ за формулами (1.14). Отримаємо

$$g_1(1) = g_1(0), \quad g_2(1) = C_2 g_2(0), \quad g_3(1) = C_3 g_3(0),$$

$$h_1(1) = h_1(0), \quad h_2(1) = C_2 h_2(0), \quad h_3(1) = C_3 h_3(0). \tag{1.18}$$

Помітимо, що перша рівність (1.13) та співвідношення (1.18) надають змогу сформувати нове лінійне рівняння відносно координат векторів $x_1(0), x_2(0), x_3(0)$:

$$\gamma_1 = x_1(0)h_1(1) \oplus x_2(0)h_2(1) \oplus x_3(0)h_3(1). \tag{1.19}$$

Для побудови наступних двох рівнянь виберемо довільним чином допустиме значення $\varepsilon(1)$, наприклад, $\varepsilon(1) = (1,1,1)$. На підставі рівностей (1.11), (1.13) отримаємо

$$x_1(0)g_1(1) \oplus x_2(0)g_2(1) = 0, \quad x_1(0)g_1(1) \oplus x_3(0)g_3(1) = 0. \qquad (1.20)$$

Якщо система, яка складається з рівнянь (1.16), (1.17), (1.19), (1.20), є несумісною, то виберемо нове допустиме значення $\varepsilon(1)$ і повторимо описані вище обчислення. В протилежному випадку, використовуючи рівності (1.14), обчислимо вектори

$$g_1(2) = C_1 g_1(1), \quad g_2(2) = C_2 g_2(1), \quad g_3(2) = C_3 g_3(1),$$

$$h_1(2) = C_1 h_1(1), \quad h_2(2) = C_2 h_2(1), \quad h_3(2) = C_3 h_3(1)$$

та продовжимо подальше опробування індексів руху ЛРЗ в тактах з номерами $2, 3, \ldots$.

Зрозуміло, що наведений алгоритм побудови систем лінійних рівнянь полягає у послідовному переборі індексів руху ЛРЗ методом пошуку з поверненням. Опишемо зараз цей алгоритм більш докладно.

Нехай відомі знаки гами, які виробляються генератором в перших n тактах. Для відновлення початкового стану $x(0)$ генератора за відрізком $\gamma = \gamma_0, \gamma_1, \ldots, \gamma_{n-1}$ розглянемо позначене орієнтоване дерево $D = D(\gamma)$, вершини якого розташовані на n рівнях, занумерованих числами $0, 1, \ldots, n-1$ (рис. 1.11).

За означенням 0-й рівень містить єдину (кореневу) вершину дерева D, а з кожної вершини, що розташована на i-ому рівні, виходить точно 4 дуги, спрямовані у вершини $(i+1)$-го рівня. Вважається, що ці дуги позначені різними допустимими значеннями параметра $\varepsilon(i)$, тобто векторами $(1,1,1)$, $(1,1,0)$, $(1,0,1)$, $(0,0,1)$. Таким чи-

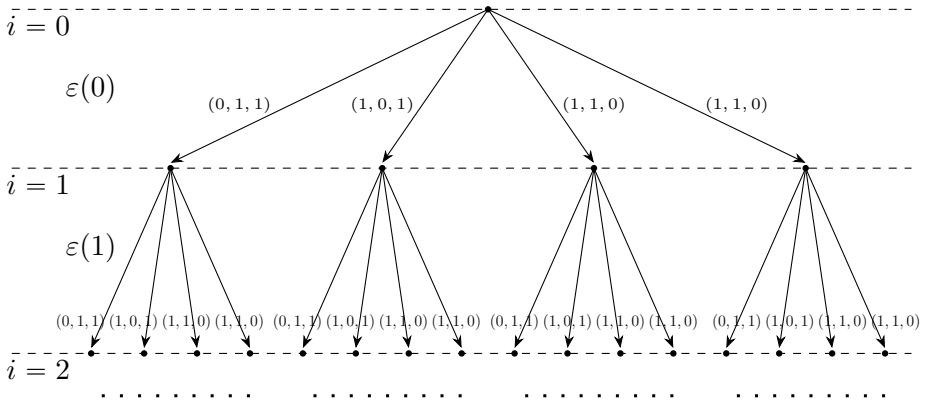

Рис. 1.11: Кореневе дерево для процедури перебору індексів руху

ном, загальна кількість вершин на i-ому рівні дерева становить 4^i, $i \in \overline{0, n-1}$.

Кожній вершині v, розташованій на рівні з номером $i \in \overline{1, n-1}$, відповідає система лінійних рівнянь $S(v)$, яка отримується в результаті фіксації у рівняннях (1.11), (1.13), (1.14) параметрів $\varepsilon(0), \varepsilon(1), \ldots, \varepsilon(i-1)$ значеннями, що дорівнюють позначкам над дугами єдиного шляху з кореня дерева D в задану вершину v. Кореневій вершині ставиться у відповідність система лінійних рівнянь, яка складається з єдиного рівняння (1.16).

Назвемо вершину v дерева D *дозволеною*, якщо система рівнянь $S(v)$ є сумісною, і *забороненою* – в протилежному випадку.

Алгоритм відновлення початкового стану генератора за відрізком гами довжини n полягає в послідовному обході дозволених вершин дерева D, починаючи з кореневої вершини, методом пошуку в глибину.

Спочатку всі вершини дерева D позначаються як непройдені. При першому потраплянні в поточну вершину v, розташовану на i-ому рівні ($i \in \overline{0, n-1}$), ця вершина позначається як пройдена. Далі фор-

мується система лінійних рівнянь $S(v)$ та (з використанням алгоритму Гауса) перевіряється її сумісність. Якщо система $S(v)$ сумісна, то вершина v позначається як дозволена. Далі здійснюється перехід в одну з чотирьох суміжних з нею вершин, розташованих на наступному, $(i+1)$-ому, рівні дерева D. Якщо система $S(v)$ є несумісною, то вершина v позначається як заборонена. Потім шукається (єдина) найближча до v пройдена дозволена вершина, серед «нащадків» якої містяться непройдені вершини, і здійснюється перехід в одну з цих вершин.

Алгоритм закінчує роботу, якщо знайдено дозволену вершину v_0, яка знаходиться на рівні з заданим номером N, близьким до числа $n-1$ (наприклад, $N = n-1$ або $N = n-2$), або після того, як пройдені всі дозволені вершини дерева D. В першому випадку множина розв'язків системи лінійних рівнянь $S(v_0)$ становить сукупність допустимих значень шуканого вектора $x(0)$.

Опишемо докладніше алгоритм побудови системи лінійних рівнянь $S(v)$, яка відповідає заданій вершині v, що знаходиться на i-ому рівні дерева D, $i \in \overline{0, n-1}$.

Як зазначено вище, при $i = 0$ система $S(v)$ складається з єдиного лінійного рівняння (1.16).

Нехай $i \geqslant 1$, u – «предок» вершини v, розташований на рівні з номером $i-1$, а $\varepsilon(i-1) = (a, b, c)$ є позначкою над дугою, яка спрямована з вершини u до вершини v. Припустимо, що система рівнянь $S(u)$, а також вектори $g_\nu(i-1)$, $h_\nu(i-1)$, $\nu = 1, 2, 3$, які відповідають вершині u, вже побудовані. За формулами (1.14) обчислимо вектори

$$g_1(i) = C_1^a g_1(i-1), \quad g_2(i) = C_2^b g_2(i-1), \quad g_3(i) = C_3^c g_3(i-1), \tag{1.21}$$

$$h_1(i) = C_1^a h_1(i-1), \quad h_2(i) = C_2^b h_2(i-1), \quad h_3(i) = C_3^c h_3(i-1). \tag{1.22}$$

Далі, підставляючи вирази (1.22) в першу рівність (1.13), отримаємо одне лінійне рівняння відносно невідомого вектора $x(0)$. Ще два

рівняння отримуються безпосередньо зі співвідношень (1.11), другої рівності (1.13) (з заміною в них i на $i-1$ та умови $\varepsilon(i-1)=(a,b,c)$). Приєднуючи три зазначених рівняння до системи $S(u)$, побудуємо шукану систему лінійних рівнянь $S(v)$, яка відповідає вершині v.

Оцінимо трудомісткість T описаного алгоритму.

Помітимо, що значення T прямо пропорційно числу вершин дерева D, відмінних від кореня, які пройдені до потрапляння у першу дозволену вершину v_0, розташовану на рівні з заданим номером N. Оскільки кожна пройдена вершина на рівні з номером $i>0$ є «нащадком» єдиної дозволеної вершини на рівні з номером $i-1$, а число всіх «нащадків» останньої дорівнює 4, то загальна кількість пройдених вершин, відмінних від кореня, не перевищує $4r$, де r – число всіх дозволених вершин дерева D.

Далі, при проходженні кожної вершини v потрібно скласти систему лінійних рівнянь $S(v)$ від n невідомих і перевірити її сумісність. Оскільки двійкова часова складність перевірки сумісності однієї такої системи рівнянь методом Гауса дорівнює $O(n^3)$, то загальна трудомісткість T описаного вище алгоритму становить

$$T=O\left(n^3r\right) \tag{1.23}$$

двійкових операцій.

Для отримання верхньої оцінки параметра r скористаємося такими міркуваннями.

Нехай v – довільна дозволена вершина, розташована на рівні з номером $i\in\overline{1,n-1}$, $a(0),a(1),\ldots,a(i-1)$ – послідовність позначок над дугами (єдиного) шляху з кореня дерева D до вершини v. Помітимо, що відповідно до описаного алгоритму побудови системи рівнянь $S(v)$ її розв'язками є ті й тільки ті початкові стани $x(0)$ генератора, для яких відрізки послідовностей індексів руху ЛРЗ та знаків гами в перших i та $i+1$ тактах дорівнюють

$\varepsilon(0) = a(0), \varepsilon(1) = a(1), \ldots, \varepsilon(i-1) = a(i-1)$ та $\gamma_0, \gamma_1, \ldots, \gamma_i$ відповідно. Оскільки послідовність індексів руху ЛРЗ однозначно визначається початковим станом генератора, то звідси випливає, що множини розв'язків систем рівнянь $S(v_1)$ та $S(v_2)$, які відповідають будь-яким різним вершинам v_1 та v_2, що знаходяться на тому самому рівні дерева D, не перетинаються. Зокрема, кількість r_i дозволених вершин на рівні з номером $i \in \overline{0, n-1}$ не перевищує кількості початкових станів генератора, кожному з яких відповідає фіксований відрізок гами $\gamma_0, \gamma_1, \ldots, \gamma_i$.

Зробимо зараз таке *евристичне припущення стосовно генератора гами*: для будь-якого $i \in \overline{0, n-1}$ кількість різних початкових станів, яким відповідає довільний фіксований відрізок гами довжини $i+1$, дорівнює приблизно 2^{n-i-1}. Інакше кажучи, для кожного $i \in \overline{0, n-1}$ генератор реалізує «приблизно збалансоване» відображення множини V_n початкових станів у множину V_{i+1} можливих відрізків гами довжини $i+1$. (Зауважимо, що справедливість цього припущення підтверджено експериментально в [Zen] для певної мініверсії генератора гами шифру `A5/1`).

Отже, на підставі зробленого припущення кількість початкових станів генератора гами, кожному з яких відповідає фіксований відрізок гами $\gamma_0, \gamma_1, \ldots, \gamma_i$, дорівнює 2^{n-i-1}. Звідси випливає, що кількість r_i дозволених вершин на i-ому рівні дерева D не перевищує 2^{n-i-1}:

$$r_i \leqslant 2^{n-i-1}, \ i \in \overline{0, n-1}. \tag{1.24}$$

З іншого боку зрозуміло, що r_i не перевищує загальної кількості вершин, розташованих на i-ому рівні, тобто

$$r_i \leqslant 4^i, \ i \in \overline{0, n-1}. \tag{1.25}$$

На підставі рівностей (1.24), (1.25) кількість r всіх дозволених вершин дерева D можна оцінити таким чином:

$$r = \sum_{i=0}^{n-1} r_i \leqslant \sum_{i=0}^{\left[\frac{n}{3}\right]} 4^i + \sum_{i=\left[\frac{n}{3}\right]+1}^{n-1} 2^{n-i-1} = \frac{1}{3}\left(4^{\left[\frac{n}{3}\right]+1} - 1\right) + \sum_{i=0}^{n-\left[\frac{n}{3}\right]-2} 2^i =$$

$$= \frac{1}{3}\left(4^{\left[\frac{n}{3}\right]+1} - 1\right) + \left(2^{n-\left[\frac{n}{3}\right]-1} - 1\right) \leqslant \frac{4}{3} \cdot 2^{\frac{2n}{3}} + 2^{\frac{2n}{3}} = \frac{7}{3} \cdot 2^{\frac{2n}{3}}. \quad (1.26)$$

Отже, на підставі співвідношень (1.23), (1.26) трудомісткість наведеного алгоритму відновлення початкового стану генератора гами становить

$$T = O\left(2^{\frac{2n}{3}} n^3\right) \quad (1.27)$$

двійкових операцій, в той час як трудомісткість повного перебору всіх початкових станів дорівнює $O(2^n)$.

Формула (1.27) надає оцінку трудомісткості атаки Зеннера на `A5/1`-подібний генератор гами, показаний на рис. 1.10. Поряд з тим, зазначена атака є застосовною і до інших комбінувальних генераторів гами з нерівномірним рухом.

Умови її застосовності є такими.

1. Функція виходів генератора залежить лінійно під його початкового стану.

2. Закон руху ЛРЗ генератора можна описати за допомогою лінійних рівнянь (на кшталт (1.11)), які пов'язують значення, що зберігаються у виділених комірках ЛРЗ (які керують рухом), з величинами зсувів регістрів у кожному такті.

3. Число k можливих значень зсувів регістрів є помітно менше за 2^l, де l – загальна кількість ЛРЗ.

В [Zen] показано, що за наведених умов на генератор можна побудувати атаку, аналогічну описаній вище, трудомісткість якої дорівнює

$$O\left(2^{n \cdot \left(\frac{\log k}{1+\log k}\right)} n^3\right)$$

двійкових операцій, де n – довжина початкового стану генератора гами. (Зауважимо, що для генератора на рис. 1.10 $k = 4$, що приводить до отриманої вище формули (1.27)).

На завершення сформулюємо наслідки, які випливають з аналізу наведеної атаки.

1. Комбінувальна функція генератора гами повинна бути нелінійною.

2. Число k, яке дорівнює кількості можливих значень зсувів ЛРЗ, має бути якомога більшим. Якщо генератор складається з l ЛРЗ, то k має дорівнювати числу 2^l. Більше того, відображення $(c_1(i), \ldots, c_l(i)) \mapsto (\varepsilon_1(i), \ldots, \varepsilon_l(i))$ наборів значень, що зберігаються у виділених комірках ЛРЗ, в набори значень зсувів цих ЛРЗ в i-му такті має бути підстановкою на множині V_l.

3. Зазначена підстановка повинна мати високу нелінійність, що гарантує відсутність для неї високоймовірних лінійних наближень (як приклад, відзначимо підстановку (s-блок), яка використовується в алгоритмі шифрування `AES`).

Зауважимо також, що при побудові генераторів гами з нерівномірним рухом слід уникати простоювань лінійних регістрів зсуву. Це пояснюється таким чином: якщо певний регістр простоює в деякому такті, то знаки гами, які залежать від виходу цього регістру в даному та наступному тактах, можуть бути сильно корельованими. Це надає змогу будувати на генератор кореляційні атаки. Отже, доцільно вибирати величини зсувів регістрів таким чином, щоб вони не простоювали, а рухалися. Досягти цього можна, наприклад, замінюючи величини зсувів 0 і 1, на 1 і 2 відповідно.

Задачі до розділу 1

Задача 1.1. Побудуйте автомат з алфавітами $X = \{0,1\}^2$, $S = Y = \{0,1\}$, який для будь-якого натурального n перетворює вхідну послідовність (x, y), де $x = (x_0, \ldots, x_{n-1})$, $y = (y_0, \ldots, y_{n-1})$, у вихідну послідовність $(x + y) \bmod 2^n$.

Задача 1.2. Побудуйте граф скінченного автомата та визначіть, чи є цей автомат оборотним за Гаффманом, якщо

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

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 всіх $s \in S$, $x \in X$, окрім $f(3,1) = 1$.

Задача 1.3. Нехай функція виходів f автомата A задовольняє таку умову: для будь-яких $s \in S$, $y \in Y$ існує єдиний елемент $x \in X$ з властивістю $f(s,x) = y$. Чи є такий автомат оборотним за Гаффманом? Чи виконується обернене твердження?

Задача 1.4. Нехай $A = (X, S, Y, h, f)$, де $X = S = Y = \{0,1\}$, $h(s,x) = x$, $f(s,x) = s \cdot x$. Позначимо $\Phi(k)$ число розв'язків системи рівнянь (1.1) при $y_0 = \ldots = y_{k-1} = 0$.

1. Доведіть, що при $k \geqslant 3$ функція $\Phi(k)$ задовольняє співвідношення $\Phi(k) = \Phi(k-1) + \Phi(k-2)$.

2. Обчисліть значення $\Phi(1)$ та $\Phi(2)$.

3. Знайдіть аналітичний вигляд функції $\Phi(k)$ та її границю при $k \to \infty$.

Задача 1.5. Нехай $A = (X, S, Y, h, f)$, $\xi_k(s_0, \overline{x}) = \eta_k(F_k(s_0, \overline{x}))$, де величини F_k та η_k визначаються за формулами з п. 1.2. Позначимо S_k усереднене значення величини ξ_k за всіма $(s_0, \overline{x}) \in S \times X$.

Доведіть, що

$$S_k = \frac{1}{|S||X|^k} \sum_{\overline{y} \in Y^k} \eta_k^2(\overline{y}).$$

Задача 1.6. Нехай Γ – генератор гами з множиною станів V_n та вихідним алфавітом V_2, 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 послідовності довжини L із середньою ймовірністю помилки p_e, використовуючи T двійкових операцій, якщо

а) $\Gamma_{N+1} : s_0 \mapsto (s_0, \widetilde{s}_0)$, де $\widetilde{s}_0$ – сума за модулем 2 координат вектора s_0, $p_e = 1/4$, $T = N$;

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

Задача 1.7. Нехай $T > 0$, $1/4 < \varepsilon < 1/2$. Генератор гами Γ називається (T, ε)-*непередбачуваним* (в сенсі наступного знаку), якщо для кожного $i \in \overline{2, L}$ виконується така умова: будь-який ймовірнісний алгоритм B відновлення i-го знаку за попередніми, який характеризується ймовірністю помилки

$$\Pr(B(y_1, y_2, \ldots, y_{i-1}) \neq y_i) \leqslant 2\varepsilon - 1/2,$$

де $(y_1, \ldots, y_L) = \Gamma_L(s_0)$, виконує принаймні T умовних операцій (ймовірність обчислюється відносно випадкового рівноймовірного вибору початкового стану s_0 та випадкових даних, які використовує алгоритм B).

Доведіть, що з (T, ε)-псевдовипадковості генератора гами випливає його (T, ε)-непередбачуваність.

Задача 1.8. Розглянемо генератор гами Г, який з початкового стану переходить у наступний стан, а далі звичайним чином виробляє гаму. Відновіть початковий стан генератора за відрізком гами γ, якщо:

а) Г є фільтрувальним генератором гами, 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. 1.12, зліва), а відрізок гами γ дорівнює $0, 1, 1$;

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

в) Г 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. 1.12, справа), а відрізок гами γ дорівнює $1, 0, 1$.

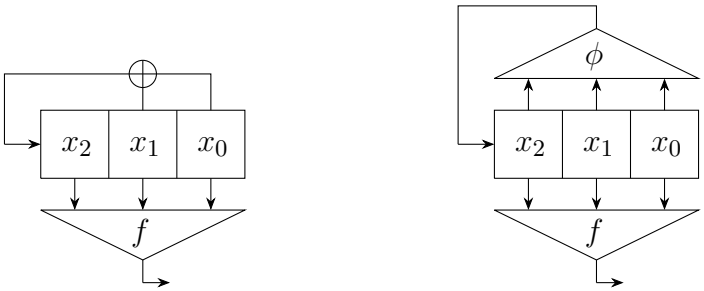

Рис. 1.12: Схеми генераторів гами до пунктів а), в) задачі 1.8

Задача 1.9. 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. 1.13). 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 співпадають, то обидва регістри зсуваються, інакше зсувається лише перший регістр. Відомо, що вихідною послідовністю генератора є $\gamma = 1, 1, 1, 1$.

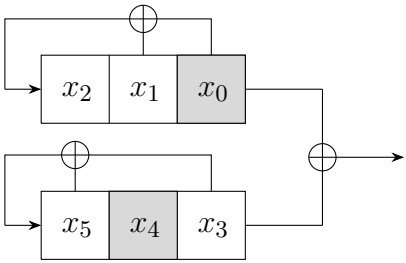

Рис. 1.13: Схема генератора гами до задачі 1.9

1. За відрізком гами γ побудуйте дерево $D = D(\gamma)$. Для кожної вершини v дерева D складіть відповідну систему лінійних рівнянь $S(v)$.

2. Розв'яжіть системи лінійних рівнянь, що відповідають значенням індексів руху $\varepsilon(0) = (1, 1)$, $\varepsilon(1) = (1, 1)$, $\varepsilon(2) = (1, 0)$ та $\varepsilon(0) = (1, 1)$, $\varepsilon(1) = (1, 0)$, $\varepsilon(2) = (1, 1)$.

2 Елементи алгебраїчного криптоаналізу

Даний розділ присвячено вивченню основних понять і результатів, що використовуються при побудови алгебраїчних атак на потокові шифри. Центральним з них є поняття базису Грьобнера ідеалу кільця булевих функцій.

Практично одразу з появою у 2001 – 2003 рр. найперших (із сучасних) алгебраїчних атак з'ясувалося, що базиси Грьобнера є потужним інструментом для розв'язання систем нелінійних булевих рівнянь, а, отже, для побудови алгебраїчних атак на потокові (а також блокові) шифри та деякі асиметричні криптоситеми. У багатьох випадках знання мінімального базису Грьобнера ідеалу, якій відповідає системі рівнянь, надає змогу отримати розв'язок цієї системи. Більш того, будь-який метод розв'язання такої системи рівнянь є одночасно методом обчислення відповідного базису Грьобнера (див. нижче п. 2.7).

Іншим важливим поняттям, що використовується для аналізу стійкості потокових шифрів, є алгебраїчна імунність (векторної) булевої функції, для обчислення якої також можна використовувати базиси Грьобнера (див. пп. 2.8, 2.9).

У завершальному пункті розділу, з метою продемонструвати на нетривіальному прикладі як використовуються деякі з наведених понять і результатів, розглянуто алгебраїчну атаку на спрощену версію SNOW 2.0-подібного потокового шифру.

2.1 Ідеали кільця булевих функцій

Для будь-якого натурального n позначимо V_n множину двійкових векторів довжини n, B_n – множину булевих функцій від n змінних. Множина B_n є комутативним кільцем відносно звичайних операцій додавання та множення булевих функцій:

$$\forall f, g \in B_n : (f \oplus g)(x) = f(x) \oplus g(x), \quad (fg)(x) = f(x)g(x),\ x \in V_n.$$

Нагадаємо, що множина $I \subseteq B_n$ називається *ідеалом* кільця B_n, якщо виконується умова:

$$\forall f \in B_n\ \forall g_1, g_2 \in I : g_1 \oplus g_2 \in I, fg_1 \in I.$$

Запис $I \lhd B_n$ означає, що I є ідеалом кільця B_n. Ідеал, породжений множиною $\{g_1, \ldots, g_m\} \subseteq B_n$, визначається за формулою

$$\langle g_1, \ldots, g_m \rangle = \{f_1 g_1 \oplus \ldots \oplus f_m g_m : f_1, \ldots, f_m \in B_n\}.$$

Для будь-яких $I \lhd B_n$, $M \subseteq V_n$ покладемо

$$V(I) = \{x \in V_n |\ \forall g \in I : g(x) = 0\}, \tag{2.1}$$

$$J(M) = \{g \in B_n |\ \forall x \in M : g(x) = 0\}. \tag{2.2}$$

Множина (2.1) називається *алгебраїчним многовидом* або *множиною нулів* ідеалу I. Множина (2.2) є ідеалом, що складається з усіх булевих функцій, які обертаються в нуль на M.

Основні властивості ідеалів кільця B_n містить таке твердження.

Твердження 2.1. *Для будь-яких $I \lhd B_n$, $M \subseteq V_n$ мають місце рівності*

$$J(V(I)) = I, \quad V(J(M)) = M.$$

Зокрема, існує взаємно однозначна відповідність між ідеалами кільця B_n та підмножинами множини V_n (так, що кожен ідеал однозначно визначається множиною його нулів). Крім того, кожен ідеал $I \lhd B_n$ породжується єдиною булевою функцією χ_I, яка визначається за формулою

$$\chi_I(x) = \begin{cases} 0, & \text{якщо } x \in V(I); \\ 1, & \text{якщо } x \notin V(I),\ x \in V_n. \end{cases} \tag{2.3}$$

Доведення. Перш за все, переконаємося у справедливості рівності $I = \langle \chi_I \rangle$. Якщо $I = \langle 0 \rangle$, то ця рівність є очевидною.

Нехай $I \neq \langle 0 \rangle$ та $x \notin V(I)$. Тоді існує функція $f \in I$ така, що $f(x) = 1$. Має місце рівність

$$f = \bigoplus_{y \in V_n : f(y) = 1} \delta_y,$$

де функція δ_y, $y \in V_n$, визначається за правилом: $\delta_y(z) = 1 \Leftrightarrow z = y$, $z \in V_n$. Оскільки $I \lhd B_n$, $f \in I$, то $\delta_x f = \bigoplus_{y \in V_n : f(y) = 1} \delta_x \delta_y = \delta_x \in I$.

Отже, для будь-якого $x \notin V(I)$ виконується співвідношення $\delta_x \in I$, звідки випливає, що $\chi_I = \bigoplus_{x \notin V(I)} \delta_x \in I$ та, як наслідок, $\langle \chi_I \rangle \subseteq I$. Крім того, для будь-якої функції $f \in I$ справедлива рівність $f = f\chi_I$, з якої випливає, що $I \subseteq \langle \chi_I \rangle$. Таким чином, $I = \langle \chi_I \rangle$, що й треба було довести.

Далі, на підставі формул (2.1), (2.2) для будь-якого $I \lhd B_n$ виконується включення $I \subseteq J(V(I))$. Крім того, якщо $f \in J(V(I))$, то $f(x) = 0$ для будь-якого $x \in V(I)$ і, отже, $f = f\chi_I$. Але згідно з доведеним вище, $\chi_I \in I$. Отже, $f \in I$ та, як наслідок, $J(V(I)) \subseteq I$. Таким чином, справедлива рівність $J(V(I)) = I$.

Нарешті, рівність $V(J(M)) = M$ випливає з доведеної рівності $J(V(I)) = I$ при $I = J(M)$ та формул (2.1), (2.2).

□

Як приклад застосування твердження 2.1, розглянемо систему

$$f_i(x_1, \ldots, x_n) = 0,\ i = 1, 2, \ldots, m, \tag{2.4}$$

яка складається з m булевих рівнянь відносно булевих невідомих $x_1, \ldots, x_n$. Нехай $I = \langle f_1, \ldots, f_m \rangle$ – ідеал, породжений множиною функцій $\{f_1, \ldots, f_m\}$. Тоді I складається з усіх функцій $g \in B_n$, для кожної з яких рівняння $g(x_1, \ldots, x_n) = 0$ є наслідком системи (2.4), а множина розв'язків цієї системи дорівнює $V(I)$. Далі, зазначена система рівносильна одному рівнянню $\chi_I(x_1, \ldots, x_n) = 0$, де функція χ_I визначається за формулою (2.3). Отже, $I = \{f\chi_I |\ f \in B_n\}$.

Нехай I – довільний ідеал кільця B_n. Тоді множина

$$\mathrm{Ann}\,(I) = \{f \in B_n |\ \forall g \in I : fg = 0\}$$

також є ідеалом, який називається *анулятором* ідеалу I. Анулятор функції $f \in B_n$ визначається як анулятор ідеалу, що породжується цією функцією: $\mathrm{Ann}\,(f) = \mathrm{Ann}\,(\langle f \rangle)$.

Твердження 2.2. *Для будь-якого $I \lhd B_n$ кільце B_n розкладається в пряму суму ідеалів I та $\mathrm{Ann}\,(I)$. Іншими словами, кожна функція f допускає однозначне представлення у вигляді $f = g \oplus g^{\perp}$, де $g \in I$, $g^{\perp} \in \mathrm{Ann}\,(I)$. Крім того, якщо $I = \langle g_0 \rangle$, то $\mathrm{Ann}\,(I) = \langle g_0 \oplus 1 \rangle$.*

Доведення. Нехай $I = \langle g_0 \rangle$. Тоді для будь-якої функції $f \in B_n$ справедлива рівність $f = fg_0 \oplus f(g_0 \oplus 1)$, причому $fg_0 \in I$, $f(g_0 \oplus 1) \in \mathrm{Ann}\,(I)$. Зокрема, $\langle g_0 \oplus 1 \rangle \subseteq \mathrm{Ann}\,(I)$.

Далі, якщо $h \in \mathrm{Ann}\,(I)$, то $hg_0 = 0$, і, отже, $h = h(g_0 \oplus 1)$, звідки випливає, що $\mathrm{Ann}\,(I) \subseteq \langle g_0 \oplus 1 \rangle$. Таким чином, $\mathrm{Ann}\,(I) = \langle g_0 \oplus 1 \rangle$, і на

підставі твердження 2.1 (а саме, рівності $I = \langle \chi_I \rangle$) для завершення доведення залишається переконатися в тому, що для кожної функції $f \in B_n$ існує тільки одне представлення у вигляді $f = g \oplus g^{\perp}$ таке, що $g \in I$, $g^{\perp} \in \mathrm{Ann}\,(I)$. Але це випливає з рівності $I \cap \mathrm{Ann}\,(I) = \{0\}$. □

На завершення цього пункту відзначимо зв'язок між ідеалами кільця B_n та блоковими кодами. Помітимо, що кожен ідеал $I \lhd B_n$ є підпростором векторного простору всіх булевих функцій від n змінних і, отже, являє собою лінійний блоковий код довжини 2^n над полем з двох елементів. Словами цього коду є вектори значень функцій, які належать ідеалу I:

$$I = \{(g(x) : x \in V_n) : g \in I\}. \tag{2.5}$$

Запишемо слова коду (2.5) один під одним у вигляді таблиці розміром $2^k \times 2^n$, де $k = \dim(I)$ позначає вимірність ідеалу I (рис. 2.1). Зрозуміло, що множина $V(I)$ співпадає з сукупністю номерів усіх нульових стовпців цієї таблиці.

Далі, всі 2^k векторів $(g(x) : x \in V_n \backslash V(I))$, де $g \in I$, є попарно різними і, оскільки їхня довжина дорівнює $|V_n \backslash V(I)|$, то $k \leqslant |V_n \backslash V(I)|$. З іншого боку, згідно з твердженням 2.1, будь-яка функція $g \in B_n$, що обертається в нуль на множині $V(I)$, належить коду I. Отже, $2^{|V_n \backslash V(I)|} \leqslant |I|$, тобто $|V_n \backslash V(I)| \leqslant k$.

Таким чином, справедливе наступне твердження, яке встановлює взаємозв'язок між вимірністю ідеалу та кількістю його нулів.

Твердження 2.3. *Для будь-якого $I \lhd B_n$ справедлива рівність*

$$|V(I)| = 2^n - \dim(I).$$

Звідси випливає такий варіант відомої теореми Гільберта про нулі.

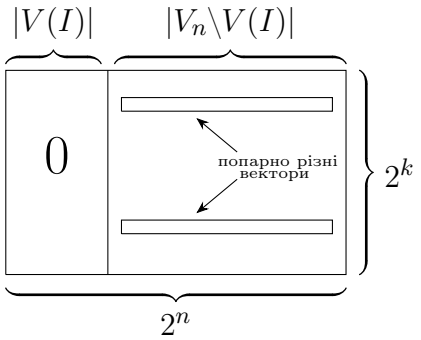

Рис. 2.1: Вигляд таблиці, що складається зі слів коду I

Наслідок 2.1. *Система рівнянь (2.4):*

1) є несумісною тоді й тільки тоді, коли $\langle f_1, \ldots, f_m \rangle = B_n$*;*

2) має єдиний розв'язок $(a_1, \ldots, a_n) \in V_n$ *тоді й тільки тоді, коли* $\langle f_1, \ldots, f_m \rangle = \langle x_1 \oplus a_1, \ldots, x_n \oplus a_n \rangle$*.*

2.2 Мономіальні впорядкування

Нагадаємо, що *відношенням часткового порядку* або *частковим впорядкуванням* на довільній множині A називається бінарне відношення $R \subseteq A^2$, яке задовольняє умови

1) $\forall \alpha \in A : \alpha R \alpha$ (рефлексивність);

2) $\forall \alpha, \beta \in A : (\alpha R \beta,\ \beta R \alpha) \Rightarrow \alpha = \beta$ (антисиметричність);

3) $\forall \alpha, \beta, \gamma : (\alpha R \beta,\ \beta R \gamma) \Rightarrow \alpha R \gamma$ (транзитивність).

Якщо виконується умова $\forall \alpha, \beta \in A : (\alpha R \beta$ або $\beta R \alpha)$, то часткове впорядкування R називається *відношенням лінійного порядку* або *лінійним впорядкуванням* на множині A.

Позначимо $\mathbb{N}_0^n$ множину векторів довжини n з невід'ємними цілими координатами. Ця множина є напівгрупою відносно операції $+$ покоординатного додавання векторів.

Відношення часткового порядку $\leqslant$ на множині $\mathbb{N}_0^n$ визначається за формулою:

$$\forall \alpha = (\alpha_1, \ldots, \alpha_n), \beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}_0^n : \alpha \leqslant \beta \Leftrightarrow (\alpha_i \leqslant \beta_i, i \in \overline{1, n}).$$

Означення 2.1. Довільне відношення лінійного порядку $\preceq$ на множині $\mathbb{N}_0^n$ називається *мономіальним впорядкуванням*, якщо виконуються умови

а) $\forall \alpha, \beta \in \mathbb{N}_0^n : \alpha \leqslant \beta \Rightarrow \alpha \preceq \beta$;

б) $\forall \alpha, \beta, \gamma \in \mathbb{N}_0^n : \alpha \preceq \beta \Rightarrow \alpha + \gamma \preceq \beta + \gamma$.

В подальшому запис $\alpha \prec \beta$ ($\alpha < \beta$) означає, що $\alpha \preceq \beta$ ($\alpha \leqslant \beta$) та $\alpha \neq \beta$. Число $|\alpha| = \alpha_1 + \ldots + \alpha_n$ називається *мультистепенем* вектора $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$.

Мономіальне впорядкування $\preceq$ називається *степеневим* або *градуйованим*, якщо для будь-яких $\alpha, \beta \in \mathbb{N}_0^n$ виконується умова $|\alpha| < |\beta| \Rightarrow \alpha \prec \beta$.

Приклад 2.1. Відношення *лексикографічного порядку* на множині $\mathbb{N}_0^n$ визначається за правилом $\alpha \preceq_{\text{lex}} \beta \Leftrightarrow (\alpha \prec_{\text{lex}} \beta$ або $\alpha = \beta)$, де

$$\alpha \prec_{\text{lex}} \beta \Leftrightarrow (\exists i \in \overline{1, n} : \alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1}, \alpha_i < \beta_i),$$

і є мономіальним впорядкуванням на $\mathbb{N}_0^n$.

Відношення *степеневого зворотного лексикографічного порядку* (degree reverse lexicographic order) визначається за правилом $\alpha \preceq_{\text{drl}} \beta \Leftrightarrow (\alpha \prec_{\text{drl}} \beta$ або $\alpha = \beta)$, де для будь-яких $\alpha = (\alpha_1, \ldots, \alpha_n)$,

$\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}_0^n$:

$$\alpha \prec_{\text{drl}} \beta \Leftrightarrow (|\alpha| < |\beta| \text{ або } (|\alpha| = |\beta| \text{ та } (\beta_n, \ldots, \beta_1) \prec_{\text{lex}} (\alpha_n, \ldots, \alpha_1)).$$

Це відношення є степеневим мономіальним впорядкуванням на множині $\mathbb{N}_0^n$.

Приклад 2.2. Нехай $n = 3$; тоді

$$(0,0,0) \prec_{\text{lex}} (0,0,1) \prec_{\text{lex}} (0,1,0) \prec_{\text{lex}} (0,1,1) \prec_{\text{lex}}$$
$$\prec_{\text{lex}} (1,0,0) \prec_{\text{lex}} (1,0,1) \prec_{\text{lex}} (1,1,0) \prec_{\text{lex}} (1,1,1).$$

Отже,

$$(0,0,0) \prec_{\text{drl}} (1,0,0) \prec_{\text{drl}} (0,1,0) \prec_{\text{drl}} (0,0,1) \prec_{\text{drl}}$$
$$\prec_{\text{drl}} (1,1,0) \prec_{\text{drl}} (1,0,1) \prec_{\text{drl}} (0,1,1) \prec_{\text{drl}} (1,1,1).$$

Надалі будемо ототожнювати довільну ненульову булеву функцію $f \in B_n$ з її поліномом Жегалкіна $f(x) = \bigoplus\limits_{\alpha \in V_n} c_{\alpha,f} x^\alpha$, де $x^\alpha = x_1^{\alpha_1} \ldots x_n^{\alpha_n}$, $c_{\alpha,f} \in \{0,1\}$, $\alpha = (\alpha_1, \ldots, \alpha_n) \in V_n$. При цьому казатимемо, що моном x^α *міститься у виразі* полінома $f(x)$ (або *входить до виразу* цього полінома), якщо $c_{\alpha,f} = 1$.

Будь-яке мономіальне впорядкування $\preceq$ дозволяє лінійно впорядкувати булеві мономи за правилом: $x^\alpha \preceq x^\beta \Leftrightarrow \alpha \preceq \beta$, $\alpha, \beta \in V_n$ (тут і далі множина двійкових векторів V_n розглядається як підмножина напівгрупи $\mathbb{N}_0^n$). Говорять, що моном x^β *старше* монома x^α (а моном x^α *молодше* монома x^β), якщо виконується умова $\alpha \prec \beta$. Говорять також, що моном x^α *ділить* моном x^β (а x^β *ділиться* на x^α або є *кратним* x^α), якщо $\alpha \leqslant \beta$. На підставі умови а) означення 2.1 кожен моном, кратний x^α, є старше або дорівнює x^α.

Впорядкування $\preceq$ на множині мономів дозволяє визначити *старший моном* (або *старший член*) будь-якої ненульової булевої фун-

кції $f(x) = \bigoplus\limits_{\alpha \in V_n} c_{\alpha,f} x^\alpha$:

$$\mathrm{LM}_{\preceq}(f) = \max\nolimits_{\preceq}\{x^\alpha : c_{\alpha,f} = 1\}.$$

Приклад 2.3. Нехай $f(x_1, x_2, x_3) = x_2x_3 \oplus x_1 \oplus x_2 \oplus x_3$; тоді $\mathrm{LM}_{\preceq_{\mathrm{lex}}}(f) = x_1$; $\mathrm{LM}_{\preceq_{\mathrm{drl}}}(f) = x_2x_3$.

Доведемо два допоміжних твердження про старші мономи суми та добутку булевих функцій.

Лема 2.1. *Нехай* $f_1, \ldots, f_m \in B_n \backslash \{0\}$, $f = f_1 \oplus \ldots \oplus f_m$. *Тоді*

а) якщо $f \neq 0$, *то* $\mathrm{LM}_{\preceq}(f) \preceq \max\nolimits_{\preceq}\{\mathrm{LM}_{\preceq}(f_i) : i \in \overline{1,m}\}$;

б) якщо $\mathrm{LM}_{\preceq}(f_i) \neq \mathrm{LM}_{\preceq}(f_j)$ *для усіх різних* $i, j \in \overline{1,m}$, *то* $f \neq 0$ *і*

$$\mathrm{LM}_{\preceq}(f) = \max\nolimits_{\preceq}\{\mathrm{LM}_{\preceq}(f_i) : i \in \overline{1,m}\}.$$

Доведення. Нехай $x^\alpha \succ \max\nolimits_{\preceq}\{\mathrm{LM}_{\preceq}(f_i) : i \in \overline{1,m}\}$. Тоді моном x^α старше кожного монома, який входить до виразу будь-якого з поліномів f_i, $i \in \overline{1,m}$. Отже, моном x^α старше кожного монома, який міститься в сумі $f_1 \oplus \ldots \oplus f_m$, тобто, $x^\alpha \succ \mathrm{LM}_{\preceq}(f_1 \oplus \ldots \oplus f_m)$. Звідси випливає справедливість першого твердження леми.

Далі, якщо старші члени поліномів f_i, $i \in \overline{1,m}$, є попарно різними, то моном $\max\nolimits_{\preceq}\{\mathrm{LM}_{\preceq}(f_i) : i \in \overline{1,m}\}$ входить у вираз суми $f_1 \oplus \ldots \oplus f_m$, звідки випливає друге твердження леми. □

Для того, щоб сформулювати наступну лему, введемо допоміжне означення.

Означення 2.2. Булеві вектори $\alpha = (\alpha_1, \ldots, \alpha_n)$ та $\beta = (\beta_1, \ldots, \beta_n)$ називаються *дизʼюнктними*, якщо виконується рівність $(\alpha_1\beta_1, \ldots, \alpha_n\beta_n) = (0, \ldots, 0)$.

Мономи x^α та x^β, де $\alpha, \beta \in V_n$, називаються *диз'юнктними*, якщо вектори α і β є диз'юнктними.

Запис $\alpha \perp \beta$ (відповідно $x^\alpha \perp x^\beta$) означає, що вектори α і β (відповідно, мономи x^α і x^β) є диз'юнктними.

Зрозуміло, що два мономи є диз'юнктними тоді й тільки тоді, коли вони не містять спільних змінних.

Лема 2.2. *Нехай* $f, g \in B_n\backslash\{0\}$ *та* $\mathrm{LM}_\preceq(f) \perp \mathrm{LM}_\preceq(g)$. *Тоді* $f \cdot g \neq 0$ *та*

$$\mathrm{LM}_\preceq(f \cdot g) = \mathrm{LM}_\preceq(f) \cdot \mathrm{LM}_\preceq(g).$$

Доведення. Нехай $f(x) = \bigoplus\limits_{\alpha \in V_n} f_\alpha x^\alpha$ та $g(x) = \bigoplus\limits_{\beta \in V_n} g_\beta x^\beta$ – поліноми Жегалкіна функцій f та g відповідно. Тоді поліном Жегалкіна функції $f \cdot g$ має вигляд

$$f(x) \cdot g(x) = \bigoplus_{(\alpha,\beta):\ f_\alpha = g_\beta = 1} x^{\alpha \vee \beta}, \tag{2.6}$$

де $\alpha \vee \beta = (\alpha_1 \vee \beta_1, \ldots, \alpha_n \vee \beta_n)$ позначає покоординатну диз'юнкцію булевих векторів $\alpha = (\alpha_1, \ldots, \alpha_n)$ та $\beta = (\beta_1, \ldots, \beta_n)$.

Позначимо $x^{\alpha^*} = \mathrm{LM}_\preceq(f)$, $x^{\beta^*} = \mathrm{LM}_\preceq(g)$. Тоді для будь-яких $\alpha, \beta \in V_n$ таких, що $f_\alpha = g_\beta = 1$, виконуються співвідношення $\alpha \preceq \alpha^*$, $\beta \preceq \beta^*$. Крім того, справедлива нерівність $\alpha \vee \beta \leqslant \alpha + \beta$. Звідси на підставі умов а) і б) означення 2.1 випливають такі співвідношення:

$$\alpha \vee \beta \preceq \alpha + \beta \preceq \alpha^* + \beta \preceq \alpha^* + \beta^*.$$

Оскільки за умовою леми $\alpha^* \perp \beta^*$, то $\alpha^* + \beta^* = \alpha^* \vee \beta^*$, звідки випливає, що $\alpha \vee \beta \preceq \alpha^* \vee \beta^*$. Таким чином,

$$\mathrm{LM}_\preceq(f \cdot g) \preceq \mathrm{LM}_\preceq(f) \cdot \mathrm{LM}_\preceq(g).$$

Нарешті, якщо $\alpha \prec \alpha^*$ або $\beta \prec \beta^*$, то $\alpha \vee \beta \prec \alpha^* \vee \beta^*$, оскільки в першому випадку

$$\alpha \vee \beta \preceq \alpha + \beta \prec \alpha^* + \beta \preceq \alpha^* + \beta^* = \alpha^* \vee \beta^*,$$

а в другому –

$$\alpha \vee \beta \preceq \alpha + \beta \preceq \alpha + \beta^* \prec \alpha^* + \beta^* = \alpha^* \vee \beta^*.$$

Звідси випливає, що $x^{\alpha^* \vee \beta^*}$ є старшим членом полінома (2.6), що й треба було довести. □

Як показує наступний приклад, умова диз'юнктивності в формулюванні леми 2.2 є суттєвою.

Приклад 2.4. Нехай $f, g \in B_3$ та $f(x_1, x_2, x_3) = x_1x_2 \oplus x_1x_2x_3$, $g(x_1, x_2, x_3) = x_3$, $\preceq = \preceq_{\mathrm{drl}}$. Тоді $f \cdot g = 0$, в той час як $\mathrm{LM}_{\preceq_{\mathrm{drl}}}(f) \cdot \mathrm{LM}_{\preceq_{\mathrm{drl}}}(g) = x_1x_2x_3 \cdot x_3 = x_1x_2x_3$.

2.3 Мономіальні ідеали

Означення 2.3. Ідеал $J \lhd B_n$ називається *мономіальним*, якщо він породжується деякою множиною мономів:

$$J = \langle x^{\beta_1}, \ldots, x^{\beta_m} \rangle, \tag{2.7}$$

де $\beta_i \in V_n$, $i \in \overline{1, m}$.

Такі ідеали мають найбільш просту будову. Зрозуміло, що будь-яка двійкова лінійна комбінація мономів, кожен з яких є кратним одному з мономів x^{β_i}, $i \in \overline{1, m}$, належить ідеалу (2.7). Як показано нижче, справедливе й обернене твердження.

Твердження 2.4. *Функція $f \in B_n\backslash\{0\}$ належить ідеалу (2.7) тоді й тільки тоді, коли кожен моном, що входить до виразу її полінома Жегалкіна, є кратним одному з мономів x^{β_i}, $i \in \overline{1,m}$.*

Доведення. Нехай $f(x) \in J$ і моном x^α міститься у виразі полінома $f(x)$. Покажемо, що існує $i \in \overline{1,m}$ таке, що $\beta_i \leqslant \alpha$.

Існують поліноми $h_i(x) \in B_n$ такі, що $f(x) = \bigoplus\limits_{i=1}^{m} x^{\beta_i} h_i(x)$. Запишемо $h_i(x)$ у вигляді $h_i(x) = \bigoplus\limits_{\gamma \in V_n} c_{i,\gamma} x^\gamma$, де $c_{i,\gamma} \in \{0,1\}$ для усіх $i \in \overline{1,m}$, $\gamma \in V_n$. Тоді

$$f(x) = \bigoplus_{i=1}^{m} \bigoplus_{\gamma \in V_n} c_{i,\gamma} x^{\beta_i \vee \gamma} = \bigoplus_{\nu \in V_n} x^\nu \left(\bigoplus_{(i,\gamma):\nu=\beta_i \vee \gamma} c_{i,\gamma} \right). \qquad (2.8)$$

Оскільки моном x^α міститься у виразі полінома $f(x)$, то коефіцієнт при x^α у правій частині рівності (2.8) є ненульовим. Отже, існує пара (i,γ) така, що $\alpha = \beta_i \vee \gamma$. Але тоді для зазначеного $i \in \overline{1,m}$ справедлива рівність $\beta_i \leqslant \alpha$, що й треба було довести.

□

Означення 2.4. Множина $M \subseteq V_n$ називається *монотонним класом*, якщо

$$\forall \alpha, \beta \in V_n : (\alpha \in M, \alpha \leqslant \beta) \Rightarrow \beta \in M.$$

Сукупність усіх мінімальних елементів монотонного класу M (тобто таких векторів $\alpha \in V_n$, для кожного з яких не існує вектора $\beta \in M$ з властивістю $\beta < \alpha$) називається *базисом* цього класу.

Помітимо, що кожному мономіальному ідеалу J вигляду (2.7) відповідає монотонний клас $M_J = \{\alpha \in V_n : x^\alpha \in J\}$. На підставі твер-

дження 2.4

$$M_J = \bigcup_{i=1}^{m} \{\alpha \in V_n : \alpha \geqslant \beta_i\}.$$

Наступне твердження показує, як побудувати найекономнішу в певному сенсі систему твірних мономіального ідеалу.

Твердження 2.5. *Нехай J – мономіальний ідеал вигляду (2.7) і $\beta_{i_1}, \ldots, \beta_{i_l}$ – усі мінімальні елементи множини $\{\beta_1, \ldots, \beta_m\}$ відносно часткового впорядкування $\leqslant$. Тоді мономи $x^{\beta_{i_1}}, \ldots, x^{\beta_{i_l}}$ складають мінімальну систему твірних ідеалу J (тобто таку, що породжує цей ідеал, але жодна її власна підсистема не володіє цією властивістю).*

Доведення. Безпосередньо з означення векторів $\beta_{i_1}, \ldots, \beta_{i_l}$ випливає, що система мономів $x^{\beta_{i_1}}, \ldots, x^{\beta_{i_l}}$ породжує ідеал J.

Припустимо, що деяка власна підсистема цієї системи, наприклад, $x^{\beta_{i_2}}, \ldots, x^{\beta_{i_l}}$ породжує зазначений ідеал. Тоді має місце співвідношення $x^{\beta_{i_1}} \in \langle x^{\beta_{i_2}}, \ldots, x^{\beta_{i_l}} \rangle$, з якого на підставі твердження 2.4 випливає, що $\beta_{i_1} \geqslant \beta_{i_j}$ для деякого $j \in \overline{2, l}$, що суперечить мінімальності елемента β_{i_1} у множині $\{\beta_1, \ldots, \beta_m\}$. Отже, $x^{\beta_{i_1}}, \ldots, x^{\beta_{i_l}}$ є мінімальною системою твірних ідеалу J. □

2.4 Теорема про подільність з остачею у кільці булевих функцій

Наступна теорема відіграє ключову роль у побудові основ теорії булевих базисів Грьобнера та надає змогу здійснювати своєрідне ділення з остачею булевої функції на систему булевих функцій.

Теорема 2.1. *Нехай $f \in B_n$, $f_1, \ldots, f_m \in B_n \backslash \{0\}$. Тоді існує єдиний набір поліномів $q_1, \ldots, q_{m+1} \in B_n$ таких, що:*

а) $f = f_1 q_1 \oplus \ldots \oplus f_m q_m \oplus f_{m+1} q_{m+1}$, *де* $f_{m+1} = 1$;

б) якщо $q_i \neq 0$, *то кожен моном, що входить до виразу полінома* q_i, *є диз'юнктним з мономом* $\mathrm{LM}_{\preceq}(f_i)$, $i \in \overline{1, m+1}$;

в) якщо $q_i \neq 0$, *то кожен моном у виразі полінома* $\mathrm{LM}_{\preceq}(f_i) \cdot q_i$ *не ділиться на мономи* $\mathrm{LM}_{\preceq}(f_1), \ldots, \mathrm{LM}_{\preceq}(f_{i-1})$, $i \in \overline{2, m+1}$;

Крім того, має місце рівність

$$\mathrm{LM}_{\preceq}(f) = \max_{i \in Q} \{\mathrm{LM}_{\preceq}(f_i q_i)\}, \tag{2.9}$$

де $Q = \{k \in \overline{1, m+1} : q_k \neq 0\}$, *причому* $\mathrm{LM}_{\preceq}(f_i q_i) \neq \mathrm{LM}_{\preceq}(f_j q_j)$ *для будь-яких різних* $i,j \in Q$.

Доведення. *Існування.* Якщо $f = 0$, то умови а), б), в) виконуються при $q_1 = \ldots = q_{m+1} = 0$, тому далі вважатимемо, що $f \neq 0$.

Нехай $\alpha_1 = (0, \ldots, 0) \prec \ldots \prec \alpha_{2^n} = (1, \ldots, 1)$ – усі булеві вектори довжини n, $x^{\alpha_1} \prec \ \ldots \prec x^{\alpha_{2^n}}$ – відповідні їм мономи. Для довільної ненульової функції $h \in B_n$ позначимо $\Theta(h)$ найбільше натуральне число t, для якого моном x^{α_t} міститься в поліномі h та ділиться хоча б на один з мономів $\mathrm{LM}_{\preceq}(f_i)$, $i \in \overline{1, m}$ (якщо зазначеного t не існує, вважатимемо $\Theta(h) = 0$).

Доведемо існування потрібного набору поліномів $q_1, \ldots, q_{m+1}$ за допомогою індукції за параметром $\Theta(f)$.

Якщо $\Theta(f) = 0$, тобто у виразі полінома f немає мономів, які діляться хоча б на один з мономів $\mathrm{LM}_{\preceq}(f_i)$, $i \in \overline{1, m}$, то, як показує безпосередня перевірка, набір поліномів $q_1 = \ldots = q_m = 0$, $q_{m+1} = f$ задовольняє умови а), б), в).

Припустимо, що існування потрібного набору доведено для кожної функції $f \in B_n$ такої, що $\Theta(f) < t$, де $t \geqslant 1$, та доведемо його для кожної функції f з властивістю $\Theta(f) = t$.

Нехай $\mathrm{LM}_{\preceq}(f_j) = x^{\beta_j}$, $j \in \overline{1,m}$, і l є найменшим натуральним числом, для якого моном x^{α_t} ділиться на моном x^{β_l}.

Розглянемо функцію

$$\widetilde{f} = f \oplus x^{\alpha_t - \beta_l} \cdot f_l, \tag{2.10}$$

де $\alpha_t - \beta_l$ позначає покоординатну різницю векторів α_t та β_l. Помітимо, що $\Theta(\widetilde{f}) < \Theta(f) = t$, оскільки старший член полінома $x^{\alpha_t - \beta_l} \cdot f_l$ дорівнює x^{α_t}, а поліном f не містить мономів $x^{\alpha_{t+1}}, \ldots, x^{\alpha_{2^n}}$. Отже, за припущенням індукції для функції $\widetilde{f}$ існує представлення у вигляді

$$\widetilde{f} = \widetilde{q}_1 f_1 \oplus \ldots \oplus \widetilde{q}_{l-1} f_{l-1} \oplus \widetilde{q}_l f_l \oplus \widetilde{q}_{l+1} f_{l+1} \oplus \ldots \oplus \widetilde{q}_{m+1} f_{m+1}, \tag{2.11}$$

де поліноми $\widetilde{q}_j$, $j \in \overline{1, m+1}$, задовольняють умови б), в).

На підставі формул (2.10), (2.11) справедлива рівність

$$f = \widetilde{q}_1 f_1 \oplus \ldots \oplus \widetilde{q}_{l-1} f_{l-1} \oplus (\widetilde{q}_l \oplus x^{\alpha_t - \beta_l}) f_l \oplus$$

$$\oplus\, \widetilde{q}_{l+1} f_{l+1} \oplus \ldots \oplus \widetilde{q}_{m+1} f_{m+1}. \tag{2.12}$$

Отже, для завершення цієї частини доведення залишається переконатися в тому, що поліноми $\widetilde{q}_1, \ldots, \widetilde{q}_{l-1}, \widetilde{q}_l \oplus x^{\alpha_t - \beta_l}, \widetilde{q}_{l+1}, \ldots, \widetilde{q}_{m+1}$ задовольняють умови б), в).

За припущенням індукції умова б) виконується для поліномів $\widetilde{q}_1, \ldots, \widetilde{q}_{l-1}, \widetilde{q}_{l+1}, \ldots, \widetilde{q}_{m+1}$, а також для полінома $\widetilde{q}_l$. Оскільки при цьому $x^{\alpha_t - \beta_l} \perp x^{\beta_l}$, то умова б) виконується і для полінома $\widetilde{q}_l \oplus x^{\alpha_t - \beta_l}$.

Далі, за припущенням індукції поліноми $\widetilde{q}_1, \ldots, \widetilde{q}_{l-1}, \widetilde{q}_{l+1}, \ldots, \widetilde{q}_{m+1}$ задовольняють умову в).

Покажемо, що цю умову задовольняє також поліном $\widetilde{q}_l \oplus x^{\alpha_t - \beta_l}$, а саме, що кожен моном у виразі полінома $(\widetilde{q}_l \oplus x^{\alpha_t - \beta_l}) x^{\beta_l}$ не ділиться

на мономи $x^{\beta_1}, \ldots, x^{\beta_{l-1}}$. Дійсно, справедлива рівність

$$(\widetilde{q}_l \oplus x^{\alpha_t - \beta_l}) x^{\beta_l} = \widetilde{q}_l x^{\beta_l} \oplus x^{\alpha_t},$$

причому x^{α_t} не ділиться на $x^{\beta_1}, \ldots, x^{\beta_{l-1}}$ внаслідок вибору числа l (нагадаємо, що l є найменшим натуральним числом, для якого моном x^{α_t} ділиться на моном x^{β_l}). Водночас жоден з мономів, які входять у вираз полінома $\widetilde{q}_l x^{\beta_l}$, не ділиться на $x^{\beta_1}, \ldots, x^{\beta_{l-1}}$ за припущення індукції.

Таким чином, поліноми $\widetilde{q}_1, \ldots, \widetilde{q}_{l-1}, \widetilde{q}_l \oplus x^{\alpha_t - \beta_l}, \widetilde{q}_{l+1}, \ldots, \widetilde{q}_{m+1}$ у розкладі (2.12) задовольняють умови б), в), що й треба було довести.

Переконаємося зараз, що для будь-якого набору поліномів $q_1, \ldots, q_{m+1} \in B_n$, які задовольняють умови б) і в), виконується нерівність $\mathrm{LM}_{\preceq}(f_i q_i) \neq \mathrm{LM}_{\preceq}(f_j q_j)$ для усіх різних $i, j \in Q = \{k \in \overline{1, m+1} : q_k \neq 0\}$.

Дійсно, на підставі умови б) та леми 2.2 для будь-якого $k \in Q$ маємо

$$\mathrm{LM}_{\preceq}(f_k q_k) = \mathrm{LM}_{\preceq}(f_k)\,\mathrm{LM}_{\preceq}(q_k) = x^{\beta_k} \cdot \mathrm{LM}_{\preceq}(q_k).$$

Отже, якщо $\mathrm{LM}_{\preceq}(f_i q_i) = \mathrm{LM}_{\preceq}(f_j q_j)$ для деяких $i, j \in Q$, де $i < j$, то $x^{\beta_i} \cdot \mathrm{LM}_{\preceq}(q_i) = x^{\beta_j} \cdot \mathrm{LM}_{\preceq}(q_j)$ і старший член полінома $\mathrm{LM}_{\preceq}(f_j) \cdot q_j$ ділиться на моном x^{β_i}, що суперечить умові в).

Помітимо тепер, що оскільки мономи $\mathrm{LM}_{\preceq}(f_i q_i)$, $i \in Q$, є попарно різними, то за умовою а) та лемою 2.1 справедлива рівність (2.9). Тому для завершення доведення теореми залишається переконатися у єдиності набору поліномів $q_1, \ldots, q_{m+1} \in B_n$, які задовольняють умови а), б), в).

Єдиність. Припустимо, що існують два різних представлення:

$$f = q_1 f_1 \oplus \ldots \oplus q_{m+1} f_{m+1}, \quad f = \widetilde{q}_1 f_1 \oplus \ldots \oplus \widetilde{q}_{m+1} f_{m+1},$$

де поліноми $q_1, \ldots, q_{m+1}, \widetilde{q}_1, \ldots, \widetilde{q}_{m+1}$ задовольняють умови б), в). Додаючи наведені рівності, отримаємо, що

$$0 = (q_1 \oplus \widetilde{q}_1) f_1 \oplus \ldots \oplus (q_1 \oplus \widetilde{q}_{m+1}) f_{m+1}. \tag{2.13}$$

Оскільки поліноми q_i та $\widetilde{q}_i$ задовольняють умови б) і в), то поліноми $q'_i = q_i \oplus \widetilde{q}_i$ теж задовольняють ці умови, $i \in \overline{1, m+1}$. Отже, за доведеним вище для будь-яких різних $i, j \in \{k \in \overline{1, m+1} : q'_k \neq 0\}$ справедлива нерівність $\mathrm{LM}_{\preceq}(f_i q'_i) \neq \mathrm{LM}_{\preceq}(f_j q'_j)$. Звідси на підставі леми 2.1 випливає, що функція $(q_1 \oplus \widetilde{q}_1) f_1 \oplus \ldots \oplus (q_1 \oplus \widetilde{q}_{m+1}) f_{m+1}$ є ненульовою, що, однак, суперечить рівності (2.13). □

З доведеної теореми випливає коректність такого означення.

Означення 2.5. Поліном q_{m+1} називається *залишком від ділення* функції $f \in B_n$ на систему функцій $f_1, \ldots, f_m \in B_n \backslash \{0\}$ і позначається $\mathrm{Res}(f; f_1, \ldots, f_m)$, якщо існують $q_1, \ldots, q_m \in B_n$ такі, що поліноми $q_1, \ldots, q_m, q_{m+1}$ задовольняють умови а), б), в) теореми 2.1.

Безпосередньо з доведеної теореми випливає такий результат.

Наслідок 2.2. *Нехай* $f, f_1, \ldots, f_m \in B_n \backslash \{0\}$, $r = \mathrm{Res}(f; f_1, \ldots, f_m)$. *Тоді рівність* $\mathrm{LM}_{\preceq}(r) = \mathrm{LM}_{\preceq}(f)$ *виконується в тому й тільки тому випадку, коли моном* $\mathrm{LM}_{\preceq}(f)$ *не ділиться на мономи* $\mathrm{LM}_{\preceq}(f_1), \ldots, \mathrm{LM}_{\preceq}(f_m)$.

Твердження 2.6. *Для будь-яких* $f, g \in B_n$, $f_1, \ldots, f_m \in B_n \backslash \{0\}$ *виконується таке співвідношення:*

$$\mathrm{Res}(f \oplus g; f_1, \ldots, f_m) = \mathrm{Res}(f; f_1, \ldots, f_m) \oplus \mathrm{Res}(g; f_1, \ldots, f_m).$$

Таким чином, $\mathrm{Res}(\,\cdot\,; f_1, \ldots, f_m)$ *є лінійним перетворенням векторного простору* B_n.

Доведення. Розглянемо представлення функцій f і g, зазначені в теоремі 2.1, та додамо їх:

$$f \oplus g = (q_1 \oplus \widetilde{q}_1)f_1 \oplus \ldots \oplus (q_1 \oplus \widetilde{q}_{m+1})f_{m+1}.$$

Оскільки поліноми q_i та $\widetilde{q}_i$ задовольняють умови б), в) теореми, то поліноми $q_i \oplus \widetilde{q}_i$ також задовольняють ці умови, $i \in \overline{1, m+1}$. Звідси випливає, що $q_{m+1} \oplus \widetilde{q}_{m+1}$ є залишком від ділення функції $f \oplus g$ на систему функцій $f_1, \ldots, f_m$. □

Зауважимо, що доведення теореми 2.1 є конструктивним і надає можливість запропонувати такий алгоритм ділення (ненульової) булевої функції на систему ненульових булевих функцій.

Алгоритм 2.1.

Вхідні дані. Функції $f, f_1, \ldots, f_m \in B_n \backslash \{0\}$, мономіальне впорядкування $\preceq$.

Позначимо $\mathrm{LM}_{\preceq}(f_j) = x^{\beta_j}$, $j \in \overline{1, m}$.

1. Покласти $\widetilde{f} = f$, $q_1 = \ldots = q_{m+1} = 0$.

2. Поки $\widetilde{f} \neq 0$:

   – якщо l є найменшим натуральним числом, для якого моном $x^{\alpha} = \mathrm{LM}_{\preceq}(\widetilde{f})$ ділиться на x^{β_l}, покласти

   $$\widetilde{f} = \widetilde{f} \oplus x^{\alpha-\beta_l} \cdot f_l, \quad q_l = q_l \oplus x^{\alpha-\beta_l};$$

   – якщо зазначеного l не існує, то покласти

   $$\widetilde{f} = \widetilde{f} \oplus x^{\alpha}, \quad q_{m+1} = q_{m+1} \oplus x^{\alpha}.$$

При виході з циклу на кроці 2 алгоритм сформує набір поліномів $q_1, \ldots, q_{m+1}$, що задовольняють умови а), б), в) теореми 2.1. Коректність алгоритму випливає безпосередньо з доведення цієї теореми.

Приклад 2.5. Застосуємо наведений алгоритм до мономіального впорядкування $\preceq = \preceq_{\mathrm{drl}}$ та функцій $f, f_1, f_2, f_3 \in B_3$, де

$$f = x_2x_3 \oplus x_1x_3 \oplus x_3 \oplus x_2,$$

$$f_1 = x_1x_3 \oplus x_1, f_2 = x_2 \oplus 1, f_3 = x_2x_3 \oplus x_1.$$

Зазначимо, що $\mathrm{LM}_{\preceq_{\mathrm{drl}}}(f_1) = x_1x_3$, $\mathrm{LM}_{\preceq_{\mathrm{drl}}}(f_2) = x_2$, $\mathrm{LM}_{\preceq_{\mathrm{drl}}}(f_3) = x_2x_3$.

1. Покладемо $\widetilde{f} = f$, $q_1 = q_2 = q_3 = q_4 = 0$.

2. Виконаємо такі обчислення.

   2.1. Моном $x_2x_3 = \mathrm{LM}_{\preceq}(\widetilde{f})$ ділиться на мономи x_2 та x_2x_3, при цьому $l = 2$. Отже, покладемо $\widetilde{f} = \widetilde{f} \oplus x_3f_2 = x_1x_3 \oplus x_2$ та $q_2 = q_2 \oplus x_3 = x_3$.

   2.2. Моном $x_1x_3 = \mathrm{LM}_{\preceq}(\widetilde{f})$ ділиться лише на моном x_1x_3, тому $l = 1$. Відповідно, покладемо $\widetilde{f} = \widetilde{f} \oplus f_1 = x_2 \oplus x_1$ та $q_1 = q_1 \oplus 1 = 1$.

   2.3. Моном $x_2 = \mathrm{LM}_{\preceq}(\widetilde{f})$ ділиться лише на моном x_2, тому $l = 2$. Покладемо $\widetilde{f} = \widetilde{f} \oplus f_2 = x_1 \oplus 1$ та $q_2 = q_2 \oplus 1 = x_3 \oplus 1$.

   2.4. Моном $x_1 = \mathrm{LM}_{\preceq}(\widetilde{f})$ не ділиться на жоден зі старших членів поліномів f_1, f_2, f_3, тому покладемо $\widetilde{f} = \widetilde{f} \oplus x_1 = 1$ та $q_4 = q \oplus x_1 = x_1$.

   2.5. Моном $1 = \mathrm{LM}_{\preceq}(\widetilde{f})$ не ділиться на жоден зі старших членів поліномів f_1, f_2, f_3, тому покладемо $\widetilde{f} = \widetilde{f} \oplus 1 = 0$ та $q_4 = q_4 \oplus 1 = x_1 \oplus 1$.

В результаті отримаємо шуканий розклад полінома f:

$$f = \underbrace{(x_1x_3 \oplus x_1)}_{f_1} \cdot \underbrace{1}_{q_1} \oplus \underbrace{(x_2 \oplus 1)}_{f_2} \cdot \underbrace{(x_3 \oplus 1)}_{q_2} \oplus \underbrace{(x_2x_3 \oplus x_1)}_{f_3} \cdot \underbrace{0}_{q_3} \oplus \underbrace{(x_1 \oplus 1)}_{q_4}.$$

2.5 Означення та основні властивості базисів Грьобнера

Означення 2.6. Нехай $I \lhd B_n$, $I \neq \{0\}$. Тоді набір функцій $g_1, \ldots, g_m \in I \backslash \{0\}$ називається *базисом Грьобнера* ідеалу I, якщо для будь-якого $f \in I \backslash \{0\}$ існує $i \in \overline{1,m}$ таке, що моном $\mathrm{LM}_{\preceq}(g_i)$ ділить моном $\mathrm{LM}_{\preceq}(f)$.

Твердження 2.7. *Для будь-якого ненульового ідеалу $I \lhd B_n$ існує базис Грьобнера.*

Доведення. Зрозуміло, що набір, який складається з усіх ненульових елементів ідеалу I, є базисом Грьобнера цього ідеалу. □

Звичайно, такі базиси є дуже надлишковими, тому в наступному пункті наведено більш корисні приклади базисів Грьобнера.

Теорема 2.2. *Нехай $I \lhd B_n$, $I \neq \{0\}$, $g_1, \ldots, g_m \in I \backslash \{0\}$. Тоді є рівносильними такі твердження:*

1) $g_1, \ldots, g_m$ – базис Грьобнера ідеалу I;

2) для будь-якого $f \in I$ виконується рівність $\mathrm{Res}(f; g_1, \ldots, g_m) = 0$;

3) $\langle g_1, \ldots, g_m \rangle = I$ та

$$\langle \mathrm{LM}_{\preceq}(g_1), \ldots, \mathrm{LM}_{\preceq}(g_m) \rangle = \langle x^{\alpha} | \ \exists f \in I : x^{\alpha} = \mathrm{LM}_{\preceq}(f) \rangle. \qquad (2.14)$$

Доведення. 1) $\Rightarrow$ 2) Нехай $f \in I$. Оскільки $g_1, \ldots, g_m \in I$, то за теоремою 2.1 (див. умову а)) $\mathrm{Res}(f; g_1, \ldots, g_m) \in I$. Якщо $\mathrm{Res}(f; g_1, \ldots, g_m) \neq 0$, то за цією ж теоремою (див. умову в)) старший член полінома $\mathrm{Res}(f; g_1, \ldots, g_m)$ не ділиться на старші члени поліномів $g_1, \ldots, g_m$. Однак це суперечить тому, що зазначені поліноми утворюють базис Грьобнера ідеалу I.

2) $\Rightarrow$ 3) Нехай $f \in I$. Тоді $\mathrm{Res}\,(f; g_1, \ldots, g_m) = 0$ і на підставі теореми 2.1 функцію f можна представити у вигляді

$$f = q_1 g_1 \oplus \ldots \oplus q_m g_m, \tag{2.15}$$

де поліноми $q_1, \ldots, q_m$ задовольняють умови б), в) зазначеної теореми. Звідси випливає, що $f \in \langle g_1, \ldots, g_m \rangle$. Таким чином, $\langle g_1, \ldots, g_m \rangle = I$.

Доведемо рівність (2.14). Позначимо J ідеал у правій частині цієї рівності, $x^{\beta_1}, \ldots, x^{\beta_m}$ – старші члени поліномів $g_1, \ldots, g_m$ відповідно. Оскільки $g_1, \ldots, g_m \in I$, то $\langle x^{\beta_1}, \ldots, x^{\beta_m} \rangle \subseteq J$.

Для доведення оберненого включення достатньо переконатися в тому, що кожен моном x^α, який є старшим членом деякого полінома $f \in I$, належить ідеалу $\langle x^{\beta_1}, \ldots, x^{\beta_m} \rangle$.

За теоремою 2.1 справедлива рівність (2.15). При цьому

$$\mathrm{LM}_{\preceq}(f) = \max_{i \in Q} \{\mathrm{LM}_{\preceq}(q_i g_i)\},$$

де $Q = \{k \in \overline{1,m} : q_k \neq 0\}$, і на підставі умови б) теореми 2.1 і леми 2.2

$$\mathrm{LM}_{\preceq}(q_i g_i) = \mathrm{LM}_{\preceq}(q_i) \cdot \mathrm{LM}_{\preceq}(g_i) = \mathrm{LM}_{\preceq}(q_i) \cdot x^{\beta_i}, i \in \overline{1,m}.$$

Звідси випливає, що

$$x^\alpha = \max_{i \in Q} \{\mathrm{LM}_{\preceq}(q_i) \cdot x^{\beta_i}\},$$

а отже, існує $j \in \overline{1,m}$ таке, що $x^\alpha = \mathrm{LM}_{\preceq}(q_j) \cdot x^{\beta_j}$. Таким чином, $x^\alpha \in \langle x^{\beta_1}, \ldots, x^{\beta_m} \rangle$, що й треба було довести.

3) $\Rightarrow$ 1) Нехай $f \in I \backslash \{0\}$, $\mathrm{LM}_{\preceq}(f) = x^\alpha$, $\mathrm{LM}_{\preceq}(g_i) = x^{\beta_i}, i \in \overline{1,m}$. На підставі рівності (2.14) $x^\alpha \in \langle x^{\beta_1}, \ldots, x^{\beta_m} \rangle$, а тоді за твердженням

2.4 моном x^α ділиться на один з мономів $x^{\beta_1}, \ldots, x^{\beta_m}$. Отже, згідно з означенням 2.6 набір $g_1, \ldots, g_m$ є базисом Грьобнера ідеалу I. □

2.6 Мінімальні та редуковані базиси Грьобнера

Як зазначено вище, довільний базис Грьобнера ідеалу може бути дуже надлишковим, тому постає питання про найекономніший у певному природному сенсі базис Грьобнера.

Означення 2.7. Базис Грьобнера $g_1, \ldots, g_m$ ідеалу I називається *мінімальним*, якщо старші члени різних поліномів $g_1, \ldots, g_m$ не ділять один одний.

Твердження 2.8. *Для будь-якого ненульового ідеалу кільця B_n існує мінімальний базис Грьобнера.*

Доведення. Нехай $g_1, \ldots, g_m$ – довільний базис Грьобнера ідеалу I, $x^{\beta_1} = \mathrm{LM}_{\preceq}(g_1), \ldots, x^{\beta_m} = \mathrm{LM}_{\preceq}(g_m)$. Нехай, далі, $\beta_{i_1}, \ldots, \beta_{i_l}$ – усі мінімальні елементи множини $\{\beta_1, \ldots, \beta_m\}$ відносно часткового впорядкування $\leqslant$. Тоді система $g_{i_1}, \ldots, g_{i_l}$ є мінімальним базисом Грьобнера ідеалу I. □

Наступне твердження надає характеризацію мінімальних базисів Грьобнера в термінах монотонних класів (див. означення 2.4).

Твердження 2.9. *Базис Грьобнера $g_1, \ldots, g_m$ ідеалу I є мінімальним тоді й тільки тоді, коли вектори $\beta_1, \ldots, \beta_m$, де $\mathrm{LM}_{\preceq}(g_i) = x^{\beta_i}, i \in \overline{1,m}$, утворюють базис монотонного класу M_J, який відповідає мономіальному ідеалу J, породженому старшими членами усіх ненульових функцій $f \in I$.*

Доведення. Якщо вектори $\beta_1, \ldots, \beta_m$ утворюють базис монотонного класу M_J, то співвідношення $\beta_i \leqslant \beta_j$ є неможливим для

будь-яких різних $i, j \in \overline{1,m}$. Отже, $g_1, \ldots, g_m$ є мінімальним базисом Грьобнера ідеалу I.

Навпаки, нехай $g_1, \ldots, g_m$ – мінімальний базис Грьобнера зазначеного ідеалу. Тоді на підставі твердження 3) теореми 2.2 $J = \langle x^{\beta_1}, \ldots, x^{\beta_m} \rangle$ і за твердженням 2.4 клас M_J складається з усіх векторів $\alpha \in V_n$, для кожного з яких існує $i \in \overline{1,m}$ з властивістю $\beta_i \leqslant \alpha$. Звідси випливає, що кожен мінімальний елемент класу M_J співпадає з одним з векторів $\beta_1, \ldots, \beta_m$. З іншого боку, якщо для деякого $i \in \overline{1,m}$ існує $\gamma \in M_J$ таке, що $\beta_i > \gamma$, то за доведеним існує $j \in \overline{1,m}$ таке, що $\beta_j \leqslant \gamma$. Але тоді виконується нерівність $\beta_i > \beta_j$, що суперечить мінімальності базису $g_1, \ldots, g_m$. Таким чином, усі вектори $\beta_1, \ldots, \beta_m$ є мінімальними елементами класу M_J, що й треба було довести. □

З наведеного твердження випливає, що набір старших членів мінімального базису Грьобнера довільного ненульового ідеалу (а, отже, й кількість елементів у такому базисі) не залежить від базису. Разом з тим, в загальному випадку ідеал може мати декілька різних мінімальних базисів Грьобнера.

Означення 2.8. Базис Грьобнера $g_1, \ldots, g_m$ ідеалу I називається *редукованим*, якщо для будь-яких різних $i, j \in \overline{1,m}$ кожен моном у виразі полінома g_i не ділиться на старший член полінома g_j.

Теорема 2.3. *Для будь-якого ненульового ідеалу I кільця B_n існує єдиний редукований базис Грьобнера.*

Доведення. Нехай $g_1, \ldots, g_m$ – мінімальний базис Грьобнера ідеалу I, $\mathrm{LM}_{\preceq}(g_i) = x^{\beta_i}$, $i \in \overline{1,m}$. Відсортуємо поліноми $g_1, \ldots, g_m$ відносно впорядкування $\preceq$ за спаданням їхніх старших членів:

$$\mathrm{LM}_{\preceq}(g_m) \prec \mathrm{LM}_{\preceq}(g_{m-1}) \prec \ldots \prec \mathrm{LM}_{\preceq}(g_1) \tag{2.16}$$

та визначимо таку *процедуру редукції*:

$$\begin{aligned} r_m &= g_m, \\ r_{m-1} &= \mathrm{Res}\,(g_{m-1}; r_m), \\ r_{m-2} &= \mathrm{Res}\,(g_{m-2}; r_{m-1}, r_m), \\ &\dots \quad \dots \quad \dots \quad \dots \\ r_1 &= \mathrm{Res}\,(g_1; r_2, \dots, r_m). \end{aligned}$$

Покажемо, що поліноми $r_1, \dots, r_m$ утворюють редукований базис Грьобнера ідеалу I.

Перш за все, зрозуміло, що вони належать зазначеному ідеалу. По-друге, старші члени поліномів $g_1, \dots, g_m$ попарно не ділять один одний. Звідси, використовуючи індукцію по i та наслідок 2.2, отримаємо, що $\mathrm{LM}_{\preceq}(r_i) = \mathrm{LM}_{\preceq}(g_i)$ для всіх $i \in \overline{1,m}$. Отже, поліноми $r_1, \dots, r_m$ утворюють мінімальний базис Грьобнера ідеалу I. Нарешті, для будь-якого $i \in \overline{1,m}$ поліном r_i є сумою мономів, жоден з яких не ділиться на мономи $x^{\beta_{i+1}}, \dots, x^{\beta_m}$ (за умовою в) теореми 2.1), а також на мономи $x^{\beta_1}, \dots, x^{\beta_{i-1}}$ (на підставі рівностей $\mathrm{LM}_{\preceq}(r_i) = x^{\beta_i}$, $i \in \overline{1,m}$ та умови (2.16)). Таким чином, поліноми $r_1, \dots, r_m$ утворюють редукований базис Грьобнера ідеалу I, що й треба було довести.

Нехай зараз $r'_1, \dots, r'_{m'}$ – інший редукований базис Грьобнера цього ідеалу. Помітимо, що оскільки обидва базиси є мінімальними, то $m = m'$, $\mathrm{LM}_{\preceq}(r'_i) = \mathrm{LM}_{\preceq}(r_i) = x^{\beta_i}$для кожного $i \in \overline{1,m}$. Якщо $r_i \oplus r'_i \neq 0$ для деякого i, то за означенням базису Грьобнера старший член полінома $r_i \oplus r'_i$ (який належить ідеалу I) ділиться на один з мономів x^{β_j} для деякого $j \neq i$. Але тоді хоча б один з поліномів r_i, r'_i містить моном, кратний x^{β_j}, що суперечить редукованості базисів $r_1, \dots, r_m$ та $r'_1, \dots, r'_{m'}$.

□

Приклад 2.6. Нехай $f(x_1, x_2, x_3) = x_1x_2 \oplus x_3 \oplus x_2 \oplus x_1$. Побудуємо базис Грьобнера ідеалу $I = \langle f \rangle$ для мономіального впорядкування $\preceq_{\text{drl}}$.

Помітимо, що ідеал I містить функції f, $x_1 \cdot f = x_1x_3 \oplus x_1$ та $x_2 \cdot f = x_2x_3 \oplus x_2$, старші мономи яких

$$\text{LM}_{\preceq_{\text{drl}}}(f) = x_1x_2, \text{LM}_{\preceq_{\text{drl}}}(x_1f) = x_1x_3, \text{LM}_{\preceq_{\text{drl}}}(x_2f) = x_2x_3$$

утворюють множину всіх мономів степеня 2 від змінних x_1, x_2, x_3.

Нагадаємо, що за твердженням 2.1 ідеал I складається з усіх функцій, які обертаються в нуль на множині $V(I)$ нулів функції f:

$$I = J(V(I)) = \{g \in B_3 |\ \forall x \in V_3 : f(x) = 0 \Rightarrow g(x) = 0\}.$$

При цьому

$$V(I) = \{(0,0,0),\ (0,1,1),\ (1,0,1),\ (1,1,1)\}.$$

Звідси випливає, що ідеал I не містить ненульових афінних функцій. (Дійсно, якщо існує афінна функція $g \in I\backslash\{0\}$, то вона обертається в нуль точно на 4 двійкових векторах довжини 3. Але тоді g має ті ж самі нулі, що і f, і, отже, співпадає з f, що суперечить рівності $\deg f = 2$).

Таким чином, ідеал I містить тільки ненульові поліноми, степінь яких не менше 2, причому серед них є три поліноми, старші члени яких є утворюють множину всіх мономів степеня 2 від трьох змінних. Звідси випливає, що для довільного $g \in I\backslash\{0\}$ моном $\text{LM}_{\preceq_{\text{drl}}}(g)$ ділиться принаймні на один з мономів $\text{LM}_{\preceq_{\text{drl}}}(f)$, $\text{LM}_{\preceq_{\text{drl}}}(x_1f)$, $\text{LM}_{\preceq_{\text{drl}}}(x_2f)$. Отже, система функцій f, x_1f, x_2f є мінімальним базисом Грьобнера ідеалу I.

Більше того, як показує безпосередня перевірка, отриманий базис Грьобнера є редукованим.

2.7 Застосування базисів Грьобнера до побудови алгебраїчних атак на потокові шифри

Як зазначено в п. 1.5, алгебраїчні атаки базуються на розв'язанні систем алгебраїчних рівнянь, що пов'язують знаки гами, виробленої генератором, з його початковим станом.

Розглянемо довільну систему булевих рівнянь вигляду (2.4) та позначимо $I = \langle f_1, \ldots, f_m \rangle$ ідеал, породжений множиною функцій у лівій частині цієї системи.

Має місце наступне твердження.

Твердження 2.10. *Система рівнянь (2.4) є несумісною тоді й тільки тоді, коли редукований базис Грьобнера ідеалу I складається з єдиної функції* 1. *Крім того, ця система має єдиний розв'язок $(a_1, \ldots, a_n)$ тоді й тільки тоді, коли редукований базис Грьобнера ідеалу I складається з функцій $x_1 \oplus a_1, \ldots, x_n \oplus a_n$.*

Доведення. Скористаємося наслідком 2.1 та помітимо, що функція 1 утворює редукований базис Грьобнера ідеалу $\langle 1 \rangle$, а функції $x_1 \oplus a_1, \ldots, x_n \oplus a_n$ утворюють редукований базис Грьобнера ідеалу $\langle x_1 \oplus a_1, \ldots, x_n \oplus a_n \rangle$ (останнє твердження є наслідком того, що старший член будь-якої ненульової функції $f \in \langle x_1 \oplus a_1, \ldots, x_n \oplus a_n \rangle$ є відмінним від 1, а отже, ділиться, принаймні, на один з мономів $x_1, \ldots, x_n$).

□

Доведене твердження показує, що за умови існування єдиного розв'язку системи рівнянь (2.4) цей розв'язок можна знайти, обчислюючи редукований базис Грьобнера ідеалу, породженого функціями в лівій частині системи. (Більш того, будь-який метод розв'язання булевих систем рівнянь із зазначеною властивістю є

методом знаходження редукованих базисів Грьобнера відповідних ідеалів).

Зауважимо також, що припущення про єдиність розв'язку системи рівнянь (2.4) часто приймається при побудові атак на потокові шифри, оскільки вважається, що противник має доступ до необмеженої кількості знаків гами (а відстань єдиності генератора є обмеженою величиною).

Таким чином, алгоритми обчислення базисів Грьобнера можна безпосередньо використовувати для побудови алгебраїчних атак. На сьогодні відомо чимало таких алгоритмів (для ідеалів кільця поліномів від декількох змінних над довільним полем, проте вони без особливих утруднень переносяться на випадок ідеалів кільця булевих функцій). Зазначені алгоритми реалізовано в сучасних системах комп'ютерної алгебри, на кшталт `Magma`, `Maple` та `Sage`, проте питання щодо теоретичних оцінок їхньої часової складності залишається предметом активних досліджень. Більш докладні відомості з цих питань можна знайти в [SM, BFS, ST].

2.8 Мінімальний степінь ідеалу кільця булевих функцій

Одним із загальних методів розв'язання систем рівнянь вигляду (2.4) є побудова наслідків з них, які мають менший степінь ніж рівняння вхідної системи. Оскільки всі такі наслідки визначаються ідеалом, породженим функціями у лівій частині системи (2.4), видається природним ввести таке означення.

Означення 2.9. Нехай $I \lhd B_n$, $I \neq \{0\}$. Тоді *мінімальним степенем* ідеалу I називається число

$$\operatorname{mindeg} I = \min\{\deg f : \ f \in I \backslash \{0\}\},$$

де $\deg f$ позначає степінь полінома Жегалкіна функції f.

Мінімальний степінь ідеалу є важливим параметром, від якого залежить складність розв'язання систем булевих рівнянь. Тому постає запитання про обчислення цього параметра, а також про знаходження самих функцій найменшого степеня, які містяться в заданому ідеалі.

Відповідь на це запитання надає наступна теорема, що належить Г. Арсу та Ж.-Ш. Фожеру [AF].

Теорема 2.4. *Нехай $I \lhd B_n$, $I \neq \{0\}$, $\preceq$ – степеневе мономіальне впорядкування на множині $\mathbb{N}_0^n$, G – мінімальний базис Грьобнера ідеалу I відносно цього впорядкування. Нехай, далі, $g_1, \ldots, g_m$ є усі функції з G, що мають найменший степінь d. Тоді*

1) $\operatorname{mindeg} I = d$;

2) кожна функція $f \in I$ степеня d може бути однозначно представлена у вигляді

$$f = c_1 g_1 \oplus \ldots \oplus c_m g_m, \tag{2.17}$$

де $c_i \in \{0, 1\}$, $i \in \overline{1, m}$. Зокрема, ідеал I містить точно $2^m - 1$ функцій степеня d.

Доведення. Нехай $f \in I \backslash \{0\}$, $\mathrm{LM}_{\preceq}(f) = x^{\alpha}$. Тоді $\deg f = |\alpha| = \alpha_1 + \ldots + \alpha_n$, оскільки $\preceq$ є степеневим впорядкуванням. При цьому, згідно з означенням базису Грьобнера, x^{α} ділиться на один з мономів $x^{\beta} = \mathrm{LM}_{\preceq}(g)$, де $g \in G$. Отже, $\alpha \geqslant \beta$ і $\deg f = |\alpha| \geqslant |\beta| = \deg g \geqslant d$, де остання нерівність випливає з означення параметра d. Таким чином, степінь кожної функції $f \in I \backslash \{0\}$ є не менше ніж d і, оскільки $g_1 \in I$, $\deg g_1 = d$, то $\operatorname{mindeg} I = d$.

Нехай зараз $f \in I$, $\deg f = d$. Тоді на підставі наведених вище міркувань отримаємо, що $d = \deg f = |\alpha| \geqslant |\beta| = \deg g \geqslant d$ і $\alpha \geqslant \beta$,

звідки випливає, що $\alpha = \beta$ і $g = g_i$ для деякого $i \in \overline{1,m}$. Таким чином, функції f та g_i мають однакові старші мономи x^α, де $|\alpha| = \deg f = \deg g_i = d$.

Розглянемо функцію $f^{(1)} = f \oplus g_i$, яка належить ідеалу I. Якщо $f^{(1)} = 0$, то $f = g_i$ має вигляд (2.17). У протилежному випадку маємо: $f^{(1)} \in I\backslash\{0\}$, $\deg f^{(1)} = d$, $\mathrm{LM}_\preceq(f) \succ \mathrm{LM}_\preceq(f^{(1)})$ і до функції $f^{(1)}$ є застосовними наведені вище міркування: існує $j \in \overline{1,m}$ таке, що $\mathrm{LM}_\preceq(f^{(1)}) = \mathrm{LM}_\preceq(g_j)$ і, отже, або $f^{(2)} \stackrel{\text{def}}{=} f^{(1)} \oplus g_j = 0$ (і тоді $f = f^{(1)} \oplus g_i = g_j \oplus g_i$ має вигляд (2.17)), або $f^{(2)} \in I\backslash\{0\}$, $\deg f^{(2)} = d$ і $\mathrm{LM}_\preceq(f^{(1)}) \succ \mathrm{LM}_\preceq(f^{(2)})$. Зрозуміло, що за скінченне число кроків ланцюг $\mathrm{LM}_\preceq(f) \succ \mathrm{LM}_\preceq(f^{(1)}) \succ \mathrm{LM}_\preceq(f^{(2)}) \succ \ldots$ обірветься, і для функції f буде отримане представлення у вигляді (2.17).

Нарешті, оскільки G є мінімальним базисом Грьобнера ідеалу I, то старші члени поліномів $g_1, \ldots, g_m$ є попарно різними, звідки на підставі леми 2.1 випливає лінійна незалежність цих функцій над полем з двох елементів. Отже, для кожної функції $f \in I$ степеня d існує єдине представлення у вигляді (2.17). □

Приклад 2.7. Нехай $f(x_1, x_2, x_3) = x_1x_2 \oplus x_3 \oplus x_2 \oplus x_1$, $I = \langle f \rangle$. Як показано вище (див. приклад 2.6), редукований базис Грьобнера ідеалу I складається з функцій f, x_1f, x_2f, кожна з яких має степінь 2. Отже, $\mathrm{mindeg}\, I = 2$, причому ідеал I містить рівно 7 функцій найменшого степеня (зауважимо також, що загальна кількість функцій в I дорівнює 16).

Доведемо зараз твердження, яке надає змогу оцінювати (а в деяких випадках – обчислювати точно) мінімальний степінь ідеалу за допомогою алгоритму Гауса. Попередньо введемо декілька позначень.

Для будь-якого натурального d позначимо $m(n,d) = \sum\limits_{i=0}^{d} \binom{n}{i}$. Для заданого ненульового ідеалу I кільця B_n розглянемо $|V(I)| \times m(n,d)$-

матрицю $M_{I,d}$, рядки якої занумеровані векторами $a \in V(I)$, а стовпці – векторами $\alpha \in V_n$ мультистепеня $|\alpha| \leqslant d$. За означенням елемент матриці $M_{I,d}$, що знаходиться на перетині її рядка з номером a та стовпця з номером α, дорівнює значенню монома x^α у точці $x = a$.

Твердження 2.11. *Справедливе співвідношення*

$$\operatorname{mindeg} I \geqslant d+1 \Leftrightarrow \operatorname{rank}(M_{I,d}) = m(n,d).$$

Доведення. Згідно з означенням матриці $M_{I,d}$ і твердженням 2.1 ненульова функція $f(x) = \bigoplus\limits_{\alpha \in V_n : |\alpha| \leqslant d} c_\alpha x^\alpha$ належить ідеалу I тоді й тільки тоді, коли вектор $(c_\alpha : \alpha \in V_n, |\alpha| \leqslant d)$ є ненульовим розв'язком системи лінійних рівнянь $M_{I,d} z^{\downarrow} = 0^{\downarrow}$. Отже, $\operatorname{mindeg} I \geqslant d+1 \Leftrightarrow (\forall f \in I \backslash \{0\} : \deg f \geqslant d+1) \Leftrightarrow$ (система рівнянь $M_{I,d} z^{\downarrow} = 0^{\downarrow}$ не має ненульових розв'язків) $\Leftrightarrow \operatorname{rank}(M_{I,d}) = m(n,d)$. □

Наслідок 2.3. *Нехай d є найбільшим натуральним числом, що задовольняє нерівність $m(n,d) \leqslant |V(I)|$. Тоді* $\operatorname{mindeg} I \leqslant d+1$*; при цьому* $\operatorname{mindeg} I = d+1$ *тоді й тільки тоді, коли* $\operatorname{rank}(M_{I,d}) = m(n,d)$.

Таким чином, згідно з наслідком 2.3 для оцінювання мінімального степеня ненульового ідеалу $I \lhd B_n$ достатньо:

1) знайти найбільше натуральне d, для якого $m(n,d) \leqslant |V(I)|$;

2) побудувати матрицю $M_{I,d}$ та обчислити її ранг за допомогою алгоритму Гаусса.

Якщо $\operatorname{rank}(M_{I,d}) = m(n,d)$, то $\operatorname{mindeg} I = d+1$; в іншому випадку $\operatorname{mindeg} I \leqslant d$.

Приклад 2.8. Розглянемо ідеал I, породжений функцією f з прикладу 2.6. Тоді $|V(I)| = 4$ і найбільше натуральне d, що задовольняє умову $m(3,d) \leqslant |V(I)|$, дорівнює 1.

Побудуємо матрицю $M_{f_I,1}$:

$$M_{f_I,1} = \begin{pmatrix} 1|_{(0,0,0)} & x_1|_{(0,0,0)} & x_2|_{(0,0,0)} & x_3|_{(0,0,0)} \\ 1|_{(0,1,1)} & x_1|_{(0,1,1)} & x_2|_{(0,1,1)} & x_3|_{(0,1,1)} \\ 1|_{(1,0,1)} & x_1|_{(1,0,1)} & x_2|_{(1,0,1)} & x_3|_{(1,0,1)} \\ 1|_{(1,1,1)} & x_1|_{(1,1,1)} & x_2|_{(1,1,1)} & x_3|_{(1,1,1)} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

Використовуючи алгоритм Гауса, знайдемо, що $\operatorname{rank}(M_{I,d}) = 4$. Отже, $\operatorname{mindeg} I = 2$.

2.9 Атака Куртуа-Майєра та алгебраїчна імунність булевих функцій

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

Розглянемо генератор, функціонування якого описується системою рівнянь

$$f(xL_i) = \gamma_i, \quad i = 0, 1, 2, \ldots, \tag{2.18}$$

де $x \in V_n$ – невідомий початковий стан генератора, $f \in B_n$ – відома булева функція, L_i – відома матриця розміру $n \times n$ над полем з двох елементів, $i = 0, 1, 2, \ldots$ (Як приклади генераторів, що описуються системами рівнянь вигляду (2.18), відзначимо фільтрувальний та комбінувальний генератори гами; див. рис. 1.7).

Припустимо, що виконується хоча б одна з двох наступних умов:

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

2) існує ненульова функція $h \in \operatorname{Ann}(f \oplus 1)$ 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 (2.18) 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, $\alpha \in V_n$.

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 $O(t \cdot N_d^2)$ двійкових операцій, де $t \geqslant N_d$ позначає кількість рівнянь у системі. Таким чином, виграш у часовій складності атаки Куртуа-Майєра в порівнянні зі «звичайною» атакою, що полягає у розв'язанні вхідної системи (2.18) методом введення нових змінних, є величиною порядку $(N_D/N_d)^3$, де $D = \deg f$.

Описана атака є підставою для введення такого важливого поняття.

Означення 2.10. Число

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

називається *алгебраїчною імунністю* функції $f \in B_n$.

Зауважимо, що для обчислення алгебраїчної імунності можна безпосередньо використовувати результати п. 2.8. Окрім того, на підставі твердження 2.2 справедлива рівність

$$\mathrm{AI}(f) = \min\{\deg g : \ g \in (\langle f\rangle \cup \langle f \oplus 1\rangle)\backslash\{0\}\}.$$

Наведемо верхню оцінку алгебраїчної імунності.

Твердження 2.12. *Для будь-якої функції $f \in B_n$ виконується нерівність*

$$\mathrm{AI}\,(f) \leqslant \left\lceil \frac{n}{2} \right\rceil.$$

Доведення. Позначимо $||f||$ вагу функції f, тобто кількість одиниць у векторі її значень. З функцій f та $f \oplus 1$ виберемо ту, вага якої не перевищує 2^{n-1}. Не обмежуючи загальності, припустимо, що це є функція f.

Розглянемо матрицю M, рядки якої занумеровані векторами $x \in V_n$ такими, що $f(x) = 1$ (їхня кількість дорівнює $||f||$), а стовпці – мономами степенів $0, 1, \ldots, \left\lceil \frac{n}{2} \right\rceil$(їхня кількість дорівнює $\sum\limits_{i=0}^{\left\lceil \frac{n}{2} \right\rceil} \binom{n}{i} > 2^{n-1} \geqslant ||f||$); на перетині рядка та стовпця запишемо значення монома у точці x.

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 $\deg g \leqslant \left\lceil \frac{n}{2} \right\rceil$. Ця функція обертається в нуль на усіх векторах $x \in V_n$ таких, що $f(x) = 1$, тобто задовольняє умову $g \in \mathrm{Ann}\,(f)$. $\square$

Приклад 2.9. 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 надає змогу побудувати на шифр алгебраїчну атаку, помітно ефективнішу за тривіальну (див. [CM]).

На завершення цього пункту розглянемо поняття алгебраїчної імунності для булевих вектор-функцій. На даний час є декілька варіантів означення цього поняття, серед яких найбільш адекватним з практичного погляду видається означення Арса-Фожера [AF].

Розглянемо довільну вектор-функцію $s = (s_1, \ldots, s_m)$, де $s_i : V_n \to \{0,1\}$, $i \in \overline{1,m}$. Позначимо I_s ідеал кільця булевих функцій від $n+m$ змінних $x = (x_1, \ldots, x_n) \in V_n$ та $y = (y_1, \ldots, y_m) \in V_m$, породжений функціями $y_1 \oplus s_1(x), \ldots, y_m \oplus s_m(x)$.

Означення 2.11. *Алгебраїчною імунністю вектор-функції* s називається число

$$\mathrm{AI}'(s) = \mathrm{mindeg}\, I_s.$$

Як випливає з твердження 2.1, алгебраїчна імунність вектор-функції s дорівнює мінімуму степенів усіх ненульових функцій $g \in B_{m+n}$, що задовольняють умову:

$$\forall x \in V_n, y \in V_m : s(x) = y \Rightarrow g(x,y) = 0.$$

Іншими словами, число $\mathrm{AI}'(s)$ є найменшим степенем рівнянь вигляду $g(x,y) = 0$, які є наслідками рівняння $s(x) = y$. Таке означення алгебраїчної імунності вектор-функції є найбільш корисним для

випадку $m = n$, хоча воно має сенс і для звичайних булевих функцій (коли $m = 1$). Стосовно того, як співвідносяться в останньому випадку параметри $\mathrm{AI}(s)$ та $\mathrm{AI}'(s)$, див. задачу 2.29.

2.10 Алгебраїчна атака на спрощену версію SNOW 2.0-подібного потокового шифру

Як приклад, що ілюструє практичне застосування окремих понять і результатів, наведених вище, розглянемо алгебраїчну атаку на спрощену версію `SNOW 2.0`-подібного потокового шифру.

Зафіксуємо цілі числа $p, t \geqslant 2$, позначимо $r = pt$ і задамо на множині V_r структуру поля $\mathbb{F}_{2^r}$ (порядку 2^r), узгоджену з операцією $\oplus$ покоординатного булевого додавання двійкових векторів. Зафіксуємо базис $\mathfrak{B}_1$ поля $\mathbb{F}_{2^t} \subset \mathbb{F}_{2^r}$ над полем $\mathbb{F}_2$, базис $\mathfrak{B}_2$ поля $\mathbb{F}_{2^r}$ над підполем $\mathbb{F}_{2^t}$ і позначимо $\mathfrak{B}$ базис поля $\mathbb{F}_{2^r}$ над підполем $\mathbb{F}_2$, який складається з усіх добутків елементів $b_1 \in \mathfrak{B}_1$ та $b_2 \in \mathfrak{B}_2$. Надалі ототожнюватимемо елементи полів $\mathbb{F}_{2^t}$ та $\mathbb{F}_{2^r}$ з векторами їхніх координат у базисах $\mathfrak{B}_1$ та $\mathfrak{B}$ відповідно.

Окрім того, ототожнимо елементи множини V_r з r-розрядними цілими числами, вважаючи, що вектору $x = (x_1, x_2, \ldots, x_r) \in V_r$ відповідає число $2^{r-1}x_1 + 2^{r-2}x_2 + \ldots + x_r$, та позначимо символом $\overset{r}{+}$ операцію додавання цих чисел за модулем 2^r.

Вхідними даними для побудови генератора гами `SNOW 2.0`-подібного потокового шифру (рис. 2.2) є такі об'єкти:

– примітивний поліном $g(z) = z^n \oplus c_{n-1}z^{n-1} \oplus \ldots \oplus c_0$ над полем $\mathbb{F}_{2^r}$;

– число $\mu \in \overline{1, n-2}$;

– підстановки $s_j : V_t \to V_t$, $j \in \overline{0, p-1}$;

– оборотна $p \times p$-матриця D над полем $\mathbb{F}_{2^t}$.

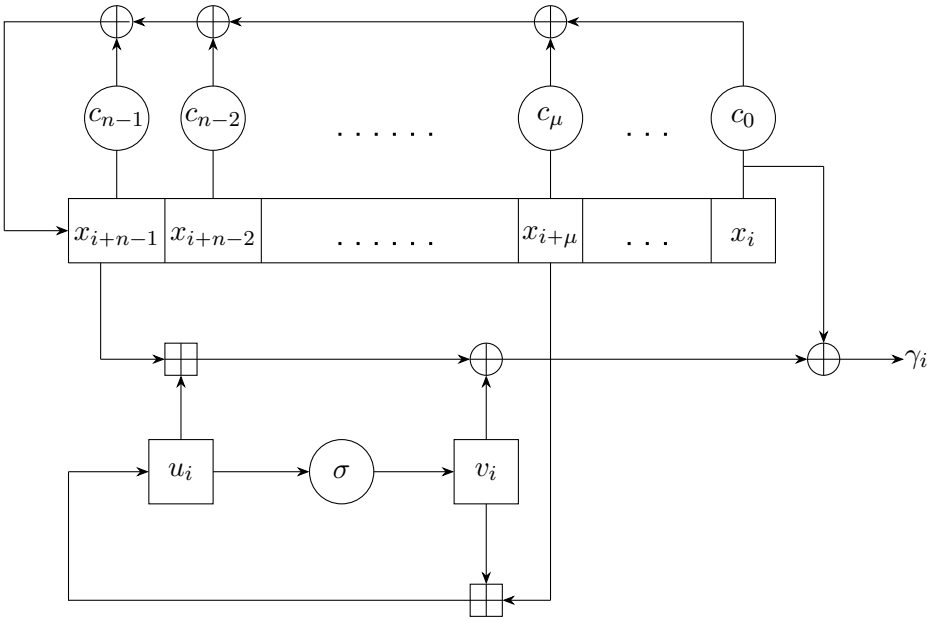

Рис. 2.2: Схема генератора гами SNOW 2.0-подібного потокового шифру

Задамо підстановку $\sigma : V_r \to V_r$, вважаючи

$$\sigma(u) = (s_0(u^{(0)}), \ldots, s_{p-1}(u^{(p-1)}))D, \tag{2.19}$$

де $u = (u^{(0)}, \ldots, u^{(p-1)}) \in V_r = V_t^p$ та кожен двійковий вектор $s_j(u^{(j)})$ ототожнюється зазначеним вище чином з елементом поля $\mathbb{F}_{2^t}$, $j \in \overline{0, p-1}$, а множення рядка $(s_0(u^{(0)}), \ldots, s_{p-1}(u^{(p-1)}))$ на матрицю D здійснюється над цим полем.

Генератор гами SNOW 2.0-подібного шифру визначається як скінченний автономний автомат з множиною внутрішніх станів $V_r^n \times V_r^2$, функцією переходів

$$h((x_{n-1}, x_{n-2}, \ldots, x_0), u, v) = ((x_n, x_{n-1}, \ldots, x_0), x_\mu \overset{r}{+} v, \sigma(u))$$

та функцією виходів

$$f((x_{n-1}, x_{n-2}, \ldots, x_0), u, v) = x_0 \oplus (x_{n-1} \overset{r}{+} u) \oplus v,$$

де $x_0, \ldots, x_{n-1}$, u, $v \in V_r$, $x_n = c_{n-1}x_{n-1} \oplus \ldots \oplus c_0 x_0$. Знак гами в i-ому такті визначається за початковим станом $((x_{n-1}, x_{n-2}, \ldots, x_0), u_0, v_0)$ генератора за допомогою рекурентних співвідношень

$$\gamma_i = x_i \oplus (x_{i+n-1} \overset{r}{+} u_i) \oplus v_i, \tag{2.20}$$

$$u_{i+1} = x_{i+\mu} \overset{r}{+} v_i, \ v_{i+1} = \sigma(u_i), \tag{2.21}$$

$$x_{n+i} = c_{n-1}x_{n-1+i} \oplus \ldots \oplus c_0 x_i, \tag{2.22}$$

які мають місце для усіх $i = 0, 1, \ldots$.

Приклад 2.10. В алгоритмі шифрування SNOW 2.0 використовуються такі параметри: $t = 8$, $p = 4$ ($r = 32$). При цьому $n = 16$, $\mu = 5$, а підстановки s_j, $j \in \overline{0, p-1}$, та матриця D задаються так само, як у раундовому перетворенні блокового шифру Rijndael.

Потоковий шифр Струмок [ДСТУ1] є SNOW 2.0-подібним шифром з параметрами $t = 8$, $p = 8$ ($r = 64$). При цьому $n = 16$, $\mu = 13$, а підстановки s_j, $j \in \overline{0, p-1}$, та матриця D визначаються так само, як в алгоритмі шифрування Калина [ДСТУ2].

В [BillG] запропоновано алгебраїчну атаку на шифр SNOW 2.0, яка, в принципі, є застосовною до будь-якого SNOW 2.0-подібного шифру. Для того, щоби проілюструвати основну ідею цієї атаки, не ускладнюючи викладення, розглянемо спрощену версію генератора гами на рис. 2.2, яка відрізняється від оригіналу застосуванням операції $\oplus$ замість операції $\overset{r}{+}$. У цьому випадку рівняння (2.20), (2.21) спрощуються і приймають такий вигляд:

$$\gamma_i = x_i \oplus x_{i+n-1} \oplus u_i \oplus v_i, \tag{2.23}$$

$$u_{i+1} = x_{i+\mu} \oplus v_i, \;\; v_{i+1} = \sigma(u_i), \tag{2.24}$$

де $i = 0, 1, \ldots$. Отже, далі вважатимемо, що генератор функціонує за законом, що описується рівняннями (2.22) – (2.24). При цьому метою алгебраїчної атаки є відновлення значень $x_0, x_1, \ldots, x_{n-1}, v_0$ за відомою гамою.

Атака складається з двох етапів, на першому з яких формується певна система булевих рівнянь, що описує підстановку σ вигляду (2.19). Потім, на другому етапі будуються лінійні рівняння, які пов'язують змінні v_i та u_{i-1} з невідомими $x_0, x_1, \ldots, x_{n-1}, v_0$, а також знаками гами, $i = 1, 2, \ldots$. Далі отримана система рівнянь розв'язується одним з відомих методів (наприклад, шляхом введення нових змінних).

Побудова рівнянь на першому етапі здійснюється таким чином. Спочатку для кожної підстановки $s_j : V_t \to V_t$, $j \in \overline{0, p-1}$, будується максимальна лінійно незалежна система булевих функцій $g_{j,l}$, $l \in \overline{1, n_j}$, від $2t$ змінних, які мають найменший степінь серед усіх функцій $g \in B_{2t}$, що задовольняють умову

$$\forall\; u^{(j)}, w^{(j)} \in V_t : s_j(u^{(j)}) = w^{(j)} \Rightarrow g(u^{(j)}, w^{(j)}) = 0. \tag{2.25}$$

Зауважимо, що в силу означення 2.11 степінь кожної функції $g_{j,l}$ дорівнює числу $\mathrm{AI}'(s_j)$. При цьому для знаходження цих функцій можна скористатися теоремою 2.4, згідно з якою їхня кількість n_j дорівнює числу поліномів степеня $\mathrm{AI}'(s_j)$ у мінімальному базисі Грьобнера ідеалу, який відповідає підстановці s_j, $j \in \overline{0, p-1}$.

Далі, використовуючи формули (2.19), (2.25), отримаємо, що для будь-яких $u^{(j)}, v^{(j)} \in V_t$, $j \in \overline{0, p-1}$, справедливі такі співвідношення:

$$\sigma((u^{(0)}, \ldots, u^{(p-1)})) = (v^{(0)}, \ldots, v^{(p-1)}) \Leftrightarrow$$

$$\Leftrightarrow (s_0(u^{(0)}), \ldots, s_{p-1}(u^{(p-1)})) = (v^{(0)}, \ldots, v^{(p-1)})D^{-1} =$$

$$= (vD^{(0)}, \ldots, vD^{(p)}) \Rightarrow (g_{j,l}(u^{(j)}, vD^{(j)}) = 0,\ l \in \overline{1, n_j}, j \in \overline{0, p-1}),$$

де $v = (v^{(0)}, \ldots, v^{(p-1)})$, $D^{(j)}$ – j-й стовпець матриці D^{-1}, а $vD^{(j)}$ позначає набір координат у базисі $\mathfrak{B}_1$ скалярного добутку зазначених векторів над полем $\mathbb{F}_{2^t}$, $j \in \overline{0, p-1}$. Звідси отримаємо систему рівнянь

$$g_{j,l}(u^{(j)}, vD^{(j)}) = 0,\ l \in \overline{1, n_j}, j \in \overline{0, p-1}, \tag{2.26}$$

яка формується на першому етапі атаки та виконується для усіх наборів $u = (u^{(0)}, \ldots, u^{(p-1)})$, $v = (v^{(0)}, \ldots, v^{(p-1)}) \in V_t^p$ таких, що $\sigma(u) = v$.

На другому етапі атаки, використовуючи рівності (2.23), (2.24), отримаємо, що

$$v_i = \gamma_i \oplus v_{i-1} \oplus x_i \oplus x_{i+n-1} \oplus x_{i+\mu-1},$$

$$v_{i-1} = \gamma_{i-1} \oplus v_{i-2} \oplus x_{i-1} \oplus x_{i+n-2} \oplus x_{i+\mu-2},$$

$$\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots$$

$$v_1 = \gamma_1 \oplus v_0 \oplus x_0 \oplus x_{n-1} \oplus x_{\mu-1}.$$

На підставі формули (2.22) кожен елемент x_k, $k = 0, 1, \ldots$, є лінійною комбінацією над полем $\mathbb{F}_{2^r}$ елементів $x_0, \ldots, x_{n-1}$. Отже, підсумовуючи наведені рівняння, отримаємо, що

$$v_i = v_0 \oplus (\gamma_i \oplus \gamma_{i-1} \oplus \ldots \oplus \gamma_1) \oplus L_i(x_0, \ldots, x_{n-1}),$$

де L_i – деяка лінійна над полем $\mathbb{F}_{2^r}$ функція, $i = 1, 2, \ldots$.

Таким чином, існує афінна (над полем $\mathbb{F}_{2^r}$) функція A_i від $n+1$ змінних така, що

$$v_i = A_i(v_0, x_0, \ldots, x_{n-1}),\ i = 1, 2, \ldots. \tag{2.27}$$

Далі, використовуючи перше рівняння (2.24) та формулу (2.27) отримаємо, що $u_{i-1} = x_{i+\mu-2} \oplus v_{i-2} = x_{i+\mu-2} \oplus A_{i-2}(v_0, x_0, \ldots, x_{n-1})$. Отже, існує афінна (над полем $\mathbb{F}_{2^r}$) функція $\widetilde{A}_i$ від $n+1$ змінних така, що

$$u_{i-1} = \widetilde{A}_i(v_0, x_0, \ldots, x_{n-1}),\ i = 1, 2, \ldots. \tag{2.28}$$

Нарешті, використовуючи рівність $\sigma(u_{i-1}) = v_i$, яка випливає з другого рівняння (2.24), підставимо отримані співвідношення (2.27), (2.28) в систему рівнянь (2.26), вважаючи $u = (u^{(0)}, \ldots, u^{(p-1)}) = u_{i-1}$, $v = (v^{(0)}, \ldots, v^{(p-1)}) = v_i$ (та використовуючи базис $\mathfrak{B}$ для переходу від елементів поля $\mathbb{F}_{2^r}$ до двійкових векторів). Таким чином, маючи l знаків гами $\gamma_1, \ldots, \gamma_l$, сформуємо кінцеву систему, яка складається з $T = l \sum\limits_{j=0}^{p-1} n_j$ булевих рівнянь від $m = r(n+1)$ змінних – координат двійкових векторів $x_0, x_1, \ldots, x_{n-1}, v_0$. Зауважимо, що внаслідок афінності функцій A_i, $\widetilde{A}_i$ у правих частинах рівностей (2.27), (2.28), а також лінійності функції $vD^{(j)}$ (від аргументу v при фіксованому векторі $D^{(j)}$) у формулі (2.26) степінь кожного рівняння отриманої системи не перевищує числа $\Theta = \max\{\mathrm{AI}'(s_j) : j \in \overline{0, p-1}\}$.

Таким чином, за умови $T \geqslant \sum\limits_{i=1}^{\Theta} \binom{m}{i}$ складність розв'язання отриманої системи рівнянь методом введення нових змінних становить $O\left(T\left(\sum\limits_{i=1}^{\Theta} \binom{m}{i}\right)^2\right)$ двійкових операцій.

Приклад 2.11. В алгоритмі шифрування `SNOW 2.0` усі підстановки s_j співпадають; при цьому $\mathrm{AI}'(s_j) = 2$, $n_j = 39$ для кожного $j \in \overline{0, p-1}$, де $p = 4$. Отже, розглянута алгебраїчна атака на спрощену версію цього шифру полягає у розв'язанні системи, що складається зі $156l$ булевих рівнянь другого степеня від $32 \cdot 17 = 644$ невідомих, де l – довжина доступного відрізку гами.

В алгоритмі `Струмок` використовується 4 різні підстановки s_j, причому $\mathrm{AI}'(s_j) = 3$, $n_j = 441$ для кожного $j \in \overline{0, p-1}$, де $p = 8$. Отже, атака на спрощену версію цього шифру полягає у розв'язанні системи, яка складається з $3528l$ булевих рівнянь третього степеня від 1288 невідомих.

Задачі до розділу 2

Задача 2.1. Доведіть, що для будь-яких ідеалів I_1, I_2 кільця B_n справедливі рівності

$$V(I_1 \cap I_2) = V(I_1) \cup V(I_2),\ V(I_1 \cup I_2) = V(I_1) \cap V(I_2).$$

Задача 2.2. Нехай $f \in B_n$. Доведіть, що $|\operatorname{Ann}(f)| = 2^{2^n - ||f||}$, де $||f||$ – вага функції f.

Задача 2.3. Нехай $n \geqslant 3$, $f \in B_n$ і

$$\langle f \rangle = \langle x_1 \oplus x_2, x_2 \oplus x_3, \ldots, x_{n-1} \oplus x_n \rangle.$$

Доведіть, що $\deg f = n - 1$.

Задача 2.4. Нехай I – ідеал кільця B_n. Обчисліть $|I|$, якщо

а) n є парним числом та $I = \langle x_1x_2, x_3x_4, \ldots, x_nx_{n-1} \rangle$;

б) $n \geqslant 2$ та $I = \langle x_1x_2, x_1x_2x_3, \ldots, x_1x_2 \ldots x_n \rangle$.

Задача 2.5. Переконайтесь, що відношення лексикографічного порядку $\preceq_{\text{lex}}$ на множині $\mathbb{N}_0^n$ є мономіальним впорядкуванням.

Задача 2.6. Нехай $\preceq$ – мономіальне впорядкування на множині $\mathbb{N}_0^n$. Доведіть, що відношення $\preceq_{\text{rev}}$, яке визначається за правилом

$$\forall(\alpha_1, \ldots, \alpha_n), (\beta_1, \ldots, \beta_n) \in \mathbb{N}_0^n :$$
$$(\alpha_1, \ldots, \alpha_n) \preceq_{\text{rev}} (\beta_1, \ldots, \beta_n) \Leftrightarrow (\alpha_n, \ldots, \alpha_1) \preceq (\beta_n, \ldots, \beta_1)$$

також є мономіальним впорядкуванням.

Задача 2.7. Доведіть наступне твердження. Нехай $\preceq$ – мономіальне впорядкування на множині $\mathbb{N}_0^n$. Тоді відношення $\preceq_{\deg}$, що ви-

значається за правилом

$$\alpha \preceq_{\deg} \beta \Leftrightarrow (|\alpha| < |\beta| \text{ або } (|\alpha| = |\beta| \text{ та } \alpha \preceq \beta)),$$

є степеневим мономіальним впорядкуванням на $\mathbb{N}_0^n$.

Задача 2.8. Переконайтесь, що відношення степеневого зворотного лексикографічного порядку $\preceq_{\mathrm{drl}}$ є мономіальним впорядкуванням на множині $\mathbb{N}_0^n$.

Задача 2.9. Нехай A – матриця з дійсними елементами розміру $n \times k$ і рангу n, найперший (зліва) елемент кожного рядку якої є додатним числом. Доведіть, що відношення $\preceq$ на множині $\mathbb{N}_0^n$ таке, що $\alpha \preceq \beta \Leftrightarrow \alpha A \preceq_{\mathrm{lex}} \beta A$, $\alpha, \beta \in \mathbb{N}_0^n$, є мономіальним впорядкуванням. (Зауважимо, що будь-яке мономіальне впорядкування може бути визначено наведеним чином; див., наприклад, [OZ]).

Задача 2.10. Нехай $\preceq$ є лінійним впорядкування на множині V_n з найменшим елементом 0, яке задовольняє умову

$$\forall \alpha, \beta, \gamma \in V_n : (\alpha \preceq \beta, \beta \wedge \gamma = 0) \Rightarrow (\alpha \vee \gamma \preceq \beta \vee \gamma).$$

Доведіть, що для будь-яких $\alpha_1, \alpha_2, \beta_1, \beta_2 \in V_n$ справедлива імплікація

$$(\alpha_1 \preceq \beta_1, \alpha_2 \preceq \beta_2, \beta_1 \wedge \beta_2 = 0) \Rightarrow (\alpha_1 \vee \alpha_2 \preceq \beta_1 \vee \beta_2).$$

(Символи $\wedge$ та $\vee$ позначають відповідно покоординатну кон'юнкцію та покоординатну диз'юнкцію двійкових векторів).

Задача 2.11. Нехай $M_k = \{\alpha \in V_n : ||\alpha|| \geqslant k\}$, $0 \leqslant k \leqslant n$. Переконайтесь, що множина M_k є монотонним класом. Знайдіть мінімальну систему твірних мономіального ідеалу J_k, який відповідає цьому монотонному класу, та обчисліть значення $|J_k|$.

Задача 2.12. Нехай $f = x_1 \oplus x_2 \oplus x_1x_2 \oplus x_1x_3$ та $f, f_1, f_2, f_3 \in B_3$. Обчисліть $\mathrm{Res}\,(f; f_1, f_2, f_3)$, якщо

а) $f_1 = x_1 \oplus 1$, $f_2 = x_2$, $f_3 = x_1x_2$;

б) $f_1 = x_2 \oplus 1$, $f_2 = x_2x_3$, $f_3 = x_1x_2x_3$.

Задача 2.13. Доведіть, що число елементів у мінімальному базисі Грьобнера будь-якого ідеалу кільця B_n не перевищує $\binom{n}{\lfloor \frac{n}{2} \rfloor}$. Чи є досяжною зазначена межа?

Задача 2.14. Нехай $g_1, \ldots, g_m$ є базисом Грьобнера ідеалу $I = \langle g_1, \ldots, g_m \rangle$. Доведіть, що множина $\{\mathrm{Res}(f; g_1, \ldots, g_m) : \ f \in B_n\}$ є підпростором вимірності $|V(I)|$ векторного простору B_n.

Задача 2.15. Нехай $f \in B_n \backslash \{0\}$, $I = \langle f \rangle$. Доведіть, що функція f утворює базис Грьобнера ідеалу I тоді й тільки тоді, коли $\mathrm{Res}(x_i f; f) = 0$ для будь-якої змінної x_i, яка міститься у виразі старшого монома полінома f.

Задача 2.16. Нехай поліном f утворює базис Грьобнера ідеалу $I = \langle f \rangle$ відносно мономіального впорядкування $\preceq$. Доведіть, що $\mathrm{LM}_{\preceq}(f)$ є найменшим відносно $\preceq$ елементом множини $\{\mathrm{LM}_{\preceq}(g) |\ g \in I \backslash \{0\}\}$. Чи є правильним обернене твердження?

Задача 2.17. Обчисліть мінімальний базис Грьобнера ідеалу $I = \langle f \rangle$, якщо

а) $\preceq = \preceq_{\mathrm{lex}}$, $f(x_1, x_2, x_3) = x_1 \oplus x_2x_3$;

б) $\preceq = \preceq_{\mathrm{lex}}$, $f(x_1, x_2, x_3) = x_1 \oplus x_1x_2x_3$;

в) $\preceq = \preceq_{\mathrm{drl}}$, $f(x_1, x_2, x_3) = x_1 \oplus x_2x_3$;

г) $\preceq = \preceq_{\mathrm{drl}}$, $f(x_1, x_2, x_3) = x_1 \oplus x_1x_2x_3$.

Задача 2.18. Чи існує мономіальне впорядкування на множині $\mathbb{N}_0^n$, для якого ідеал, породжений функціями $x_1 \oplus a_1, \ldots, x_n \oplus a_n$, де $(a_1, \ldots, a_n) \in V_n$, має декілька мінімальних базисів Грьобнера?

Задача 2.19. Нехай $f_i(x_1, \ldots, x_n) = 0$, $i \in \overline{1, m}$ – система булевих рівнянь така, що $f_i(0, \ldots, 0) = 0$ для кожного $i \in \overline{1, m}$. Доведіть, що ця система має єдиний ненульовий розв'язок $(a_1, \ldots, a_n) \in V_n$ тоді й тільки тоді, коли редукований базис Грьобнера ідеалу $\langle f_1, \ldots, f_m \rangle$ складається з $n - 1$ функцій

$$g_i = \begin{cases} x_i \oplus x_{i_0}, & \text{якщо } a_i = 1; \\ x_i, & \text{якщо } a_i = 0, \end{cases}$$

де $i \in \overline{1, n} \backslash \{i_0\}$, а i_0 – таке число від 1 до n, що

$$x_{i_0} = \min\nolimits_{\preceq} \{x_i : a_i = 1, i \in \overline{1, n}\}.$$

Задача 2.20. Нехай $f, g \in B_n$, причому існують невироджена булева $n \times n$-матриця A і вектор $b \in V_n$ такі, що $g(x) = f(xA \oplus b)$, $x \in V_n$. Доведіть, що $\operatorname{mindeg} \langle f \rangle = \operatorname{mindeg} \langle g \rangle$.

Задача 2.21. Нехай $f \in B_n$, $\operatorname{mindeg} \operatorname{Ann}(f) = d$ та D_f – кількість функцій степеня d, які містяться в ідеалі $\operatorname{Ann}(f)$. Доведіть такі твердження:

а) $D_f \leqslant 2^{\binom{n}{d}}$;

б) якщо n є парним числом, f – збалансованою функцією та $d = n/2$, то $D_f \geqslant 2^{1/2 \cdot \binom{n}{n/2}}$;

в) якщо n є непарним число, f – збалансованою функцією та $d = \lceil n/2 \rceil$, то $D_f = 2^{\binom{n}{\lceil n/2 \rceil}}$.

Задача 2.22. Нехай $f, g \in B_n$. Доведіть, що

$$\mathrm{AI}(f \oplus g) \leqslant \mathrm{AI}(f) + \mathrm{AI}(g).$$

Задача 2.23. Нехай $f \in B_n$, $\mathrm{AI}(f) = d$ та g – афінна булева функція від n змінних. Доведіть, що $d - 1 \leqslant \mathrm{AI}(f \oplus g) \leqslant d + 1$.

Задача 2.24. Нехай $f_1, f_2 \in B_n$, $\mathrm{AI}(f_1) = d_1$, $\mathrm{AI}(f_2) = d_2$ та

$$f(x_1, \ldots, x_n, x_{n+1}) = x_{n+1} f_1(x_1, \ldots, x_n) \oplus (x_{n+1} \oplus 1) f_2(x_1, \ldots, x_n).$$

Доведіть, що $\mathrm{AI}(f) \leqslant \min\{d_1, d_2\} + 1$.

Задача 2.25. Нехай $f \in B_n$, $\mathrm{AI}(f) = d$. Доведіть, що

$$\sum_{i=0}^{d-1} \binom{n}{i} \leqslant ||f|| \leqslant \sum_{i=0}^{n-d} \binom{n}{i}.$$

Задача 2.26. Нехай n – непарне число,

$$f(x) = \begin{cases} 1, & \text{якщо } ||x|| \geqslant \left\lceil \frac{n}{2} \right\rceil; \\ 0, & \text{якщо } ||x|| < \left\lceil \frac{n}{2} \right\rceil, x \in V_n. \end{cases}$$

Доведіть, що $\mathrm{AI}(f) = \left\lceil \frac{n}{2} \right\rceil$.

Задача 2.27. Нехай n – непарне число, $f \in B_n$ та $\mathrm{AI}(f) = \left\lceil \frac{n}{2} \right\rceil$. Доведіть, що f є збалансованою функцією.

Задача 2.28. 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) $f(x_1, x_2, x_3) = x_2 \oplus x_1x_2 \oplus x_1x_3$;

в) $f(x_1, x_2, x_3, x_4) = x_1 \oplus x_1x_2x_3 \oplus x_2x_3x_4$;

г) $f(x_1, x_2, x_3, x_4) = x_1 \oplus x_2 \oplus x_3 \oplus x_1x_4 \oplus x_1x_2x_3$.

Задача 2.29. Нехай $f \in B_n$, I – ідеал кільця булевих функцій від $n+1$ змінних $x \in V_n, y \in \{0,1\}$, породжений функцією $y \oplus f(x)$. Доведіть, що число $\mathrm{AI}(f)$ співпадає з мінімумом степенів за набором змінних x усіх ненульових функцій, які належать цьому ідеалу. Отримайте звідси нерівність, що пов'язує параметри $\mathrm{AI}(f)$ та $\mathrm{AI}'(f)$.

Задача 2.30. Доведіть, що для будь-якої вектор-функції $s : V_8 \to V_8$ виконується нерівність $\mathrm{AI}'(s) \leqslant 3$. За якої умови досягається рівність?

3 Елементи статистичного криптоаналізу

Зазвичай статистичними називають атаки, які базуються на розв'язанні задач статистичної класифікації (або перевірки декількох статистичних гіпотез). Основним етапом при побудові таких атак є розробка ймовірнісної моделі, яка описує функціонування алгоритму шифрування або генератора гами. Ця модель повинна бути достатньо простою для того, щоб на її основі можна було розв'язувати криптоаналітичні задачі, а також достатньо адекватною для того, щоб зберегти найсуттєвіші риси процесу функціонування алгоритму шифрування (генератора гами). Тому при розробці статистичних атак часто-густо роблять так звані стандартні криптографічні припущення, які приймаються де факто, хоча формально вони можуть і не виконуватися. Приклади таких припущень можна знайти в описах атак, наведених в цьому розділі.

Окремий клас статистичних атак утворюють кореляційні атаки, що базуються на можливості статистичного наближення складного об'єкта (наприклад, булевої функції від великої кількості змінних) більш просто збудованим об'єктом (функцією від малої кількості змінних або афінною функцією). Найвідоміша атака такого типу належить Зігенталеру [Sie] і розглядається нижче.

Для побудови та аналізу ефективності кореляційних атак широко використовується апарат перетворення Фур'є псевдобулевих функцій, викладенню основ якого присвячено значну частину цього

розділу. Вивчаються також алгоритми розв'язання систем лінійних рівнянь зі спотвореними правими частинами, зокрема, над полями порядку 2^r, де $r \geqslant 2$.

Завершується розділ оглядом швидких алгоритмів знаходження лінійних наближень булевих функцій; ці наближення є необхідними для побудови багатьох кореляційних атак.

3.1 Атака Беббіджа-Голіча

Розглянемо атаку на довільний генератор гами, яка базується на методі балансування (time-memory-data trade off), запропоновану незалежно С. Беббіджем [Bab] та Й. Голічем [Gol]. Зауважимо, що цю атаку можна віднести до статистичних лише з певною часткою умовності. Проте вона є дуже важливою для обґрунтування загального співвідношення між довжинами ключа та початкового стану генератора гами, а її аналіз базується на ймовірнісних міркуваннях.

Атака будується на основі відомих відкритих повідомлень: 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 відрізок, 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 відрізки гами $f(s_1), \ldots, f(s_M)$. Далі він формує таблицю, яка складається зі слів $(s_i, f(s_i))$, $i \in \overline{1, M}$, впорядкованих за другою компонентою (інакше кажучи, слова в таблиці записуються в порядку неспадання

значень $f(s_i)$, $i \in \overline{1, M}$, відносно лексикографічного впорядкування на множині V_n).

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

Нехай, не обмежуючи загальності міркувань, $\gamma_1, \ldots, \gamma_D \in V_n$. 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 відрізок 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 міститься 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 відрізків гами.

Таким чином, справедливі такі співвідношення:

$$1 \leqslant T \leqslant D, \quad P = O(M). \tag{3.1}$$

З'ясуємо, як вибрати значення M для відомих $N = 2^n$ 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

$$\Pr\left(f(s_1), \ldots, f(s_M) = a_1, \ldots, a_M, \gamma_1, \ldots, \gamma_D = b_1, \ldots, b_D\right) =$$

$$= \frac{1}{(N)_M (N)_D},$$

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

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

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

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

$$> 1 - \left(1 - \frac{M}{N}\right)^D \geqslant 1 - e^{-\frac{MD}{N}}, \tag{3.2}$$

де останнє співвідношення випливає з відомої нерівності

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

Отже, на підставі формули (3.2) за умови

$$M = C \cdot \frac{N}{D}, \quad C = const \geqslant 1, \tag{3.3}$$

ймовірність успішного завершення атаки становить

$$\pi_n(M, D) \geqslant 1 - e^{-C} \tag{3.4}$$

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

Таким чином, на підставі формул (3.1), (3.3) мають місце такі співвідношення, що пов'язують основні характеристики ефективності описаної атаки:

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

Зокрема, вважаючи $D = N^{1/2}$, $M = C \cdot N^{1/2}$, де $C \geqslant 1$, отримаємо, що трудомісткість атаки складає $T = O(N^{1/2})$. При цьому ймовірність її успіху оцінюється знизу за формулою (3.4), 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 операцій необхідно, щоб довжина початкового стану генератора гами цього шифру складала не менш ніж*

$2l$ бітів. Зокрема, довжина початкового стану потокового шифру має бути принаймні вдвічі більше за довжину його ключа.

3.2 Статистична атака на фільтрувальний генератор гами з лінійним законом формування початкового стану та функцією ускладнення, близькою до алгебраїчно виродженої

Розглянемо генератор гами, функціонування якого в режимі реініціалізації початкового стану описується такою системою рівнянь:

$$x^{(j)} = kA \oplus c^{(j)}B,\ f(x^{(j)}L^iP) = \gamma_i^{(j)},\ i \in \overline{0, T-1}, j \in \overline{1, r}. \qquad (3.5)$$

В цій формулі:

- $x^{(j)} \in V_N$ – початковий стан генератора, що формується за ключем $k \in V_{l_0}$ та вектором ініціалізації $c^{(j)} \in V_{l_1}$ в j-ому запуску;
- A і B – булеві матриці;
- f – функція ускладнення, яка залежить суттєво від n змінних $x_{\mu_1}, \ldots, x_{\mu_n}$, де $0 \leqslant \mu_1 < \ldots < \mu_n \leqslant N-1$;
- P – булева $(N \times n)$-матриця така, що $xP = (x_{\mu_n}, \ldots, x_{\mu_1})$ для будь-якого $x = (x_{N-1}, \ldots, x_0) \in V_N$;
- L – оборотна булева матриця порядку N;
- $\gamma_i^{(j)}$ – знак гами в i-му такті при j-му запуску генератора, $i \in \overline{0, T-1}, j \in \overline{1, r}$.

Необхідно відновити ключ k за відомими значеннями f, P, L, A, B, $\gamma_i^{(j)}$, $c^{(j)}$, $i \in \overline{0, T-1}, j \in \overline{1, r}$.

Типовим прикладом генератора, що розглядається, є фільтрувальний генератор гами, який складається з ЛРЗ довжини N та функції ускладнення f (рис. 3.1).

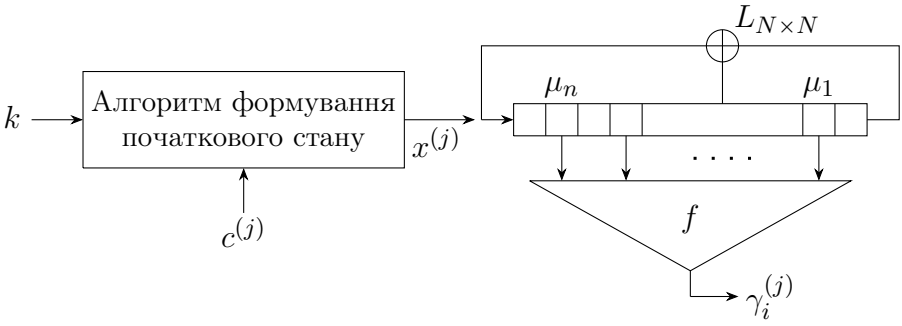

Рис. 3.1: Фільтрувальний генератор гами в режимі реініціалізації початкового стану

Якщо здійснюється r запусків генератора, то в j-му з них за ключем k та вектором ініціалізації $c^{(j)}$ формується початковий стан $x^{(j)}$, після чого генератор виробляє відрізок гами довжини T, причому i-й знак гами в j-му запуску визначається за формулою

$$\gamma_i^{(j)} = f(x^{(j)} L^i P),\ j \in \overline{1, r}, i \in \overline{0, T-1},$$

де L – матриця, що задається поліномом зворотного зв'язку ЛРЗ (див. формулу (1.3)), а P – $(N \times n)$-матриця, яка виділяє з вектора довжини N підвектор довжини n з відповідними координатами.

Вважається, що противнику відомі усі вектори ініціалізації та відповідні їм відрізків гами. Задача противника полягає в тому, щоб відновити ключ k.

Перед тим як описати алгоритм, який за певних умов розв'язує поставлену задачу, розглянемо її окремий випадок.

Припустимо, що число n є настільки малим, що повний перебір усіх двійкових векторів довжини n є практично можливим. Тимчасово позначимо це число символом s. Далі, позначимо $A_i = AL^iP$, $B_i = BL^iP$, $i = 0, 1, \ldots$, та запишемо систему рівнянь (3.5) у вигляді

$$f(kA_i \oplus c^{(j)}B_i) = \gamma_i^{(j)},\ i \in \overline{0, T-1}, j \in \overline{1, r}. \tag{3.6}$$

Припустимо, що функція f не має ненульових *несуттєвих векторів*, тобто таких векторів $a \in V_n \backslash \{0\}$, що рівність $f(x \oplus a) = f(x)$ виконується для усіх $x \in V_s$.

Нехай для деякого $i \in \overline{0, T-1}$ виконується рівність

$$\{c^{(j)}B_i |\ j \in \overline{1, r}\} = V_s.$$

Тоді існує єдиний вектор $y_i \in V_s$ такий, що $f(y_i \oplus c^{(j)}B_i) = \gamma_i^{(j)}$ для усіх $j \in \overline{1, r}$. Цей вектор можна знайти за допомогою повного перебору, причому на підставі формули (3.6) має місце рівність $y_i = kA_i$. Отримавши достатню кількість таких рівностей для декількох значень $i \in \{i_1, i_2, \ldots, i_t\}$, можна відновити ключ k шляхом розв'язання системи лінійних рівнянь

$$k(A_{i_1}, \ldots, A_{i_t}) = (y_{i_1}, \ldots, y_{i_t}). \tag{3.7}$$

(Зауважимо, що ця система має єдиний розв'язок тоді й тільки тоді, коли ранг її матриці коефіцієнтів дорівнює числу l_0).

Оцінимо часову складність наведеного алгоритму відновлення ключа.

Помітимо, що для знаходження кожного вектора y_{i_l}, $l \in \overline{1, t}$, треба перебрати 2^s векторів $y \in V_s$ та перевірити для кожного з них r рівностей $f(y \oplus c^{(j)}B_{i_l}) = \gamma_{i_l}^{(j)}$, $j \in \overline{1, r}$, що потребує $O\left(2^s s l_1 r\right)$ операцій.

Отже, для побудови системи рівнянь (3.7) треба виконати $O\left(2^s tsl_1 r\right)$ операцій. Ще $O\left(stl_0^2\right)$ операцій (за умови $st \geqslant l_0$) потрібно для розв'язання цієї системи рівнянь методом Гаусса. Таким чином, часова складність наведеного алгоритму становить $O\left(2^s tsl_1 r + stl_0^2\right)$ операцій, що за природних припущень $r = O\left(2^s\right)$, $t = O\left(l_0 s^{-1}\right)$ дорівнює $O\left(2^{2s} l_0 l_1 + l_0^3\right)$.

Зауважимо, що описана атака на фільтрувальний генератор гами запропонована в 1993 р. [DGV] та є цілком алгебраїчною. Основним параметром, що визначає її застосовність, є кількість змінних, від яких залежить функція ускладнення генератора. Окрім того, суттєвою умовою, яка надає змогу побудувати таку атаку, є лінійність закону формування початкового стану генератора гами.

Повернемося до загального випадку, в якому функція ускладнення генератора на рис. 3.1 залежить від довільної (не обов'язково малої) кількості змінних, але припустимо, що для цієї функції існує s-вимірне статистичне наближення у сенсі наступних означень.

Означення 3.1. Функція $g : V_n \to \{0,1\}$ називається *s-вимірною*, $s \in \overline{0,n}$, якщо існують функція $\varphi : V_s \to \{0,1\}$ та булева $(n \times s)$-матриця M такі, що $g(x) = \varphi(xM)$ для усіх $x \in V_n$. Булева функція від n змінних, що є s-вимірною для деякого $s < n$, називається *алгебраїчно виродженою*.

Означення 3.2. Функція $g : V_n \to \{0,1\}$ називається *(статистичним) наближенням* (або *статистичним аналогом*) функції $f : V_n \to \{0,1\}$, якщо виконується нерівність $\Pr(f(X) = g(X)) > 1/2$, де X – випадковий рівноймовірний двійковий вектор довжини n.

Зауважимо, що булева функція є s-вимірною тоді й тільки тоді, коли вона лінійно еквівалентна функції, яка суттєво залежить від s або меншої кількості змінних. Зокрема, 0-вимірними функціями є константи 0 та 1, а 1-вимірними – афінні функції. Таким чином, алгебраїчно вироджені функції являють собою узагальнення

як афінних, так і функцій, що залежать від малої кількості змінних. Припустимо, що виконані такі умови.

1. Існує функція $g(x) = \varphi(xM)$, $x \in V_n$ (де $\varphi : V_s \to \{0,1\}$, M – булева матриця розміру $n \times s$) така, що

$$\Pr\left(f(X) = g(X)\right) = p \geqslant 1/2 \cdot (1+\varepsilon),\ \varepsilon \in (0,1). \tag{3.8}$$

Інакше кажучи, для функції f існує s-вимірний статистичний аналог g, який знаходиться від f на відстані (Геммінга) не більш ніж $2^{n-1}(1-\varepsilon)$, де $\varepsilon \in (0,1)$.

2. Існує множина $I = \{i_1, i_2, \ldots, i_t\} \subseteq \overline{0, T-1}$ така, що

$$\operatorname{rank}\left(B_{i_1}\right) = \operatorname{rank}\left(B_{i_2}\right) = \ldots = \operatorname{rank}\left(B_{i_t}\right) = n < l_1 \tag{3.9}$$

та

$$\operatorname{rank}(A_{i_1}M, \ldots, A_{i_t}M) = l_0 \tag{3.10}$$

(нагадаємо, що l_0 та l_1 позначають довжину ключа та довжину вектора ініціалізації відповідно).

Статистична атака на генератор гами, що розглядається, складається з трьох етапів, на першому з яких будується множина I, яка задовольняє умову 2, та обчислюються матриці A_iM, B_iM для кожного $i \in I$.

На другому етапі застосовується метод максимуму правдоподібності. А саме, для кожного $i \in I$ обчислюється значення

$$\nu_i(y) = \sum_{j=1}^{r} \left(\varphi(y \oplus c^{(j)}B_iM) \oplus \gamma_i^{(j)}\right),\ y \in V_s \tag{3.11}$$

та знаходиться вектор $\widehat{y}_i \in V_s$ такий, що $\nu_i(\widehat{y}_i) = \min\limits_{y \in V_s} \nu_i(y)$.

Нарешті, на третьому етапі атаки складається та розв'язується (відносно ключа k) система лінійних рівнянь

$$kA_iM = \widehat{y}_i,\ i \in I. \tag{3.12}$$

Зауважимо, що на підставі рівності (3.10) система рівнянь (3.12) має не більше одного розв'язку. Тому за умови її сумісності ключ відновлюється однозначно.

Для того, щоб оцінити ефективність наведеної атаки, зробимо два додаткових припущення відносно функціонування генератора гами.

Перш за все, припустимо, що вектори ініціалізації $c^{(1)}, c^{(2)}, \ldots, c^{(r)}$ є незалежними випадковими рівноймовірними двійковими векторами довжини l_1.

Далі, для будь-яких $i \in I$, $y \in V_s$ розглянемо події

$$\Omega_i^{(j)}(y) = \{\varphi(y \oplus c^{(j)}B_iM) \oplus \gamma_i^{(j)} = 1\},\ j \in \overline{1,r}.$$

Зауважимо, що ці події є незалежними в сукупності для кожної пари значень $i \in I$, $y \in V_s$. Окрім того, на підставі умови (3.9) випадкові вектори $c^{(j)}B_i$, $j \in \overline{1,r}$, рівномірно розподілені на множині V_n. Звідси на підставі співвідношень (3.6), (3.8) випливає, що при $y = kA_iM$

$$\begin{aligned}\Pr\left(\Omega_i^{(j)}(kA_iM)\right) &= \Pr\left(\varphi(kA_iM \oplus c^{(j)}B_iM) \oplus \gamma_i^{(j)} = 1\right) = \\ &= \Pr\left(g(kA_i \oplus c^{(j)}B_i) \oplus f(kA_i \oplus c^{(j)}B_i) = 1\right) = \\ &= \Pr\left(g(X) \oplus f(X) = 1\right) = 1 - p \leqslant 1/2 \cdot (1 - \varepsilon).\end{aligned}$$

Отже, для будь-яких $i \in I$, $j \in \overline{1,r}$ виконується таке співвідношення:

$$\Pr\left(\Omega_i^{(j)}(kA_iM)\right) \leqslant 1/2 \cdot (1 - \varepsilon). \tag{3.13}$$

Приймемо зараз, як друге припущення стосовно функціонування генератора гами, що

$$\Pr\left(\Omega_i^{(j)}(y)\right) = 1/2 \tag{3.14}$$

для будь-яких $i \in I$, $j \in \overline{1,r}$ та $y \neq kA_iM$.

Зауважимо, що це припущення відноситься до стандартних у статистичному криптоаналізі та означає по суті, що закон розподілу певної випадкової величини при хибному значенні ключа відрізняється від закону її розподілу при істинному значенні.

Сформулюємо важливу лему, яка належить В. Гефдінгу [Hoe] та неодноразово використовується надалі.

Лема 3.1. *Нехай $\zeta_1, \ldots, \zeta_t$ – незалежні випадкові величини такі, що $\alpha_j \leqslant \zeta_j \leqslant \beta_j$, де α_j, β_j – дійсні числа, $j \in \overline{1,t}$. Тоді для будь-якого $x > 0$ має місце нерівність*

$$\Pr\left(\sum_{l=1}^{t}\zeta_l - \sum_{l=1}^{t}\mathbb{E}\zeta_l > tx\right) \leqslant \exp\left\{\frac{-2t^2x^2}{\sum\limits_{l=1}^{t}(\beta_l - \alpha_l)^2}\right\}.$$

Позначимо p_{err} ймовірність помилки описаної атаки, тобто ймовірність події, яка полягає в тому, що атака не відновлює шуканий ключ k.

Лема 3.2. *Нехай виконуються зазначені вище припущення. Тоді справедлива нерівність*

$$p_{err} \leqslant 2^s t \exp\{-1/8 \cdot r\varepsilon^2\}. \tag{3.15}$$

Доведення. Якщо атака завершується помилково, то порушується хоча б одна з рівностей (3.12). Отже,

$$p_{err} \leqslant \sum_{i \in I} \Pr(kA_iM \neq \widehat{y}_i) \leqslant t \max_{i \in I} \Pr(kA_iM \neq \widehat{y}_i)$$

і для доведення формули (3.15) достатньо переконатися в тому, що виконуються такі нерівності:

$$\Pr(kA_iM \neq \widehat{y}_i) \leqslant 2^s \exp\{-1/8 \cdot r\varepsilon^2\}, \ i \in I. \tag{3.16}$$

Зафіксуємо $i \in I$. Зауважимо, що в силу означення вектора $\widehat{y}_i$ для будь-якого $C > 0$ виконуються співвідношення

$$\{kA_iM \neq \widehat{y}_i\} \subseteq \{\nu_i(kA_iM) \geqslant C\} \cup \bigcup_{y \in V_s : y \neq kA_iM} \{\nu_i(y) < C\},$$

з яких випливає, що

$$\Pr\left(kA_iM \neq \widehat{y}_i\right) \leqslant \Pr\left(\nu_i(kA_iM) \geqslant C\right) +$$

$$+ (2^s - 1) \max_{y \in V_s : y \neq kA_iM} \Pr\left(\nu_i(y) < C\right). \tag{3.17}$$

Далі, на підставі рівності (3.11), $\nu_i(kA_iM)$ є сумою незалежних випадкових величин $\xi_j = \varphi(kA_iM \oplus c^{(j)}B_iM) \oplus \gamma_i^{(j)}$, $j \in \overline{1,r}$. Отже, вважаючи

$$C = 1/4 \cdot r(2 - \varepsilon), \tag{3.18}$$

на підставі формули (3.13) та леми 3.1 отримаємо такі співвідношення:

$$\Pr\left(\nu_i(kA_iM) \geqslant C\right) \leqslant \Pr\left(\sum_{i=1}^{r} \xi_i - \sum_{i=1}^{r} \mathbb{E}\xi_i \geqslant C - 1/2 \cdot r(1 - \varepsilon)\right) =$$

$$= \Pr\left(\sum_{i=1}^{r}\xi_i - \sum_{i=1}^{r}\mathbb{E}\xi_i \geqslant 1/4\cdot r\varepsilon\right) \leqslant \exp\left\{-1/8\cdot r\varepsilon^2\right\}. \qquad (3.19)$$

Нехай зараз $y \in V_s$, $y \neq kA_iM$; тоді на підставі рівностей (3.11), (3.14) $\nu_i(y)$ є сумою незалежних випадкових величин $\eta_j = \varphi(y\oplus c^{(j)}B_iM)\oplus\gamma_i^{(j)}$, $j \in \overline{1,r}$, кожна з яких розподілена рівномірно на множині $\{0,1\}$. Отже, на підставі формули (3.18) та леми 3.1

$$\Pr\left(\nu_i(y) < C\right) = \Pr\left(\sum_{i=1}^{r}\eta_i - \sum_{i=1}^{r}\mathbb{E}\eta_i < C - 1/2\cdot r\right) =$$

$$= \Pr\left(\sum_{i=1}^{r}\eta_i - \sum_{i=1}^{r}\mathbb{E}\eta_i < -1/4\cdot r\varepsilon\right) \leqslant \exp\left\{-1/8\cdot r\varepsilon^2\right\}. \qquad (3.20)$$

Підставляючи оцінки (3.19), (3.20) у формулу (3.17), отримаємо нерівність (3.16). □

Наступне твердження надає змогу оцінити ефективність описаної атаки.

Твердження 3.1. *Нехай виконуються зазначені вище припущення і*

$$r = \lceil 8\cdot\varepsilon^{-2}\ln\left(2^s t\delta^{-1}\right)\rceil, \qquad (3.21)$$

де $\delta \in (0,1)$. Тоді наведена атака відновлює ключ k з ймовірністю не менше $1-\delta$, використовуючи (без урахування передобчислень на першому етапі) $O\left((2^s l_1 r + l_0^2)ts\right)$ операцій.

Зокрема, при $t = O\left(l_0 s^{-1}\right)$ часова складність атаки становить $O\left(2^s\varepsilon^{-2}l_1 l_0\ln\left(2^s l_0 s^{-1}\right) + l_0^3\right)$ операцій.

Доведення. Перше частина твердження випливає безпосередньо з формул (3.15), (3.21). Для доведення другої частини достатньо помітити, що для знаходження векторів $\widehat{y}_i$ $(i \in I)$ необхідно $O\left(2^s ts l_1 r\right)$ операцій, а для розв'язання системи лінійних рівнянь (3.12) мето-

дом Гауса – $O\left(l_0^2 ts\right)$ операцій. Отже, трудомісткість атаки становить $O\left((2^s l_1 r + l_0^2)ts\right)$ операцій.

□

Наведена атака показує, що послаблення умови «функція ускладнення генератора гами залежить від невеликої кількості змінних» до умови «ця функція є статистично близькою до маловимірної булевої функції» надає можливість отримати замість алгебраїчної статистичну атаку на фільтрувальний генератор гами. Ця статистична атака є застосовною за менш жорстких умов та, взагалі кажучи (в залежности від параметра ε), має меншу часову складність в порівнянні з алгебраїчною. Наведена атака показує також, що закон формування початкового стану генератора гами повинен бути нелінійним (більш того, цей закон повинен задовольняти умову псевдовипадковості, зазначеній в п. 1.4).

З результатами моделювання наведеної атаки та її узагальненням на випадок генератора з довільним законом формування початкового стану можна ознайомитись в [АКС1, АКС2].

3.3 Кореляційна атака Зігенталера

Зазначена атака є історично першою кореляційною атакою, опублікованою у відкритих джерелах [Sie]. 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. 3.2).

Вважається, що поліноми зворотного зв'язку ЛРЗ є примітивними, а комбінувальна функція $f : V_n \to \{0, 1\}$ – збалансованою. Знак

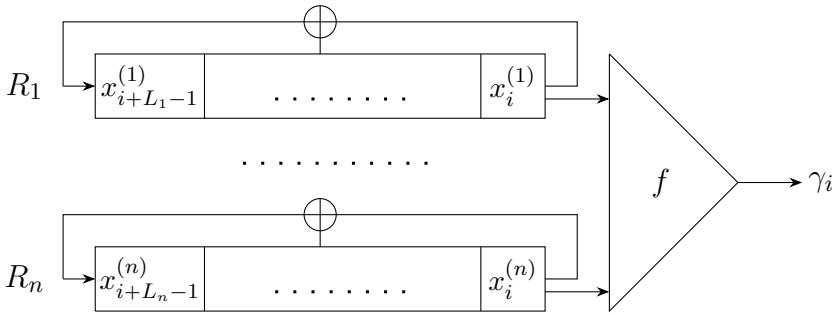

Рис. 3.2: Комбінувальний генератор гами

гами, що виробляється в i-му такті, обчислюється за формулою

$$\gamma_i = f(x_i^{(1)}, \ldots, x_i^{(n)}), \tag{3.22}$$

де $x_i^{(j)}$ – i-й знак лінійної рекуренти, яка виробляється j-м ЛРЗ, $i = 0, 1, \ldots$, $j \in \overline{1, n}$.

Як зазначено вище, атака Зігенталера спрямована на те, щоб відновити початковий стан генератора гами за послідовністю (3.22). 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 $1 \leqslant i_1 < ... < i_k \leqslant n$ такі, що

$$\Pr\left(f(X_1, \ldots, X_n) \neq g(X_{i_1}, \ldots, X_{i_k})\right) = p \leqslant 1/2 \cdot (1 - \varepsilon), \tag{3.23}$$

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 побудує-

мо новий, який складається з перших k ЛРЗ вхідного генератора та комбінувальної функції g (рис. 3.3). Відповідно до означення 3.2 назвемо новий генератор гами статистичним аналогом вхідного.

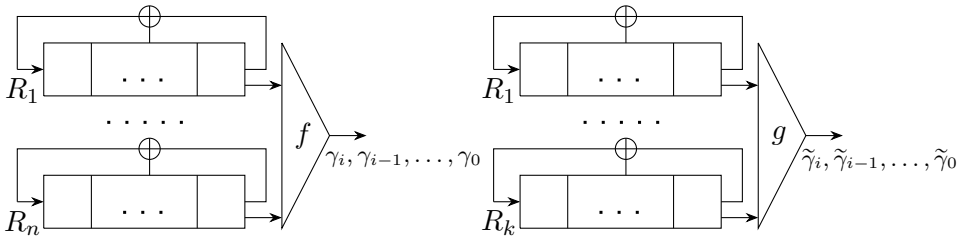

Рис. 3.3: Вхідний генератор гами та його статистичний аналог

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 (3.22) отримується в результаті спотворення вихідної послідовності $\widetilde{\gamma}_0, \widetilde{\gamma}_1, \ldots$ нового генератора гами так, що (згідно з формулою (3.23))

$$\Pr\left(\gamma_i \neq \widetilde{\gamma}_i\right) = p \leqslant 1/2 \cdot (1 - \varepsilon),\ i = 0, 1, \ldots.$$

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 $x^{(1)}, \ldots, x^{(k)}$ ЛРЗ з номерами $1, \ldots, k$ відповідно, обчислюючи значення

$$\xi(x^{(1)},\ldots,x^{(k)}) = \sum_{i=0}^{T-1} (g(x_i^{(1)},\ldots,x_i^{(k)}) \oplus \gamma_i), \qquad (3.24)$$

де T – довжина відрізка гами, доступного для аналізу, $x_i^{(j)}$ – i-й знак рекуренти, що виробляється j-м ЛРЗ при початковому стані $x^{(j)}$, $i \in \overline{0, T-1}$, $j \in \overline{1, k}$.

2. Вважатимемо істинним набір $(\widehat{x}^{(1)},\ldots,\widehat{x}^{(k)})$ початкових станів, що задовольняє умову

$$\xi(\widehat{x}^{(1)},\ldots,\widehat{x}^{(k)}) = \min_{x^{(1)},\ldots,x^{(k)}} \xi(x^{(1)},\ldots,x^{(k)}).$$

3. Знаючи початкові стани ЛРЗ з номерами $1,\ldots,k$, відновимо початкові стани решти ЛРЗ генератора шляхом повного перебору.

Зауважимо, що сума в правій частині формули (3.24) дорівнює числу 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 ЛРЗ, на якому досягається мінімум цих чисел.

Зрозуміло, що часова складність наведеної атаки становить

$$O\left(T \cdot 2^{L_1+\ldots+L_k} + (L_1+\ldots+L_n) \cdot 2^{L_{k+1}+\ldots+L_n}\right) \qquad (3.25)$$

операцій, в той час, як складність повного перебору дорівнює $O\left((L_1+\ldots+L_n) \cdot 2^{L_1+\ldots+L_n}\right)$ (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 ЛРЗ 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 початкових станів перших k ЛРЗ $(\widetilde{x}^{(1)}, \ldots, \widetilde{x}^{(k)}) \neq (\breve{x}^{(1)}, \ldots, \breve{x}^{(k)})$ знаки $\widetilde{x}_i^{(j)}$, $i \in \overline{0, T-1}$, $j \in \overline{1, k}$, є незалежними випадковими величинами з рівномірним розподілом на множині $\{0, 1\}$, які не залежать від знаків $\breve{x}_i^{(j)}$ для усіх $i \in \overline{0, T-1}$ та $j \in \overline{1, n}$.

З першого припущення та формул (3.22), (3.23) випливає, що при $(x^{(1)}, \ldots, x^{(k)}) = (\breve{x}^{(1)}, \ldots, \breve{x}^{(k)})$ значення $\xi(x^{(1)}, \ldots, x^{(k)})$ вигляду (3.24) співпадає з кількістю успіхів у схемі Бернуллі з числом випробувань T та ймовірністю успіху $p \leqslant 1/2 \cdot (1 - \varepsilon)$. 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 $1/2$. Виходячи з цього, за допомогою міркувань, аналогічних використаним у доведенні леми 3.2, можна переконатися, що для ймовірності помилкового відновлення початкових станів перших k ЛРЗ на кроці 2 наведеної атаки справедлива така нерівність:

$$p_{err} = \Pr\left((\widehat{x}^{(1)}, \ldots, \widehat{x}^{(k)}) \neq (\breve{x}^{(1)}, \ldots, \breve{x}^{(k)})\right) \leqslant$$

$$\leqslant 2^{L_1 + \ldots + L_k} \exp\{-1/8 \cdot T\varepsilon^2\}.$$

Звідси випливає наступне твердження.

Твердження 3.2. *Нехай виконуються зазначені вище припущення,* $\delta \in (0,1)$ *і*

$$T = \lceil 8 \cdot \varepsilon^{-2} \ln (2^{L_1+\ldots+L_k} \delta^{-1}) \rceil.$$

Тоді описана атака відновлює початковий стан генератора гами на рис. 3.2 з ймовірністю не менше $1-\delta$ *та часовою складністю, що визначається за формулою (3.25).*

Таким чином, для забезпечення стійкості комбінувального генератора гами відносно атаки Зігенталера потрібно вибирати його комбінувальну функцію так, щоб для неї не існувало високоймовірних наближень від достатньо малої кількості змінних. Такі функції отримали назву кореляційно-імунних (більш докладно про них див. задачі 3.5, 3.6, 3.22).

Зауважимо також, що в оригінальній роботі Зігенталера [Sie] 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.

3.4 Загальна кореляційна задача

Наведені вище статистичні атаки є по суті окремими випадками математичної задачі, яка отримала назву *загальної кореляційної задачі* [Can+]. Тому аналіз зазначених атак є дуже подібним.

Розглянемо цю задачу більш докладно.

Нехай S – скінченна множина, кожному елементу s якої відповідає розподіл ймовірностей P_s на множині V_T двійкових векторів

довжини T. При цьому вважається, що існує такий елемент $s_0 \in S$, що

$$P_s = \begin{cases} P, & \text{якщо } s = s_0; \\ Q, & \text{якщо } s \neq s_0, \end{cases}$$

де P і Q є різними відомими розподілами ймовірностей на множині V_T. Задача полягає в тому, щоб відновити елемент s_0 за умови доступу к оракулу, який для будь-якого $s \in S$ генерує випадкову послідовність, розподілену за законом P_s.

Зрозуміло, що атаки, описані в п. 3.2 та 3.3, зводяться до загальної кореляційної задачі, причому в цих атаках параметр s_0 є початковим станом відповідного генератора гами, розподіл Q є рівномірним на множині V_T, а розподіл P визначається за формулою

$$P(x) = p^{\mathrm{wt}(x)}(1-p)^{T-\mathrm{wt}(x)},$$

де $\mathrm{wt}(x)$ – вага (число одиниць у запису) вектора $x \in V_T$, причому $p \leqslant 1/2 \cdot (1-\varepsilon)$, $\varepsilon \in (0,1)$.

В зазначеному випадку природний метод розв'язання загальної кореляційної задачі полягає в тому, щоб отримати за допомогою оракула для кожного $s \in S$ випадковий вектор ξ_s, розподілений за занконом P_s, та прийняти в ролі s_0 такий елемент $\widehat{s} \in S$, для якого досягається мінімум значень $\mathrm{wt}(\xi_s)$ за всіма $s \in S$ (якщо існує декілька таких елементів $\widehat{s}$, треба взяти навмання один з них).

Наступне твердження (яке доводиться аналогічно твердженню 3.1) надає змогу оцінити ймовірність успішного розв'язання задачі за допомогою цього методу.

Твердження 3.3. *Справедлива нерівність*

$$p_{err} = \Pr\left(\widehat{s} \neq s_0\right) \leqslant |S| \exp\left\{-1/8 \cdot T\varepsilon^2\right\}.$$

Зокрема, якщо

$$T = \lceil 8 \cdot \varepsilon^{-2} \ln(|S|\delta^{-1}) \rceil,$$

де $\delta \in (0,1)$*, то ймовірність правильного відновлення елемента* s_0 *становить не менше* $1 - \delta$*.*

3.5 Перетворення Фур'є псевдобулевих функцій

Позначимо $\mathbb{R}^{2^n}$ векторний простір усіх функцій, заданих на множині V_n, які приймають значення в полі дійсних чисел. Довільну функцію $f \in \mathbb{R}^{2^n}$ будемо називати *псевдобулевою* і ототожнювати її з вектор-стовпцем її значень: $f = (f(x) : x \in V_n)^T$.

Векторний простір псевдобулевих функцій від n змінних є евклідовим простором відносно *скалярного добутку*

$$\langle f, g \rangle = \sum_{x \in V_n} f(x)g(x), f, g \in \mathbb{R}^{2^n},$$

що надає змогу надалі використовувати результати, які стосуються цих просторів та їхніх лінійних перетворень. Зокрема, для будь-якої функції $f \in \mathbb{R}^{2^n}$ можна визначити її *норму*:

$$||f||_2 = \sqrt{\langle f, f \rangle}.$$

При цьому для довільних функцій $f, g \in \mathbb{R}^{2^n}$ виконується *нерівність Коші-Буняковського* (або *нерівність Шварца*):

$$|\langle f, g \rangle| \leqslant ||f||_2 \cdot ||g||_2.$$

Ключову роль в означенні перетворення Фур'є псевдобулевих функцій відіграї наступне поняття.

Означення 3.3. *Матрицею Адамара* (типу Сільвестра) порядку 2^n називається квадратна матриця

$$H_n = ((-1)^{\alpha\beta})_{\alpha,\beta\in V_n},$$

де $\alpha\beta = \bigoplus\limits_{i=1}^{n} \alpha_i\beta_i$ – 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.

Твердження 3.4. *Матриця H_n є оборотною, причому*

$$H_n^{-1} = 2^{-n} H_n.$$

Доведення. Достатньо переконатися в тому, що для будь-яких $\alpha, \beta \in V_n$ виконується рівність

$$2^{-n} \sum_{x\in V_n} (-1)^{\alpha x} \cdot (-1)^{\beta x} = \delta_{\alpha,\beta}, \tag{3.26}$$

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 збалансованою за умови $\alpha \neq \beta$ та дорівнює 0 в протилежному випадку.

□

Співвідношення (3.26) (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 $\mathbb{R}$

називається ортогональною, якщо обернена до неї матриця збігається з транспонованою: $U^{-1} = U^T$).

За допомогою матриці Адамара H_n визначається перетворення Фур'є псевдобулевих функцій.

Означення 3.4. *Перетворенням Фур'є* функції $f \in \mathbb{R}^{2^n}$ називається функція

$$C_f = H_n f$$

(нагадаємо, що функції f та C_f ототожнюються з вектор-стовпцями їх значень). При цьому *коефіцієнтом Фур'є* функції f, який відповідає вектору $\alpha \in V_n$, називається число

$$C_f(\alpha) = \sum_{x \in V_n} f(x)(-1)^{\alpha x}. \tag{3.27}$$

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 (3.27).

Розглянемо основні властивості перетворення Фур'є, які випливають з його означення та ортогональності матриці Адамара.

1. Перетворення Фур'є є лінійним перетворенням векторного простору $\mathbb{R}^{2^n}$.

2. Має місце *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 $f, g \in \mathbb{R}^{2^n}$. Застосовуючи цей факт до матриці $2^{-\frac{n}{2}} H_n$, отримуємо таку рівність:

$$\langle f, g\rangle = 2^{-n}\langle H_n f, H_n g\rangle$$

або в координатній формі

$$\sum_{x\in V_n} f(x)g(x) = 2^{-n} \sum_{\alpha\in V_n} C_f(\alpha)C_g(\alpha). \tag{3.28}$$

Таким чином, скалярний добуток псевдобулевих функцій збігається з точністю до співмножника зі скалярним добутком їхніх коефіцієнтів Фур'є.

4. Вважаючи в формулі (3.28) $f = g$, 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 значень квадратів її коефіцієнтів Фур'є.

3.6 Алгоритм швидкого перетворення Адамара

Задача обчислення коефіцієнтів Фур'є псевдобулевої функції є дуже розповсюдженою у криптографічних (та інших) застосуван-

нях. Тому постає запитання про існування ефективних алгоритмів розв'язання цієї задачі.

Нехай $a \in \mathbb{R}^{2^n}$ – довільний вектор-стовпець довжини 2^n, H_n – матриця Адамара порядку 2^n. Тоді для знаходження вектора

$$b = H_n a \tag{3.29}$$

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 (3.29), використовуючи лише $2^n n$ операцій додавання чи віднімання.

В основі зазначеного алгоритму лежить наступне твердження, яке доводиться шляхом безпосередньої перевірки.

Твердження 3.5. *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 процедуру $\mathcal{A}(n)$, яка визначається таким чином.

Процедура $\mathcal{A}(n)$.

Вхід: вектор-стовпець $a = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$ довжини 2^n, де $a_0, a_1 \in \mathbb{R}^{2^{n-1}}$.

Результат: вектор-стовпець $b = H_n a$.

Якщо $n = 1$, обчислити

$$b_0 = a_0 + a_1, b_1 = a_0 - a_1, b = \begin{pmatrix} b_0 \\ b_1 \end{pmatrix}. \tag{3.30}$$

Якщо $n \geqslant 2$, обчислити вектори b_0 та b_1, застосовуючи процедуру $\mathcal{A}(n-1)$ 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 (3.29) за допомогою наведеного алгоритму.

Твердження 3.6. *Для будь-якого натурального n має місце рівність*

$$t(n) = 2^n n.$$

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

З рівностей (3.30) випливає, що

$$t(1) = 2. \tag{3.31}$$

Далі, при $n \geqslant 2$ для обчислення вектора b за допомогою процедури $\mathcal{A}(n)$ необхідно виконати 2^n операцій додавання (віднімання) для обчислення векторів $a_0 + a_1$, $a_0 - a_1$ та ще $2t(n-1)$ таких опе-

рацій при застосуванні до отриманих векторів процедури $\mathcal{A}(n-1)$. Таким чином,

$$t(n) = 2^n + 2 \cdot t(n-1),\ n = 2, 3, \ldots. \tag{3.32}$$

Покладемо $\tau(n) = 2^{-n}t(n)$, $n = 1, 2, \ldots$. На підставі формул (3.31), (3.32) 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. □

3.7 Перетворення Уолша-Адамара та афінні наближення булевих функцій

Розглянемо окремий випадок перетворення Фур'є, що використовується для аналізу кореляційних властивостей булевих функцій.

Означення 3.5. *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 має місце 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*:

$$\sum_{\alpha \in V_n} \hat{f}(\alpha)^2 = 2^{2n}. \tag{3.33}$$

Таким чином, сума квадратів коефіцієнтів Уолша-Адамара дорівнює 2^{2n}.

Як показує наступне твердження, коефіцієнти Уолша-Адамара надають можливість оцінювати якість афінних наближень булевих функцій та знаходити їхні афінні статистичні аналоги (див. означення 3.2).

Твердження 3.7. *Для будь-яких $f : V_n \to \{0,1\}$, $\alpha \in V_n$, $c \in \{0,1\}$ виконується рівність*

$$\Pr\left(f(X) = \alpha X \oplus c\right) = 1/2 \cdot (1 + (-1)^c 2^{-n} \hat{f}(\alpha)), \tag{3.34}$$

де X – випадковий рівноймовірний двійковий вектор довжини n.

Доведення. Достатньо довести формулу (3.34) при $c = 0$.
Дійсно, мають місце співвідношення

$$\hat{f}(\alpha) = \sum_{x \in V_n} (-1)^{f(x) \oplus \alpha x} =$$

$$= |\{x \in V_n : f(x) = \alpha x\}| - |\{x \in V_n : f(x) \neq \alpha x\}| =$$

$$= 2 \cdot |\{x \in V_n : f(x) = \alpha x\}| - 2^n = 2^{n+1} \Pr(f(X) = \alpha X) - 2^n,$$

що й треба було довести.

□

З твердження 3.7 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 (3.33)) афінні статистичні аналоги існують для будь-якої булевої функції.

Розглянемо такий важливий криптографічний параметр булевої функції як її нелінійність.

Означення 3.6. *Нелінійністю* функції $f : V_n \to \{0, 1\}$ називається відстань (Геммінга) від неї до класу афінних функцій:

$$N_f = \min_{\substack{\alpha \in V_n, \\ c \in \{0,1\}}} ||f \oplus l_{\alpha,c}||.$$

Твердження 3.8. *Нелінійність функції $f : V_n \to \{0, 1\}$ задовольняє таке співвідношення*

$$N_f = 2^{n-1}(1 - 2^{-n} \max_{\alpha \in V_n} |\hat{f}(\alpha)|).$$

Доведення. На підставі твердження 3.7

$$||f \oplus l_{\alpha,c}|| = 2^n \Pr(f(X) \neq l_{\alpha,c}(X)) =$$

$$= 2^{n-1}(1 - (-1)^c 2^{-n} \hat{f}(\alpha)).$$

Отже,

$$\min_{\substack{\alpha \in V_n, \\ c \in \{0,1\}}} ||f \oplus l_{\alpha,c}|| = \min_{\substack{\alpha \in V_n, \\ c \in \{0,1\}}} 2^{n-1}(1 - (-1)^c 2^{-n} \hat{f}(\alpha)) =$$

$$= \min_{\alpha \in V_n} 2^{n-1}(1 - 2^{-n}|\hat{f}(\alpha)|) = 2^{n-1}(1 - 2^{-n} \max_{\alpha \in V_n} |\hat{f}(\alpha)|),$$

що і треба було довести. □

Твердження 3.9. *Нелінійність будь-якої функції $f : V_n \to \{0,1\}$ задовольняє нерівність*

$$N_f \leqslant 2^{n-1} - 2^{\frac{n}{2}-1}, \tag{3.35}$$

яка перетворюється на рівність тоді й тільки тоді, коли $|\hat{f}(\alpha)| = 2^{\frac{n}{2}}$ для всіх $\alpha \in V_n$.

Доведення. Використовуючи рівність Парсеваля, отримаємо, що

$$2^{2n} = \sum_{\alpha \in V_n} \hat{f}(\alpha)^2 \leqslant 2^n \max_{\alpha \in V_n} \hat{f}(\alpha)^2. \tag{3.36}$$

Отже, $\max\limits_{\alpha \in V_n} |\hat{f}(\alpha)| \geqslant 2^{\frac{n}{2}}$. Звідси, на підставі твердження 3.8, випливає нерівність (3.35).

Далі, якщо $|\hat{f}(\alpha)| = 2^{\frac{n}{2}}$ для усіх $\alpha \in V_n$, то зазначена нерівність досягається. Навпаки, якщо $N_f = 2^{n-1} - 2^{\frac{n}{2}-1}$, то в силу твердження 3.8 $\max\limits_{\alpha \in V_n} |\hat{f}(\alpha)| = 2^{\frac{n}{2}}$, звідки випливає, що нерівність (3.36) перетво-

рюється на рівність. Отже,

$$|\hat{f}(\alpha)| = \max_{\alpha \in V_n} |\hat{f}(\alpha)| = 2^{\frac{n}{2}}$$

для кожного $\alpha \in V_n$, то що й треба було довести.

□

Означення 3.7. 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 усіх $\alpha \in V_n$.

Зрозуміло, що бент-функції від n змінних існують тільки для парних значень n. Найвідомішим прикладом бент-функції є функція $xy = \bigoplus_{i=1}^{n} x_i y_i$, де $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in V_n$.

3.8 Застосування швидкого перетворення Адамара до розв'язання систем лінійних рівнянь зі спотвореними правими частинами

Більшість кореляційних атак на потокові шифри зводиться до розв'язання такої задачі.

Задано систему рівнянь

$$Ax = b, \tag{3.37}$$

де A – булева матриця розміру $m \times n$, b – вектор-стовпець довжини m з координатами

$$b_i = A_i a \oplus \xi_i, \ i \in \overline{1, m}, \tag{3.38}$$

де $A_1, \ldots, A_m$ – рядки матриці A, $a = (a_1, \ldots, a_n)^T$ – невідомий двійковий вектор (істинний розв'язок системи рівнянь (3.37)),

$\xi_1, \ldots, \xi_m$ – незалежні випадкові величини, розподілені за законами

$$\Pr(\xi_i = 0) = 1 - \Pr(\xi_i = 1) = 1/2 \cdot (1 + \theta_i),\ i \in \overline{1, m}, \qquad (3.39)$$

де $\theta_i \geqslant \theta > 0$ для кожного $i \in \overline{1, m}$. Треба відновити вектор a за відомими значеннями A, b і θ.

Наведена система рівнянь називається *системою лінійних рівнянь зі спотвореними правими частинами*, а задача її розв'язання (за умови, що матриця A вибирається навмання) є обчислювально складною, відомою під назвою задачі LPN (Learning Parity with Noise).

Якщо $\theta_i = \theta$ для усіх $i \in \overline{1, m}$, то розв'язання системи (3.37) методом максимуму правдоподібності полягає в обчисленні ваги $||Ax \oplus b||$ для кожного $x \in V_n$ та вибору в якості кандидата на істинний розв'язок a такого вектора $\widehat{x}$, що значення $||A\widehat{x} \oplus b||$ є найменшим (якщо існує декілька таких векторів, то навмання вибирається будь-який з них; див. задачі 3.16, 3.17). Зрозуміло, що трудомісткість цієї процедури становить $O(2^n nm)$ операцій. Поряд з тим, існує алгоритм знаходження вектора $\widehat{x}$, який базується на застосуванні швидкого перетворення Адамара та потребує $O(n2^n + m)$ операцій.

Для опису цього алгоритму задамо псевдобулеву функцію

$$g(y) = \sum_{\substack{i \in \overline{1,m}: \\ A_i = y}} (-1)^{b_i},\ y \in V_n$$

та знайдемо її перетворення Фур'є:

$$C_g(x) = \sum_{y \in V_n} g(y)(-1)^{xy} = \sum_{y \in V_n} \sum_{\substack{i \in \overline{1,m}: \\ A_i = y}} (-1)^{b_i \oplus xy} = \sum_{i=1}^{m} (-1)^{A_i x \oplus b_i} =$$

$$= |\{i \in \overline{1,m} : A_i x = b_i\}| - |\{i \in \overline{1,m} : A_i x \neq b_i\}| =$$

$$= m - 2 \cdot ||Ax \oplus b||,\ x \in V_n.$$

звідки випливає, що *для знаходження вектора* $\widehat{x}$*, який мінімізує значення* $||Ax \oplus b||$ *за всіма* $x \in V_n$ *достатньо виконати наступний алгоритм.*

1. Ініціалізувати вектор значень функції g нулями: $g(y) = 0$, $y \in V_n$.

2. Для $i = 1, 2, \ldots, m$ покласти $g(A_i) = g(A_i) + (-1)^{b_i}$.

3. Обчислити значення $C_g(x)$ для усіх $x \in V_n$ за допомогою алгоритму швидкого перетворення Адамара.

4. Знайти вектор $\widehat{x}$, на якому досягається максимум значень, обчислених на кроці 3.

Безпосередньо з твердження 3.6 та опису наведеного алгоритму випливає, що його трудомісткість становить $O(n2^n + m)$ операцій.

3.9 Алгоритм BKW

Як зазначено вище, задача розв'язання випадкової системи лінійних рівнянь зі спотвореними правими частинами є обчислювально складною. Більше того, вона є NP-складною [BMT]; отже, для неї не відомо (та, ймовірно, не існує) поліноміальних алгоритмів.

Перший субекспоненційний алгоритм розв'язання цієї задачі запропоновано в 1988 р. І. М. Коваленком [Ков], який показав, що у випадку, коли матриця коефіцієнтів системи, яка складається з $2^{O\left(\frac{n}{\log n}\right)}$ спотворених лінійних рівнянь від n змінних, є випадковою та задовольняє певну загальну умову, зазначену систему можна

розв'язати з як завгодно малою при $n \to \infty$ ймовірністю помилки, використовуючи в середньому $2^{O\left(\frac{n}{\log n}\right)}$ операцій.

Алгоритм Коваленка було фактично перевідкрито тринадцять років потому А. Блюмом, А. Калаі та Х. Вассерманом [BKW], які вивчали задачу розв'язання систем лінійних рівнянь зі спотвореними правими частинами у зв'язку з однією проблемою теорії вивідування (learning theory). Алгоритм Блюма-Калаі-Вассермана (BKW) швидко набув широкої відомості та знайшов чимало застосувань. На сьогодні відомі численні вдосконалення та узагальнення цього алгоритму (див., наприклад, [BTV]).

Нижче розглядається (слідуючи роботі [Ол]) історично перший варіант алгоритму BKW, вивчення якого надає змогу з'ясувати основну ідею, покладену в основу його сучасних, більш ефективних версій.

Для викладення алгоритму розглянемо спочатку допоміжну задачу, до якої зводиться розв'язання випадкових систем лінійних рівнянь зі спотвореними правими частинами.

Задача про *адитивне r-представлення* (або *r-суму*, r-sum problem) полягає в наступному. Задано список (впорядкований набір) L, який складається з l векторів $z_1, \ldots, z_l \in V_n$. Потрібно для будь-якого вектора $z \in V_n \backslash \{0\}$ знайти r (не обов'язково різних) номерів $\nu_1, \ldots, \nu_r \in \overline{1, l}$ таких, що $z_{\nu_1} \oplus \ldots \oplus z_{\nu_r} = z$.

Припускається, що будь-який алгоритм $\mathcal{A}$ розв'язання цієї задачі або завершується успішно, тобто знаходить шуканий набір $\nu_1, \ldots, \nu_r$, або видає негативну відповідь, тобто не знаходить зазначеного набору (хоча такий може існувати).

Якщо вектори $z_1, \ldots, z_l$ у списку L генеруються незалежно випадково та рівноймовірно, то символом $\pi_{\mathcal{A}}$ позначається мінімальна за всіма векторами $z \in V_n \backslash \{0\}$ ймовірність успішного завершення алгоритму $\mathcal{A}$ при вхідних даних (L, z). Символом $T_{\mathcal{A}}$ позначається найбільше число операцій над n-вимірними двійковими векторами,

які виконуються при застосуванні алгоритму $\mathcal{A}$ до будь-яких вхідних даних (L, z).

Відзначимо окремий випадок задачі про адитивне r-представлення, в якому задається r вхідних списків $L_1, \ldots, L_r$ довжини $l_1, \ldots, l_r$ відповідно, що складаються з незалежних в сукупності випадкових рівноймовірних двійкових векторів довжини n. Потрібно знайти набір $z_1 \in L_1, \ldots, z_r \in L_r$ такий, що $z_1 \oplus \ldots \oplus z_r = 0$. Зрозуміло, що при $l_1 + \ldots + l_r = l$ будь-який алгоритм $\mathcal{A}$ розв'язання останньої задачі дозволяє розв'язувати першу: достатньо розбити вхідний список L на r частин $L_1, L_2, \ldots, L_r$ та застосувати алгоритм $\mathcal{A}$ до списків $L_1 \oplus z, L_2, \ldots, L_r$.

Задача про адитивне представлення добре відома в теорії кодування, теорії обчислювальних алгоритмів та криптоаналізі. Зокрема, на ній, тією чи іншою мірою, базуються усі відомі субекспоненційні алгоритми розв'язання систем лінійних рівнянь зі спотвореними правими частинами.

Позначимо e_i вектор довжини n, i-а координата якого дорівнює 1, а решта – 0, $i \in \overline{1, n}$.

Сформулюємо допоміжне твердження, яке доводиться за допомогою індукції по r.

Лема 3.3. *Нехай $\xi_1, \ldots, \xi_r$ – незалежні випадкові величини, розподілені за законами $\Pr(\xi_i = 1) = 1 - \Pr(\xi_i = 0) = p_i$, $i \in \overline{1, r}$. Тоді*

$$\Pr(\xi_1 \oplus \ldots \oplus \xi_r = 0) = 1/2 \cdot (1 + (1 - 2p_1) \ldots (1 - 2p_r)).$$

Розглянемо випадкову систему рівнянь (3.37), що задовольняє умови (3.38), (3.39). Наступна теорема показує, що розв'язання цієї системи рівнянь ефективно зводиться (в обчислювальному сенсі слова) до задачі про адитивне представлення.

Теорема 3.1. *Припустимо, що матриця A системи рівнянь (3.37) складається з $m = nlt$ рядків, які є незалежними випадковими векторами, що мають рівномірний розподіл на множині V_n і не залежать від випадкових величин $\xi_1, \ldots, \xi_m$. Тоді для будь-якого алгоритму $\mathcal{A}$ розв'язання задачі про адитивне представлення з параметрами n, r, l (див. вище) існує алгоритм $\mathcal{B}$, який знаходить істинний розв'язок системи рівнянь (3.37) з імовірністю*

$$p_{\mathcal{B}} \geqslant (\pi_{\mathcal{A}})^{tn}(1 - \exp\{-1/2 \cdot \theta^{2r} t\})^n, \tag{3.40}$$

використовуючи

$$t_{\mathcal{B}} = O(nt(T_{\mathcal{A}} + r)) \tag{3.41}$$

операцій над n-вимірними двійковими векторами.

Доведення. Алгоритм $\mathcal{B}$, що пропонується, має такий вигляд.

1. Розіб'ємо систему рядків матриці A на tn списків $L_{i,j}$ довжини l кожний та застосуємо алгоритм $\mathcal{A}$ до вхідних даних $(L_{i,j}, e_i)$ для всіх $i \in \overline{1,n}$, $j \in \overline{1,t}$. Якщо хоча б в одному випадку алгоритм $\mathcal{A}$ завершується неуспішно, то алгоритм $\mathcal{B}$ припиняє роботу. Інакше для кожного $i \in \overline{1,n}$ отримаємо рівності вигляду

$$e_i = A_{\nu_1(i,j)} \oplus \ldots \oplus A_{\nu_r(i,j)}, \ j \in \overline{1,t}, \tag{3.42}$$

де $A_{\nu_1(i,j)}, \ldots, A_{\nu_r(i,j)} \in L_{i,j}$.

2. Для будь-яких $i \in \overline{1,n}$, $j \in \overline{1,t}$ обчислимо значення $b(i,j) = b_{\nu_1(i,j)} \oplus \ldots \oplus b_{\nu_r(i,j)}$ та відновимо i-у координату вектора a за мажоритарним правилом:

$$a_i = 1 \Leftrightarrow \sum_{j=1}^{t} b(i,j) \geqslant t/2.$$

Безпосередньо з наведеного опису випливає, що трудомісткість алгоритму $\mathcal{B}$ визначається за формулою (3.41).

Доведемо формулу (3.40). Помітимо, що оскільки A є випадковою рівноймовірною булевою $m \times n$-матрицею, то всі списки $L_{i,j}$, які формуються на кроці 1 алгоритму, складаються з незалежних в сукупності випадкових рівноймовірних двійкових векторів довжини n.

Позначимо $\mathcal{I}$ множину значень випадкової матриці A, для кожного з яких алгоритм $\mathcal{A}$ завершується успішно при всіх його застосуваннях на кроці 1. Далі, для кожного $A^* \in \mathcal{I}$ позначимо $\mathcal{R}(A^*)$ подію, яка полягає в тому, що алгоритм $\mathcal{B}$ правильно відновлює вектор a на кроці 2 за умови, що $A = A^*$. В силу незалежності матриці A та випадкових величин $\xi_1, \ldots, \xi_m$ ймовірність правильного відновлення вектора a дорівнює

$$p_{\mathcal{B}} = \sum_{A^* \in \mathcal{I}} \Pr(A = A^*) \Pr(\mathcal{R}(A^*)). \tag{3.43}$$

Зафіксуємо матрицю $A^* \in \mathcal{I}$ та оцінимо ймовірність події $\mathcal{R}(A^*)$. Позначимо $L^*_{i,j}$, $i \in \overline{1,n}$, $j \in \overline{1,t}$, списки, які формується на кроці 1 алгоритму $\mathcal{B}$ за вхідною матрицею A^*. Помітимо, що на підставі формул (3.38) та (3.42) мають місце такі рівності:

$$a_i = e_i a = b(i,j) \oplus (\xi_{\nu_1(i,j)} \oplus \ldots \oplus \xi_{\nu_r(i,j)}),\ i \in \overline{1,n}, j \in \overline{1,t}.$$

При цьому числа $\nu_1(i,j), \ldots, \nu_r(i,j)$ є (не обов'язково різними) номерами рядків, які належать списку $L^*_{i,j}$. Отже, для будь-яких $(i,j) \neq (i',j')$ має місце співвідношення

$$\{\nu_1(i,j), \ldots, \nu_r(i,j)\} \cap \{\nu_1(i',j'), \ldots, \nu_r(i',j')\} = \varnothing,$$

з якого випливає, що випадкові величини $\xi_{\nu_1(i,j)} \oplus \ldots \oplus \xi_{\nu_r(i,j)}$, $i \in \overline{1,n}$, $j \in \overline{1,t}$, є незалежними в сукупності. Нарешті, на підставі леми 3.3, формули (3.39) та умови $\theta_s \geqslant \theta > 0$, $s \in \overline{1,m}$, виконується нерівність

$$\Pr\left(\xi_{\nu_1(i,j)} \oplus \ldots \oplus \xi_{\nu_r(i,j)} = 0\right) \geqslant 1/2 \cdot (1 + \theta^r),\ i \in \overline{1,n}, j \in \overline{1,t}.$$

Таким чином, для оцінювання ймовірності події $\mathcal{R}(A^*)$ можна скористатися нерівністю Гефдінга (див. лему 3.1). Згідно з цією нерівністю, ймовірність помилки при відновленні кожного окремого значення a_i, $i \in \overline{1,n}$, на другому кроці алгоритму $\mathcal{B}$ не перевищує $\exp\{-1/2 \cdot \theta^{2r} t\}$. Отже,

$$\Pr\left(\mathcal{R}(A^*)\right) \geqslant (1 - \exp\{-1/2 \cdot \theta^{2r} t\})^n.$$

Підставляючи зазначену оцінку в формулу (3.43), з урахуванням нерівності $\Pr\left(A \in \mathcal{I}\right) \geqslant (\pi_{\mathcal{A}})^{tn}$ отримаємо формулу (3.40).

□

Як видно з доведення, теорема 3.1 залишається справедливою і в тому випадку, коли алгоритм $\mathcal{A}$ дозволяє знаходити з ймовірністю не менше $\pi_{\mathcal{A}}$ адитивне r-представлення кожного з векторів $e_1, \ldots, e_n$ (але не обов'язково довільного вектора $z \in V_n \backslash \{0\}$). Наведемо приклад такого алгоритму, що запропоновано в [BKW].

Теорема 3.2. *Нехай u, v, λ – натуральні числа і*

$$n \leqslant uv,\ r = 2^{u-1},\ l = (u + \lambda - 1)2^v. \tag{3.44}$$

Тоді існує алгоритм $\mathcal{A}_0$, який відшукує адитивне r-представлення кожного з векторів $e_1, \ldots, e_n$ у випадковому рівноймовірному списку L довжини l з ймовірністю $\pi_{\mathcal{A}_0} \geqslant 1 - e^{-\lambda}$, використовуючи $T_{\mathcal{A}_0} = O(u(u + \lambda)2^v)$ операцій над n-вимірними двійковими векторами.

Доведення. Опишемо алгоритм відшукання r-представлення вектора e_1. Адитивні представлення векторів $e_2, \ldots, e_n$ можна побудувати, застосовуючи зазначений алгоритм до списків, які отримуються шляхом циклічного зсуву всіх векторів зі списку L на $1, \ldots, n-1$ позицій відповідно.

Не обмежуючи загальності, вважатимемо, що $n = uv$ (у протилежному випадку допишемо до кожного вектора довжини n необхідну кількість нулів). Отже, будь-який вектор $z \in V_n$ можна розглядати як послідовність u двійкових слів довжини v біт кожне та записувати у вигляді $z = (z^{(1)}, \ldots, z^{(u)})$, де $z^{(i)} \in V_v$, $i \in \overline{1, u}$.

Алгоритм $\mathcal{A}_0$ відшукання адитивного r-представлення вектора e_1 у випадковому рівноймовірному списку L має такий вигляд.

Розіб'ємо вхідний список на блоки, відносячи до одного і того ж блоку L_c ($c \in V_v$) усі вектори $z \in L$ такі, що $z^{(u)} = c$. Зауважимо, що зазначене розбиття можна отримати, використовуючи $O(l)$ операцій, де l – довжина списку L.

Далі для кожного непорожнього блоку L_c виконаємо таку процедуру: виберемо з блоку L_c випадково рівноймовірно один вектор, додамо його до кожного іншого вектора з цього блоку та вилучимо зі списку L. В результаті отримаємо новий список $L^{(1)}$, що складається не менше ніж з $l_1 = l - 2^v$ векторів, які задовольняють наступні умови:

а) для будь-якого $z \in L^{(1)}$ виконується рівність $z^{(u)} = 0$;

б) кожен вектор $z \in L^{(1)}$ є сумою точно двох векторів зі списку L;

в) підвектори, що складаються з перших $u - 1$ слів усіх векторів зі списку $L^{(1)}$, є незалежними в сукупності випадковими рівноймовірними векторами довжини $(u - 1)v$.

Справедливість тверджень а) – в) випливає безпосередньо з наведеного опису процедури формування списку $L^{(1)}$ за списком L і умови випадковості та рівноймовірності останнього.

Далі застосуємо аналогічну процедуру до списку $L^{(1)}$ та отримаємо список $L^{(2)}$, що складається не менше ніж з $l_2 = l - 2^v - 2^v$ векторів, які задовольняють умови, аналогічні а) – в). Продовжуючи зазначений процес, отримаємо послідовність списків $L^{(1)}, \ldots, L^{(u-1)}$ таких, що для кожного $i \in \overline{1, u-1}$ список $L^{(i)}$ складається не менше ніж з $l - i2^v$ векторів z, кожен з яких задовольняє умову $z^{(u-i+1)} = \ldots = z^{(u)} = 0$ та є сумою точно 2^i векторів зі списку L. При цьому підвектори, що складаються з перших $u - i$ слів усіх векторів зі списку $L^{(i)}$, є незалежними в сукупності випадковими рівноймовірними двійковими векторами довжини $(u - i)v$.

На останньому кроці, при $i = u - 1$, отримаємо список $\widetilde{L}$, який складається не менше ніж з $l - (u-1)2^v = \lambda 2^v$ незалежних випадкових рівноймовірних векторів $z^{(1)} \in V_v$ таких, що вектори $(z^{(1)}, 0, \ldots, 0)$ утворюють список $L^{(u-1)}$. Оскільки ймовірність появи будь-якого фіксованого вектора довжини v у списку $\widetilde{L}$ є не менше за $1 - \left(\frac{2^v-1}{2^v}\right)^{\lambda 2^v} \geqslant 1 - e^{-\lambda}$, то вектор e_1 зустрінеться у списку $L^{(u-1)}$ з такою самою ймовірністю. При цьому, оскільки кожен вектор з останнього списку є сумою точно $r = 2^{u-1}$ векторів, що належать списку L, то шукане адитивне r-представлення вектора e_1 можна отримати з імовірністю $\pi_{\mathcal{A}_0} \geqslant 1 - e^{-\lambda}$.

Нарешті, як випливає з наведеного опису алгоритму $\mathcal{A}_0$, його трудомісткість складає $T_{\mathcal{A}_0} = O(ul) = O(u(u+\lambda)2^v)$ операцій. □

Застосуємо теореми 3.1 і 3.2, вважаючи

$$u = \left\lceil \frac{\log n}{2} \right\rceil, \quad v = \left\lceil \frac{2n}{\log n} \right\rceil,$$

$$t = \left\lceil 2\theta^{-2r} \ln (2n\delta^{-1}) \right\rceil, \quad \lambda = \left\lceil \ln (2tn\delta^{-1}) \right\rceil,$$

де $\delta \in (0, 1)$. При фіксованому θ і $n \to \infty$ мають місце співвідношення

$$r = O(\sqrt{n}),\ t = O(\theta^{-2r}),\ \lambda = O(\sqrt{n}),$$

$$l = O(\sqrt{n}\ 2^{\frac{2n}{\log n}}) = 2^{\frac{2n}{\log n}(1+o(1))},$$

з яких випливає, що

$$m = nlt = 2^{\frac{2n}{\log n}(1+o(1))},\ t_{\mathcal{B}} = 2^{\frac{2n}{\log n}(1+o(1))},$$

$$p_{\mathcal{B}} \geqslant 1 - tne^{-\lambda} - n\exp\{-1/2 \cdot \theta^{2r}t\} \geqslant 1 - \delta.$$

Таким чином, алгоритм $\mathcal{B}$, визначений у доведенні теореми 3.1, надає змогу розв'язувати (з імовірністю не менше ніж $1-\delta$) випадкові системи, що складаються з $2^{\frac{2n}{\log n}(1+o(1))}$ спотворених лінійних рівнянь від n змінних, використовуючи $2^{\frac{2n}{\log n}(1+o(1))}$ операцій над n-вимірними двійковими векторами.

3.10 Застосування функції сліду до розв'язання систем лінійних рівнянь зі спотвореними правими частинами над полями порядку 2^r

При побудові кореляційних атак на словоорієнтовані потокові шифри (такі як `SNOW 2.0`, `SOBER`, `SNOW 3G` або `Струмок`) постає необхідність розв'язання систем лінійних рівнянь зі спотвореними правими частинами над скінченними полями порядку, більшого ніж 2.

Розглянемо систему рівнянь вигляду (3.37), де A – $m \times n$-матриця над полем $\mathbb{F}_q$, $q = 2^r$, b – вектор довжини m з координатами вигляду (3.38), де $A_1, \ldots, A_m$ – рядки матриці A, $a = (a_1, \ldots, a_n)^T$ – невідомий вектор над полем $\mathbb{F}_q$ (істинний розв'язок системи (3.37)), $\xi_1, \ldots, \xi_m$ – незалежні випадкові величини, розподілені за законом $\Pr(\xi_i = z) = p(z)$, де $p(z) \geqslant 0$ для кожного $z \in \mathbb{F}_q$, $\sum\limits_{z \in \mathbb{F}_q} p(z) = 1$.

Задача розв'язання системи рівнянь (3.37) полягає у відновленні вектора a за відомими матрицею A, вектором b і розподілом ймовірностей $p_\xi = (p(z) : z \in \mathbb{F}_q)$, який надалі вважатимемо відмінним від рівномірного розподілу на $\mathbb{F}_q$. Опишемо метод вирішення цієї задачі, що базується на її зведенні до розв'язання систем лінійних рівнянь зі спотвореними правими частинами над полем з двох елементів.

Для будь-якого $z \in \mathbb{F}_{2^r}$ позначимо $\mathrm{Tr}(z) = z^2 \oplus z^{2^2} \oplus \ldots \oplus z^{2^{r-1}}$ *(абсолютний) слід* елемента z. Нагадаємо, що слід являє собою лінійне відображення поля $\mathbb{F}_q$ в поле $\mathbb{F}_2$. При цьому з рівності $\mathrm{Tr}(xy) = 0$ для усіх $x \in \mathbb{F}_q$ випливає, що $y = 0$.

Базиси $\mathfrak{B} = \{b_1, \ldots, b_r\}$ та $\mathfrak{B}' = \{b'_1, \ldots, b'_r\}$ поля $\mathbb{F}_{2^r}$ називаються *дуальними*, якщо виконується умова

$$\mathrm{Tr}(b_i b'_j) = \delta_{ij} = \begin{cases} 1, & \text{якщо } i = j; \\ 0, & \text{якщо } i \neq j,\ i, j \in \overline{1, r}. \end{cases}$$

Наступна лема випливає безпосередньо з означення поняття дуальності базисів.

Лема 3.4. *Нехай $x, y \in \mathbb{F}_q$, $(x_1, \ldots, x_r)$ та $(y'_1, \ldots, y'_r)$ – вектори координат елементів x та y в базисах $\mathfrak{B}$ та $\mathfrak{B}'$ відповідно. Тоді* $\mathrm{Tr}(xy) = x_1 y'_1 \oplus \ldots \oplus x_r y'_r$.

Повернемося до системи рівнянь (3.37), що задовольняє умову (3.38), над полем $\mathbb{F}_q$ та побудуємо за нею систему лінійних рівнянь зі спотвореними правими частинами над полем $\mathbb{F}_2$.

Зафіксуємо пару дуальних базисів $\mathfrak{B}$ і $\mathfrak{B}'$ поля $\mathbb{F}_q$ та елемент $\alpha \in \mathbb{F}_q \backslash \{0\}$. Помітимо, що з рівностей (3.38) випливають рівності

$$\mathrm{Tr}(b_i \alpha) = \mathrm{Tr}(A_i(a\alpha)) \oplus \mathrm{Tr}(\xi_i \alpha),\ i \in \overline{1, m},$$

причому на підставі леми 3.4 значення $\mathrm{Tr}(A_i(a\alpha))$ є скалярним добутком векторів A_i^* та a^* довжини nr над полем $\mathbb{F}_2$, які отримуються в результаті заміни кожної координати вектора A_i (відповідно, вектора $a\alpha$) її двійковим представленням у базисі $\mathfrak{B}$ (відповідно, у базисі $\mathfrak{B}'$). Звідси випливає, що вектор $a^* \in V_{nr}$ співпадає з істинним розв'язком системи лінійних рівнянь зі спотвореними правими частинами

$$A_i^* x = b_i^* = A_i^* a^* \oplus \eta_i,\ i \in \overline{1,m}, \tag{3.45}$$

де $b_i^* = \mathrm{Tr}(b_i\alpha)$, $\eta_i = \mathrm{Tr}(\xi_i\alpha)$ для кожного $i \in \overline{1,m}$.

Таким чином, для відновлення вектора a з системи рівнянь (3.37) достатньо побудувати для заздалегідь вибраного елемента $\alpha \in \mathbb{F}_q\backslash\{0\}$ систему рівнянь вигляду (3.45) над полем $\mathbb{F}_2$ та відновити її істинний розв'язок a^* одним з відомих методів. Знаючи вектор a^* та базис $\mathfrak{B}'$, можна отримати вектор αa, а отже, і шуканий вектор a.

Приклад 3.1. Розглянемо рівняння $a_1x_1 \oplus a_2x_2 = b$ над полем $\mathbb{F}_q$ (яке отримане в результаті множення невідомих певного вхідного лінійного рівняння на константу α).

Представимо елементи a_1 і a_2 у вигляді векторів їхніх координат в базисі $\mathfrak{B}$:

$$a_1 = (a_{1,1}, \ldots, a_{1,r}), a_2 = (a_{2,1}, \ldots, a_{2,r}),$$

а елементи x_1 і x_2 у вигляді векторів їхніх координат в базисі $\mathfrak{B}'$:

$$x_1 = (x'_{1,1}, \ldots, x'_{1,r}), x_2 = (x'_{2,1}, \ldots, x'_{2,r}).$$

Застосовуючи функцію сліду до доданків a_1x_1 та a_2x_2 вхідного рівняння, отримаємо

$$\mathrm{Tr}(a_1x_1) = a_{1,1}x'_{1,1} \oplus \ldots \oplus a_{1,r}x'_{1,r}, \mathrm{Tr}(a_2x_2) = a_{2,1}x'_{2,1} \oplus \ldots \oplus a_{2,r}x'_{2,r}.$$

Таким чином, вхідне рівняння над полем $\mathbb{F}_q$ перетворюється на лінійне рівняння над полем $\mathbb{F}_2$:

$$a_{1,1}x'_{1,1} \oplus \ldots \oplus a_{1,r}x'_{1,r} \oplus a_{2,1}x'_{2,1} \oplus \ldots \oplus a_{2,r}x'_{2,r} = \mathrm{Tr}(b).$$

Для зазначеного вище розподілу ймовірностей $p_\xi = (p(z) : z \in \mathbb{F}_q)$ позначимо $C_{p_\xi}(\alpha) = \sum\limits_{z\in\mathbb{F}_q} p(z)(-1)^{\mathrm{Tr}(z\alpha)}$. Зауважимо, що на підставі леми 3.4 параметр $C_{p_\xi}(\alpha)$ співпадає з коефіцієнтом Фур'є в точці α розподілу p_ξ як псевдобулевої функції, якщо ототожнити кожен її аргумент $z \in \mathbb{F}_q$ з вектором його координат у базисі $\mathfrak{B}$, а елемент α – з вектором його координат у базисі $\mathfrak{B}'$.

Доведемо твердження, яке містить відповідь на запитання про вигляд розподілу спотворень у правих частинах рівнянь системи (3.45).

Твердження 3.10. *Розподіл ймовірностей випадкової величини* $\eta_i = \mathrm{Tr}(\xi_i\alpha)$ *визначається за формулою*

$$\Pr(\eta_i = 0) = 1 - \Pr(\eta_i = 1) = 1/2 \cdot (1 + C_{p_\xi}(\alpha)).$$

Доведення. Дійсно, використовуючи послідовно означення випадкової величини η_i, формулу обернення для перетворення Фур'є (п. 3.5) та лінійність функції сліду, отримаємо, що

$$\Pr(\eta_i = 0) = \sum_{\substack{x\in\mathbb{F}_q:\\ \mathrm{Tr}(x\alpha)=0}} p(x) = \sum_{\substack{x\in\mathbb{F}_q:\\ \mathrm{Tr}(x\alpha)=0}} \left(q^{-1} \sum_{y\in\mathbb{F}_q} C_{p_\xi}(y)(-1)^{\mathrm{Tr}(xy)} \right) =$$

$$= q^{-1} \sum_{y\in\mathbb{F}_q} C_{p_\xi}(y) \sum_{\substack{x\in\mathbb{F}_q:\\ \mathrm{Tr}(x\alpha)=0}} (-1)^{\mathrm{Tr}(xy)} =$$

$$= 2^{-r}\left(2^{r-1}C_{p_\xi}(0) + 2^{r-1}C_{p_\xi}(\alpha) + \sum_{y\in\mathbb{F}_q\setminus\{0,\alpha\}} C_{p_\xi}(y) \sum_{\substack{x\in\mathbb{F}_q:\\ \mathrm{Tr}(x\alpha)=0}} (-1)^{\mathrm{Tr}(xy)}\right) =$$

$$= 1/2\cdot(1 + C_{p_\xi}(\alpha)),$$

де остання рівність випливає зі співвідношень

$$\sum_{\substack{x\in\mathbb{F}_q:\\ \mathrm{Tr}(x\alpha)=0}} (-1)^{\mathrm{Tr}(xy)} = |\{x\in\mathbb{F}_q : \mathrm{Tr}(xy) = \mathrm{Tr}(x\alpha) = 0\}| -$$

$$-|\{x\in\mathbb{F}_q : \mathrm{Tr}(xy) = 1, \mathrm{Tr}(x\alpha) = 0\}| = 2^{r-2} - 2^{r-2} = 0,\ y\notin\{0,\alpha\}.$$

□

Отже, на підставі доведеного твердження відхилення ймовірності спотворення у правій частині будь-якого рівняння системи (3.45) від 1/2 є тим більше, чим більше значення $|C_{p_\xi}(\alpha)|$. Таким чином, для зменшення складності розв'язання цієї системи рівнянь слід вибирати елемент α як точку максимуму модулів коефіцієнтів Фур'є розподілу p_ξ за всіма ненульовими елементами поля $\mathbb{F}_q$.

3.11 Кореляційна атака на спрощену версію SNOW 2.0-подібного потокового шифру

Розглянемо спрощену версію `SNOW 2.0`-подібного шифру, яка описується рівняннями (2.22) – (2.24). Безпосередньо з цих рівнянь випливає, що

$$(x_i \oplus x_{i+1} \oplus x_{i+\mu} \oplus x_{i+n-1} \oplus x_{i+n}) \oplus (u_i \oplus \sigma(u_i)) =$$

$$= \gamma_i \oplus \gamma_{i+1},\ i = 0, 1, \ldots. \tag{3.46}$$

Вважаючи, що змінні $u_0, u_1, \ldots$ у формулі (3.46) є незалежними випадковими величинами з рівномірним розподілом на полі $\mathbb{F}_{2^r}$ 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. 2.2, отримаємо систему лінійних рівнянь зі спотвореними правими частинами над полем $\mathbb{F}_{2^r}$, 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 скористаємося методом, описаним в п. 3.10, який полягає в множенні рівнянь вхідної системи на певний ненульовий елемент $\alpha \in \mathbb{F}_{2^r}$ та застосуванні функції сліду до обох частин кожного рівняння. Отримана таким чином система лінійних рівнянь зі спотвореними правими частинами визначається над полем $\mathbb{F}_2$ і для її розв'язання можна використовувати відомі алгоритми (наприклад, BKW).

Позначимо $\eta_i = \mathrm{Tr}((u_i \oplus \sigma(u_i))\alpha)$. На підставі твердження 3.10 мають місце рівності

$$(2\Pr(\eta_i = 0) - 1)^2 = \left(\sum_{z \in \mathbb{F}_{2^r}} \Pr(u_i \oplus \sigma(u_i) = z)\, (-1)^{\mathrm{Tr}(z\alpha)} \right)^2 =$$

$$= \left(2^{-r} \sum_{u \in \mathbb{F}_{2^r}} (-1)^{\mathrm{Tr}(u \oplus \sigma(u))\alpha)} \right)^2. \tag{3.47}$$

Отримаємо вираз параметра (3.47) в термінах підстановок s_j ($j \in \overline{0, p-1}$) та матриці D, від яких залежить підстановка σ (див. формулу (2.19)).

Попередньо введемо декілька додаткових позначень.

Нагадаємо, що згідно з п. 2.10 елементи поля $\mathbb{F}_{2^r}$ ототожнюються з двійковими векторами довжини r за допомогою двох базисів, $\mathfrak{B}_1$ і $\mathfrak{B}_2$, перший з яких є базисом поля $\mathbb{F}_{2^t}$ над підполем $\mathbb{F}_2$, а другий – базисом поля $\mathbb{F}_{2^r}$ над підполем $\mathbb{F}_{2^t}$. Якщо $u = (u_0, \ldots, u_{p-1})$ – довільний двійковий вектор, де $u_j \in V_t$ для кожного $j \in \overline{0, p-1}$, то вектори u_j ототожнюються з елементами поля $\mathbb{F}_{2^t}$ за допомогою базису $\mathfrak{B}_1$; при цьому вектору u ставиться у відповідність елемент поля $\mathbb{F}_{2^r}$, який дорівнює $\bigoplus\limits_{j=0}^{p-1} u_j b_j$, де $\mathfrak{B}_2 = \{b_0, \ldots, b_{p-1}\}$. Навпаки, довільному елементу $x \in \mathbb{F}_{2^r}$ ставиться у відповідність набір його координат $(x_0, \ldots, x_{p-1})$ в базисі $\mathfrak{B}_2$, кожна з яких ототожнюється з двійковим вектором довжини t за допомогою базису $\mathfrak{B}_1$: $x_j \in V_t$, $j \in \overline{0, p-1}$.

Позначимо $\mathfrak{B}'_2 = \{b'_0, \ldots, b'_{p-1}\}$ базис, дуальний до $\mathfrak{B}_2$, що визначається умовою $\mathrm{Tr}_{2^t}^{2^r}(b_i b'_j) = \delta_{ij}$, $i, j \in \overline{0, p-1}$, де $\mathrm{Tr}_{2^t}^{2^r}$ – функція сліду поля $\mathbb{F}_{2^r}$ над підполем $\mathbb{F}_{2^t}$. Позначимо також $\mathrm{Tr}_2^{2^t}$ слід поля $\mathbb{F}_{2^t}$ над підполем $\mathbb{F}_2$. Зауважимо, що внаслідок транзитивності сліду

$$\mathrm{Tr}(x) = \mathrm{Tr}_2^{2^t}(\mathrm{Tr}_{2^t}^{2^r}(x))$$

для будь-якого $x \in \mathbb{F}_{2^r}$. Нарешті, позначимо d_{ij} елементи матриці D, $i, j \in \overline{0, p-1}$.

Використовуючи введені позначення, на підставі формули (2.19) отримаємо, що елемент поля $\mathbb{F}_{2^r}$, який відповідає двійковому вектору $u \oplus \sigma(u)$, дорівнює

$$\left(\bigoplus_{j=0}^{p-1} u_j b_j\right) \oplus \bigoplus_{j=0}^{p-1} \left(\bigoplus_{i=0}^{p-1} s_i(u_i) d_{ij}\right) b_j.$$

Розкладаючи елемент $\alpha \in \mathbb{F}_{2^r}$ по базису $\mathfrak{B}'_2$:

$$\alpha = \bigoplus_{l=0}^{p-1} \alpha'_l b'_l$$

і використовуючи лінійність сліду та дуальність базисів $\mathfrak{B}_2$ й $\mathfrak{B}'_2$, отримаємо звідси, що

$$\mathrm{Tr}_{2^t}^{2^r}\left((u\oplus\sigma(u))\alpha\right) =$$

$$= \mathrm{Tr}_{2^t}^{2^r}\left(\left(\bigoplus_{j=0}^{p-1} u_j b_j\right)\left(\bigoplus_{l=0}^{p-1}\alpha'_l b'_l\right)\oplus\bigoplus_{j=0}^{p-1}\left(\bigoplus_{i=0}^{p-1} s_i(u_i)d_{ij}b_j\right)\left(\bigoplus_{l=0}^{p-1}\alpha'_l b'_l\right)\right) =$$

$$= \left(\bigoplus_{j=0}^{p-1} u_j\alpha'_j\right)\oplus\left(\bigoplus_{i=0}^{p-1} s_i(u_i)\left(\bigoplus_{j=0}^{p-1} d_{ij}\alpha'_j\right)\right) =$$

$$= \left(\bigoplus_{j=0}^{p-1} u_j\alpha'_j\right)\oplus\left(\bigoplus_{i=0}^{p-1} s_i(u_i)\beta'_i\right), \qquad (3.48)$$

де вектор $(\beta'_0,\ldots,\beta'_{p-1})$ над полем $\mathbb{F}_{2^t}$ визначається як результат множення вектора $(\alpha'_0,\ldots,\alpha'_{p-1})$ на матрицю D^T.

Використовуючи транзитивність сліду, отримаємо з формули (3.48), що

$$2^{-r}\sum_{u\in\mathbb{F}_{2^r}}(-1)^{\mathrm{Tr}((u\oplus\sigma(u))\alpha)} =$$

$$= 2^{-pt}\sum_{(u_0,\ldots,u_{p-1})\in(\mathbb{F}_{2^t})^p}(-1)^{\mathrm{Tr}_2^{2^t}(u_0\alpha'_0\oplus\ldots\oplus u_{p-1}\alpha'_{p-1}\oplus s_0(u_0)\beta'_0\oplus\ldots\oplus s_{p-1}(u_{p-1})\beta'_{p-1})} =$$

$$= 2^{-pt}\sum_{(u_0,\ldots,u_{p-1})\in(\mathbb{F}_{2^t})^p}(-1)^{\mathrm{Tr}_2^{2^t}((u_0\alpha'_0\oplus s_0(u_0)\beta'_0)\oplus\ldots\oplus(u_{p-1}\alpha'_{p-1}\oplus s_{p-1}(u_{p-1})\beta'_{p-1}))} =$$

$$= \prod_{j=0}^{p-1}\left(2^{-t}\sum_{u_j\in\mathbb{F}_{2^t}}(-1)^{\mathrm{Tr}_2^{2^t}(u_j\alpha'_j\oplus s_j(u_j)\beta'_j)}\right).$$

Таким чином, доведено наступне твердження.

Твердження 3.11. *Параметр (3.47) задовольняє рівність*

$$(2\Pr(\eta_i = 0) - 1)^2 = \prod_{j=0}^{p-1} l_j(\alpha'_j, \beta'_j),$$

де $(\alpha'_0, \ldots, \alpha'_{p-1})$ *– набір координат елемента* $\alpha \in \mathbb{F}_{2^r}$ *в базисі* $\mathfrak{B}'_2$, $(\beta'_0, \ldots, \beta'_{p-1}) = (\alpha'_0, \ldots, \alpha'_{p-1})D^T$,

$$l_j(\alpha'_j, \beta'_j) = \left(2^{-t} \sum_{u_j \in \mathbb{F}_{2^t}} (-1)^{\mathrm{Tr}_2^{2^t}(u_j\alpha'_j \oplus s_j(u_j)\beta'_j)}\right)^2, \ j \in \overline{0, p-1}. \quad (3.49)$$

Зауважимо, що на підставі леми 3.4 вираз $\mathrm{Tr}_2^{2^t}(u_j\alpha'_j \oplus s_j(u_j)\beta'_j)$ у формулі (3.49) можна замінити булевим скалярним добутком $u_j\alpha'_j \oplus s_j(u_j)\beta'_j$, якщо ототожнити елементи u_j, $s_j(u_j)$ з векторами їхніх координат у базисі $\mathfrak{B}_1$, а елементи α'_j, β'_j – з векторами їхніх координат у базисі $\mathfrak{B}'_1$.

Зауважимо також, що числа вигляду (3.49) називають іноді *елементами таблиці лінійних апроксимацій* підстановки s_j, $j \in \overline{0, p-1}$. Вони характеризують спроможність цієї підстановки протистояти лінійному методу криптоаналізу та звичайно використовуються при дослідженні стійкості блокових шифрів відносно лінійних атак.

Твердження 3.11 надає можливість обчислювати на практиці ймовірності спотворень у правих частинах рівнянь системи, яка формується для реалізації кореляційної атаки на спрощену версію `SNOW 2.0`-подібного шифру. Подальші відомості з цих питань, зокрема, щодо обґрунтування стійкості шифру `Струмок` відносно таких атак, можна знайти в [АКП1, АКП2].

3.12 Швидкі алгоритми відшукання лінійних наближень булевих функцій

Як зазначено вище, необхідною умовою стійкості потокових шифрів відносно кореляційних атак є відсутність високоймовірних лінійних наближень булевих функцій, що реалізуються за допомогою компонентів зазначених шифрів. Тому задача відшукання таких наближень є важливою для кореляційного криптоаналізу.

Ця задача формулюється наступним чином. Задано булеву функцію $f : V_n \to \{0,1\}$ та число $\varepsilon \in (0,1)$. Треба побудувати множину

$$L_\varepsilon(f) = \{\alpha \in V_n : d(f, l_\alpha) \leqslant 1/2 \cdot (1-\varepsilon)\}, \tag{3.50}$$

де $l_\alpha(x) = \alpha x$, $x \in V_n$ – лінійна булева функція з вектором коефіцієнтів α, $d(f, l_\alpha) = \Pr(f(X) \neq l_\alpha(X))$ – ймовірність неспівпадання значень функцій f та l_α при випадковому рівноймовірному виборі аргументу X.

Зауважимо, що на підставі твердження 3.7

$$L_\varepsilon(f) = \{\alpha \in V_n : 2^{-n}\hat{f}(\alpha) \geqslant \varepsilon\}.$$

При цьому функція f може бути задана *вектором значень* (тобто таблицею істинності, яку можна зберігати у пам'яті) або *за допомогою оракула* (певного алгоритму, який надає змогу обчислювати її значення). Другий спосіб часто-густо зустрічається на практиці, коли булева функція залежить від багатьох (наприклад, 128 чи більшої кількості) змінних; як приклад, відзначимо окремий знак гами, що виробляється генератором, як функцію його початкового стану.

Відомі алгоритми відшукання лінійних наближень булевих функцій від n змінних поділяють на *детерміновані* та *ймовірнісні*.

Детерміновані алгоритми є застосовними до функцій, заданих таблично, і надають змогу будувати множину (3.50) без помилок. Найбільш відомим з них є алгоритм швидкого перетворення Адамара, складність якого становить $O(n2^n)$ цілочисельних (або $O(n^2 2^n)$ двійкових) операцій; див. п. 3.6 та задачу 3.31.

Менш трудомістким є детермінований алгоритм, запропонований в [ДКТ], зі складністю $O(2^n \min\{\ln^2(\varepsilon^{-2}), n^2\})$ двійкових операцій. (При фіксованому ε і достатньо великих значеннях n двійкова складність цього алгоритму становить $O(2^n \ln^2(\varepsilon^{-2}))$, в той час як алгоритм швидкого перетворення Адамара має двійкову складність $O(2^n n^2)$).

Ймовірнісні алгоритми відшукання лінійних наближень є застосовними до булевих функцій, заданих за допомогою оракулів, і можуть припускатися помилок. Найперший з них належить О. Гольдрайху та Л. Левіну [GL]; складність цього алгоритму залежить поліноміально від параметрів n та ε^{-1}. Найкращі на сьогодні модифікації алгоритму Гольдрайха-Левіна [BJT], [ADKT] мають двійкову складність $\widetilde{O}(n\varepsilon^{-2})$, де $\widetilde{O}(\cdot)$ позначає порядок величини з точністю до логарифмічних співмножників.

Для демонстрації основних ідей, які використовуються при побудові зазначених алгоритмів, розглянемо таку задачу.

Нехай f – булева функція від n змінних, задана за допомогою оракула, для якої існує вектор $\alpha \in V_n$ такий, що

$$d(f, l_\alpha) \leqslant 1/4 \cdot (1 - \varepsilon), \tag{3.51}$$

де $\varepsilon \in (0, 1)$. Треба відшукати цей вектор.

Зауважимо, що зазначений вектор α визначається однозначно (див. задачу 3.32). Позначимо α_i його i-у координату, e_i – двійковий вектор довжини n, усі координати якого, за виключенням i-ї,

дорівнюють нулю, та помітимо, що на підставі рівності (3.51)

$$2^{-n}||f(x\oplus e_i)\oplus f(x)\oplus\alpha_i||=$$

$$=2^{-n}||f(x\oplus e_i)\oplus l_\alpha(x\oplus e_i)\oplus f(x)\oplus l_\alpha(x)||\leqslant$$

$$\leqslant 2^{-n}||f(x\oplus e_i)\oplus l_\alpha(x\oplus e_i)||+2^{-n}||f(x)\oplus l_\alpha(x)||=$$

$$=d(f,l_\alpha)+d(f,l_\alpha)\leqslant 1/2\cdot(1-\varepsilon),\ i\in\overline{1,n}.$$

Звідси випливає, що при $\alpha_i=0$ відносна вага функції $D_if(x)=f(x\oplus e_i)\oplus f(x)$, $x\in V_n$, не перевищує $1/2\cdot(1-\varepsilon)$, в той час як при $\alpha_i=1$ відносна вага цієї функції є не менше ніж $1/2\cdot(1+\varepsilon)$.

Отже, для відшукання зазначеного вектора α можна скористатися *таким алгоритмом.*

Для кожного $i\in\overline{1,n}$:

1) згенерувати незалежні випадкові вектори $X_1,\ldots,X_t$ з рівномірним розподілом на множині V_n та обчислити значення

$$\xi_t=\frac{1}{t}\sum_{j=1}^{t}D_if(X_j);$$

2) якщо $\xi_t<1/2$, покласти $\alpha_i=0$, інакше покласти $\alpha_i=1$.

Твердження 3.12. *Нехай* $t=\left\lceil 2\varepsilon^{-2}\ln(\delta^{-1}n)\right\rceil$, *де* $\delta\in(0,1)$. *Тоді наведений алгоритм надає змогу відновити шуканий вектор* α *з ймовірністю не менше за* $1-\delta$, *використовуючи* $O(tn)$ *запитів до оракула, що реалізує функцію* f.

Доведення. Покажемо, що для кожного $i\in\overline{1,n}$ ймовірність помилкового відновлення значення α_i не перевищує δn^{-1}. Тоді ймовірність помилки алгоритму є не вище ніж δ.

Нехай $\alpha_i = 0$ і алгоритм припускається помилки. Тоді $\xi_t \geqslant 1/2$, в той час як $\mathbb{E}\xi_i = 2^{-n}||D_i f|| \leqslant 1/2 \cdot (1 - \varepsilon)$. Отже, на підставі леми 3.1 ймовірність помилкового відновлення значення α_i не перевищує

$$\Pr\left(\xi_t \geqslant 1/2\right) \leqslant \Pr\left(\xi_t - \mathbb{E}\xi_t \geqslant 1/2 - 1/2 \cdot (1 - \varepsilon)\right) \leqslant$$

$$\leqslant \exp\left\{-1/2 \cdot t\varepsilon^2\right\} \leqslant \delta n^{-1},$$

де остання нерівність випливає з означення параметра t.

Аналогічно можна довести, що при $\alpha_i = 1$ ймовірність помилкового відновлення цього значення також не перевищує δn^{-1}.

Нарешті, твердження про кількість запитів випливає безпосередньо з опису алгоритму.

□

Таким чином, якщо для булевої функції від n змінних існує лінійна функція, яка відрізняється від неї менше ніж на $1/4$ вхідних наборах, то цю лінійну функцію можна відновити із заздалегідь визначеною достовірністю за субквадратичний від n час.

Задачі до розділу 3

Задача 3.1. Доведіть, що булева функція є алгебраїчно виродженою тоді й тільки тоді, коли вона має ненульовий несуттєвий вектор.

Задача 3.2. Доведіть, що булева функція від n змінних є s-вимірною тоді й тільки тоді, коли вона має не менше ніж $n-s$ лінійно незалежних несуттєвих векторів, $s \in \overline{0, n-1}$.

Задача 3.3. Нехай f є s-вимірною, але не $(s-1)$-вимірною функцією від n змінних, $s \in \overline{1, n-1}$. Доведіть, що існують булева $n \times s$-матриця A рангу s та булева функція g від s змінних, яка не має ненульових несуттєвих векторів, такі, що $f(x) = g(xA)$ для кожного $x \in V_n$. Чи визначається така пара (A, g) для функції f однозначно?

Задача 3.4. Нехай f – булева функція від n змінних, A – $n \times s$-матриця рангу s, де $s \in \overline{1, n-1}$. Для будь-якої функції $h : V_s \to \{0, 1\}$ позначимо g_h булеву функцію вигляду $g_h(x) = h(xA)$, $x \in V_n$. Знайдіть функцію $h_* : V_s \to \{0, 1\}$ таку, що

$$||f \oplus g_{h_*}|| = \min_h ||f \oplus g_h||.$$

Задача 3.5. 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 $1 \leqslant i_1 < \ldots < i_k \leqslant n$ 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 (3.23), є незастосовною до генератора гами з кореляційно-імунною порядку k (збалансованою) комбінувальною функцією.

Задача 3.6. Доведіть, що збалансована 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 збалансованими.

Задача 3.7. Доведіть твердження 3.3.

Задача 3.8. Знайдіть коефіцієнти Фур'є булевої функції f, якщо її вектор значень дорівнює

а) $(1,0,1,1,0,0,1,0)$;

б) $(0,0,1,1,0,0,1,1)$;

в) $(1,1,0,1,0,1,1,0)$;

г) $(1,1,1,0,0,1,0,1)$.

Задача 3.9. Знайдіть коефіцієнт Фур'є $C_f(\alpha)$ псевдобулевої функції $f(x_1,\ldots,x_n) = (1+x_1)\ldots(1+x_n)$ при $\alpha = (1,1,\ldots,1)$.

Задача 3.10. Доведіть твердження 3.5.

Задача 3.11. Нехай f – булева функція від n змінних, X та Y – незалежні випадкові рівноймовірні двійкові вектори довжини n. Доведіть, що

$$\Pr\left(f(X)\oplus f(Y) = f(X\oplus Y)\right) = 1/2\cdot\left(1+2^{-3n}\sum_{\alpha\in V_n}\hat{f}(\alpha)^3\right).$$

Задача 3.12. Знайдіть афінні статистичні аналоги функцій, які наведені в задачі 3.8. Обчисліть нелінійність кожної з цих функцій.

Задача 3.13. Знайдіть всі найбільш ймовірні статистичні аналоги булевої функції $x_1x_2\oplus x_3\oplus\ldots\oplus x_n$.

Задача 3.14. Покажіть, що будь-яка бент-функція від $n > 2$ змінних має парну вагу.

Задача 3.15. Нехай f, g – булеві функції від n змінних, причому існують оборотна булева $n \times n$-матриця A і вектор $b \in V_n$ такі, що $g(x) = f(xA \oplus b)$, $x \in V_n$. Доведіть, що коефіцієнти Уолша-Адамара цих функцій збігаються з точністю до знака та перестановки (зокрема, якщо f є бент-функцією, то g також є бент-функцією).

Задача 3.16. Розглянемо систему рівнянь (3.37), що задовольняє умови (3.38), (3.39). Припустимо, що матриця коефіцієнтів системи є фіксованою, а вектор a – випадковим і не залежить від випадкових величин $\xi_1, \ldots, \xi_m$. Розв'язання системи (3.37) *методом максимуму правдоподібності* полягає в знаходженні вектора $x^* \in V_n$, для якого досягається максимум умовних ймовірностей $\Pr(Aa \oplus \xi = b \,/\, a = x)$ за всіма $x \in V_n$ такими, що $\Pr(a = x) > 0$. Доведіть: якщо закон розподілу вектора a є рівномірним на множині V_n, то метод максимуму правдоподібності має найменшу ймовірність помилки серед усіх процедур відновлення істинного розв'язку системи рівнянь (3.37).

Задача 3.17. Доведіть, що у випадку, коли в формулі (3.39) $\theta_i = \theta$ для кожного $i \in \overline{1,m}$ розв'язання системи рівнянь (3.37) методом максимуму правдоподібності є рівносильним знаходженню такого вектора $\widehat{x} \in V_n$, для якого досягається мінімум значень $||Ax \oplus b||$ за всіма $x \in V_n$.

Задача 3.18. Розглянемо систему рівнянь (3.37), що задовольняє умови (3.38), (3.39), де $\theta_i = \theta$, $i \in \overline{1,m}$. Припустимо, що матриця коефіцієнтів цієї системи рівнянь вибирається випадково рівноймовірно (та незалежно від випадкових величин $\xi_1, \ldots, \xi_m$) з множини булевих матриць розміру $m \times n$. Доведіть, що за умови $m \geqslant \left\lceil 8\theta^{-2} \ln(2^n \delta^{-1}) \right\rceil$, де $\delta \in (0,1)$, метод максимуму правдоподібно-

сті надає змогу відновити істинний розв'язок системи з ймовірністю не меншою за $1-\delta$.

Задача 3.19. Знайдіть найбільш правдоподібний розв'язок системи лінійних рівнянь зі спотвореними правими частинами $Ax = b$, якщо:

а) $A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$, $b = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}$; б) $A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$, $b = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$.

Задача 3.20. Нехай f – булева функція від n змінних, L – k-вимірний підпростір векторного простору V_n, $L^\perp$ – підпростір, дуальний до L, $\alpha \in V_n$. Доведіть, що

$$2^{-k} \sum_{x \in L} \hat{f}(x)^2 = \sum_{\alpha \in L^\perp} \sum_{x \in V_n} (-1)^{D_\alpha f(x)},$$

$$2^{-k} \sum_{x \in L \oplus \alpha} (-1)^{f(x)} = 2^{-n} \sum_{x \in L^\perp} \hat{f}(x)(-1)^{x\alpha},$$

де $D_\alpha f(x) = f(x \oplus \alpha) \oplus f(x)$ – похідна функції f за напрямом α.

Задача 3.21. Доведіть, що булева функція від n змінних є s-вимірною, $s \in \overline{0, n-1}$, тоді й тільки тоді, коли множина $\{\alpha \in V_n : \hat{f}(\alpha) \neq 0\}$ породжує у векторному просторі V_n підпростір вимірності не вище за s.

Задача 3.22. Доведіть, що функція $f : V_n \to \{0, 1\}$ є кореляційно-імунною порядку k тоді й тільки тоді, коли $\hat{f}(\alpha) = 0$ для кожного ненульового вектора $\alpha \in V_n$, що має вагу не вище за k.

Задача 3.23. Нехай f – булева функція від n змінних. За означенням функція f задовольняє *критерію поширення за напрямом* $\alpha \in V_n$, якщо виконується рівність

$$\Pr\left(f(X \oplus \alpha) = f(X)\right) = 1/2,$$

де X – випадковий рівноймовірний двійковий вектор довжини n. Визначимо функцію $h : V_n \to \mathbb{R}$ таким чином: $h(x) = \hat{f}(x)^2$, $x \in V_n$. Доведіть, що функція f задовольняє критерій поширення за напрямом $\alpha \in V_n \backslash \{0\}$ тоді й тільки тоді, коли $C_h(\alpha) = 0$.

Задача 3.24. Нехай f – булева функція від n змінних,

$$L_f = \{\alpha \in V_n |\ \forall x \in V_n : f(x \oplus \alpha) = f(x)\}.$$

Визначимо булеву функцію h від n змінних, вважаючи, що $h(x) = 1 \Leftrightarrow \hat{f}(x) \neq 0$, $x \in V_n$. Доведіть, що $\alpha \in V_n \backslash \{0\}$ належить L_f тоді й тільки тоді, коли $C_h(\alpha) = C_h(0)$. Переконайтесь, що $L_f = \{0\}$ якщо $||h|| > 2^{n-1}$.

Задача 3.25. Нехай f – булева функція від n змінних та $\mathrm{AI}(f) = d$. Доведіть, що

$$N_f \geqslant \sum_{i=0}^{d-2} \binom{n}{i}.$$

Задача 3.26. Нехай f – бент-функція від $n \geqslant 4$ змінних. Доведіть, що $\mathrm{AI}(f) \geqslant 2$.

Задача 3.27. Оцініть трудомісткість розв'язання системи лінійних рівнянь зі спотвореними правими частинами (3.37) над полем $\mathbb{F}_q$, де $q = 2^r$, за допомогою методу, викладеного в п. 3.10, якщо за-

кон розподілу спотворень у правих частинах рівнянь визначається за формулою $p(z) = q^{-1}(1 + (-1)^{f(z)}\theta)$, $z \in \mathbb{F}_q$, де

а) f є відмінною від константи лінійною булевою функцією від r змінних, $\theta \in (0, 1)$;

б) $f(z) = z_1 \oplus z_2 \oplus g(z_3, \ldots, z_r)$, $z = (z_1, \ldots, z_r) \in \mathbb{F}_q$, r є парним числом, а g – бент-функцією, $\theta \in (0, 1)$.

Задача 3.28. Доведіть, що параметр (3.47) не перевищує величини $(l_{max})^{\left\lceil \frac{B(D^T)}{2} \right\rceil}$, де l_{max} дорівнює максимальному значенню параметрів (3.49) за всіма ненульовими векторами α'_j, β'_j та числами $j \in \overline{0, p-1}$, а

$$B(D^T) = \min\{\mathrm{Wt}(z) + \mathrm{Wt}(zD^T) : z \in (\mathbb{F}_{2^t})^p \backslash \{0\}\},$$

де $\mathrm{Wt}(z)$ позначає число ненульових координат вектора z у базисі $\mathfrak{B}'_2$.

Задача 3.29. Підстановка $\sigma : V_r \to V_r$ називається *ортоморфізмом*, якщо відображення $u \mapsto u \oplus \sigma(u)$, $u \in V_r$ також є підстановкою. Доведіть, що при $r = 2m$ ортоморфізмом є підстановка

$$\sigma(u_1, u_2) = (u_1 \oplus \varphi(u_2), u_2 \oplus \varphi(u_1 \oplus \varphi(u_2))),\ u_1, u_2 \in V_m,$$

яка реалізується двохраундовою мережею Фейстеля з бієктивною раундовою функцією $\varphi : V_m \to V_m$. Переконайтесь, що у випадку, коли σ є ортоморфізмом, кореляційна атака на спрощену версію `SNOW 2.0`-подібного шифру (п. 3.11) є незастосовною.

Задача 3.30. Нехай f – булева функція від n змінних, $\varepsilon \in (0, 1)$. Доведіть, що потужність множини (3.50) не перевищує ε^{-2}.

Задача 3.31. Доведіть, що двійкова складність обчислення коефіцієнтів Уолша-Адамара булевої функції від n змінних за допомогою алгоритму швидкого перетворення Адамара становить $O(2^n n^2)$ операцій.

Задача 3.32. Доведіть, що для булевої функції f від n змінних існує не більше одного вектора $\alpha \in V_n$ такого, що $d(f, l_\alpha) < 1/4$.

Перелік посилань

[АКП1] *Алексейчук А. Н., Конюшок С. Н., Поремский М. В.* Верхние оценки несбалансированности дискретных функций, реализуемых последовательностями конечных автоматов. – Кибернетика и системный анализ, т. 55, №5, с. 58-66, 2019.

[АКП2] *Алексейчук А. Н., Конюшок С. Н., Поремский М. В.* Метод оценивания стойкости SNOW 2.0-подобных шифров относительно корреляционных атак над конечными расширениями поля из двух элементов. – Кибернетика и системный анализ, т. 56, №1, с. 59-63, 2020.

[АКС1] *Алексейчук А. Н., Конюшок С. Н., Сторожук А. Ю.* Статистическая атака на генератор гаммы с линейным законом реинициализации начального состояния и функцией усложнения, близкой к алгебраически вырожденной. – Радиотехника, вып. 176, с. 13-21, 2014.

[АКС2] *Алексейчук А. Н., Конюшок С. Н., Сторожук А. Ю.* Обобщенная статистическая атака на синхронные поточные шифры. – Захист інформації, т. 17, № 3, с. 54-65, 2015.

[ДКТ] *Думер И. И., Кабатянский Г. А., Тавернье С.* Списочное декодирование двоичных кодов Рида-Маллера первого порядка. – Проблемы передачи информации, т. 43, вып. 3, с. 66-74, 2007.

[ДСТУ1] ДСТУ 8845:2019 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного потокового перетворення».

[ДСТУ2] ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення».

[Ков] *Коваленко І. М.* Про алгоритм субекспоненціальної складності декодування сильно спотворених лінійних кодів. – Доп. АН УРСР, сер. А, № 10, с. 16-17, 1988.

[Ол] *Олексійчук А. М.* Суб'експоненційні алгоритми розв'язання систем лінійних булевих рівнянь зі спотвореними правими частинами. – Прикладная радиоэлектроника: науч.-техн. журн., т. 11, №2, с. 128-136, 2012.

[ADKT] *Abdouli A. S., Dumer I., Kabatiansky G., Tavernier C.* The Goldreich-Levin algorithm with reduced complexity. – Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT 2012), pp. 7-14, Pomorie, Bulgaria, June 15-21, 2012.

[AF] *Ars G., Faugère J.-C.* Algebraic immunities of functions over finite fields. – Technical Report, INRIA, 2003.

[Bab] *Babbage S.* A space/time tradeoff in exhaustive search attacks on stream ciphers. – European Convention on Security and Detection, IEE Conference Publication No. 408, May 1995.

[BFS] *Bardet M., Faugère J.-C., Salvy B.* On the complexity of Groëbner basis computation for semi-regular overdetermined sequences over $\mathbb{F}_2$ with solutions in $\mathbb{F}_2$. – Technical Report 5049, INRIA, 2003.

[BG] *Berbain C., Gilbert H.* On the security of IV dependent stream ciphers. – Biryukov A. (ed.) FSE 2007. LNCS, vol. 4593, pp. 254-273, Springer, Heidelberg, 2007.

[BillG] *Billet O., Gilbert H.* Resistance of SNOW 2.0 against algebraic attacks. – Menezes A. (ed.) CT-RSA 2005. LNCS, vol. 3376, pp. 19-28, Springer, Heidelberg, 2005.

[BJT] *Bshouty N., Jackson J., Tamon C.* More efficient PAC-learning of DNF with membership queries under the uniform distribution. – Proc. of COLT'99, pp. 286-295, 1999.

[BKW] *Blum A., Kalai A., Wasserman H.* Noise-tolerant learning, the parity problem, and the statistical query model. – J. ACM, vol. 50, №3, pp. 506-519, 2003.

[BMT] *Berlekamp E. R., McElice R. J., van Tilborg H.* On the inherent intractability of certain coding problems. – IEEE Trans. Inform. Theory, vol. 24, № 3, pp. 384-386, 1978.

[BTV] *Bogos S., Tramèr F., Vaudenay S.* On solving LPN using BKW and variants. Implementation and analysis. – Cryptology ePrint Archive, report 2015/049, `http://eprint.iacr.org/2015/049`.

[Can+] *Canteaut A., Naya-Plasencia M.* Correlation attacks on combination generators. – Cryptogr. Commun., vol. 4, №3-4, pp. 147-171, 2012.

[CM] *Courtois N. T., Meier W.* Algebraic attacks on stream ciphers with linear feedback. – Boneh D. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 345-359, Springer, Heidelberg, 2003.

[DGV] *Daemen J., Govaerts R., Vandewalle J.* Resynchronization weaknesses in synchronous stream ciphers. – Helleseth T. (ed.) EUROCRYPT 1993. LNCS, pp. 159-167, Springer-Verlag, 1993.

[GL] *Goldreich O., Levin L. A.* A hard core predicate for all one-way functions. – Proc. 21 ACM Sympos. of Theory of Computing, pp. 25-32, 1989.

[Gol] *Golić J.* Cryptanalysis of alleged A5 stream cipher. – Fumy W. (ed.) EUROCRYPT 1997. LNCS, vol. 1233, pp. 239-255, 1997.

[Hoe] *Hoeffding W.* Probability inequalities for sums of bounded random variables. – J. Amer. Statist. Assoc., vol. 58, № 301, 1963.

[Huff] *Huffman D.* Canonical forms for information loss less finite state logical machines. – IRE Trans. Circuit Theory, vol. 6, spec. suppl., pp. 41-59, 1959.

[KL] *Katz J., Lindell Y.* Introduction to modern cryptography (2nd ed.). – CRC Press, 2015.

[OZ] *Ovchinnikov A., Zobnin A.* Classification and applications of monomial orderings and the properties of differential orderings. – Ganzha V., Mayer E. and Vorozhtsov E. (ed.) Proc. CASC'02, pp. 237-252, 2002.

[Sie] *Siegenthaler T.* Decrypting a class of stream ciphers using ciphertext only. – IEEE Trans. Comput., vol. 34, pp. 81-84, 1985.

[SM] *Semaev I., Mikuš M.* Methods to solve algebraic equations in cryptanalysis. – Tatra Mt. Math. Publ., vol. 45, pp. 107-136, 2010.

[ST] *Semaev I., Tenti A.* Probabilistic analysis on Macaulay matrices over finite fields and complexity of constructing Groëbner bases. – J. Algebra, vol. 565, pp. 651-674, 2021.

[Zen] *Zenner E.* On the efficiency of the clock control guessing attack. – ICISC, pp. 200-212, 2002.

Предметний покажчик