

ПЕРІОДИЧНІ ВЛАСТИВОСТІ ШИФРГАМИ У РЕЖИМІ OUTPUT FEEDBACK*О.О. КУЗНЕЦОВ, Ю.І. ГОРБЕНКО, Є.П. КОЛОВАНОВА*

Досліджуються властивості режиму гамування зі зворотним зв'язком за шифрговою (англомовне позначення – Output Feedback). Із застосуванням математичного апарату теорії підстановок досліджуються періодичні властивості гами, зокрема проводиться оцінка ймовірності появи гами певного періоду за умови відповідності властивостей блокового симетричного шифру певним властивостям випадкової підстановки. Розробляються практичні рекомендації щодо застосування режиму гамування зі зворотним зв'язком за шифрговою, обґрунтовуються вимоги та обмеження, що випливають із отриманих оцінок періодичних властивостей гами.

Ключові слова: режим шифрування, періодичність гами, випадкова підстановка, Output Feedback.

ВСТУП

Для забезпечення інформаційної безпеки в умовах реальних та потенційних загроз, зокрема, від несанкціонованого доступу до інформаційних ресурсів, у тому числі, внаслідок використання іноземних інформаційних технологій, Адміністрацією Держспецзв'язку України ініційовано розробку вітчизняного криптографічного алгоритму симетричного блокового перетворення [1, 2]. Його призначено для забезпечення взаємної сумісності засобів криптографічного захисту інформації різних виробників, що застосовуються для вирішення завдань конфіденційності, цілісності та інших послуг безпеки, у тому числі для захисту публічної інформації, яка обробляється та циркулює в інформаційно-телекомунікаційних системах.

Специфікацію нового алгоритму симетричного блокового криптоперетворення визначено у проекті національного стандарту ДСТУ “Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення” [1, 2], в якому передбачено можливість забезпечення конфіденційності та цілісності повідомлення шляхом послідовного застосування відповідних перетворень. Однак властивості криптоперетворень залежать не тільки від характеристик шифру, але й від режимів його застосування. Тому у проекті стандарту передбачено 10 режимів криптоперетворення: проста заміна (базове перетворення), гамування, гамування зі зворотним зв'язком за шифр-текстом, вироблення імітовставки, зчеплення шифрблоків, гамування зі зворотним зв'язком за шифрговою, вибіркоче гамування із прискореним виробленням імітовставки, вироблення імітовставки і гамування, індексованої заміни, захисту ключових даних [1, 2].

Одним із найбільш поширених режимів блокового симетричного шифрування, який застосовується для забезпечення послуги конфіденційності, є режим гамування зі зворотним зв'язком за шифрговою (в англійських виданнях застосовується позначення Output Feedback – OFB). У цьому режимі вихідне повідомлення не підлягає криптоперетворенню, тобто не шифрується

у звичайному розумінні. Конфіденційність повідомлення забезпечується шляхом додавання до нього шифргою, яка формується багаторазовим шифруванням одного й того самого несекретного блоку ініціалізації (у вітчизняній термінології застосовується поняття синхропосилки). На приймальній стороні знову формується шифргою, дію якої знімають з криптограми.

Таким чином, режим OFB має кілька переваг: по-перше, шифргою може бути сформована заздалегідь, ще до появи повідомлення, внаслідок чого можна значно прискорити процес захисту інформації; по-друге, в цьому режимі, як і в режимі простої заміни (Electronic Codebook – ECB), помилки, що можуть виникнути при передачі шифротексту по каналах зв'язку, локалізуються в блоці, не поширюючись на сусідні, причому в режимі OFB помилковими будуть лише біти, які підлягали зміні (в режимі ECB зміниться весь блок); по-третє, криптографічні властивості шифргою не залежать від відкритого тексту, вони визначаються лише властивостями базового криптоперетворення, та, можливо, значенням блоку ініціалізації (синхропосилки), який і визначає конкретний вигляд та періодичність гами. Саме вивченню періодичних властивостей шифргою у режимі OFB і присвячена ця робота, адже виникнення повторення гами є найбільш небезпечним випадком, що дає зловмисникові можливість порушити встановлений режим конфіденційності повідомлень.

Робота структурована наступним чином. У розділі 2 наводиться опис режиму гамування зі зворотним зв'язком за шифрговою. При викладенні режиму застосовується термінологія і основні позначення з проекту національного стандарту ДСТУ “Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення” [1, 2]. У розділі 3 вивчається зв'язок предмета дослідження із загальними положеннями теорії підстановок [3–5], зокрема, вводяться основні поняття та визначення, які пов'язуються із певними властивостями симетричних блокових криптоперетворень, наводяться основні аналітичні співвідношення, які застосовуються в ході вивчення

випадкових підстановок, зокрема, відомі розподіли кількості циклів, зростають та інверсій тощо. Розділ 4 присвячено викладенню основних теоретичних результатів, отриманих в цій роботі. Зокрема, із застосуванням розподілів кількостей циклів певної довжини випадкової підстановки виводиться формула для оцінки ймовірності появи циклу для довільного фіксованого значення множини перетворень. Ця властивість має безпосереднє відношення до періодичних властивостей шифрґами, бо характеризує ймовірнісний розподіл появи гам певного періоду за умови виконання припущення щодо відповідності властивостей блокового симетричного шифру (БСШ) певним властивостям випадкової підстановки. У розділі 5 наводиться докладний приклад розрахунку ймовірностей появи циклу заданої довжини у випадково обраній підстановці, тобто в цьому розділі на прикладі з докладними поясненнями демонструється справедливість отриманої формули та наведених комбінаторних міркувань. Розділ 6 присвячено інтерпретації отриманих результатів щодо вивчення властивостей блокових шифрів, зокрема, наводяться результати оцінки ймовірності появи шифрґами з різною довжиною періоду. Також у цьому розділі вирішуються конкретні практичні задачі, а саме розробляються рекомендації щодо застосування режиму гамування зі зворотним зв'язком за шифрґамою, обґрунтовуються певні вимоги та обмеження. У висновках узагальнюються та конкретизуються отримані результати, обговорюються можливі шляхи подальших досліджень.

1. РЕЖИМ ГАМУВАННЯ ЗІ ЗВОРОТНИМ ЗВ'ЯЗКОМ ЗА ШИФРґАМОЮ

Режим гамування зі зворотним зв'язком за шифрґамою призначено для забезпечення послуги конфіденційності. Цей режим засновано на шифруванні вектора ініціалізації (синхропосилки) для генерації послідовності вихідних блоків (шифрґами), які додаються до звичайного тексту, щоб сформувати зашифрований текст і, навпаки, до шифртексту для його розшифрування. Режим вимагає, аби вектор ініціалізації (синхропосилка) був унікальним для кожного застосування із наданим (фіксованим) ключем. Розглянемо специфікацію режиму гамування зі зворотним зв'язком за шифрґамою, яку наведено у проекті національного стандарту БСШ «Калина» [1, 2].

Відповідно до специфікації режим гамування зі зворотним зв'язком за шифрґамою позначається як Калина- l/k -OFB. Він забезпечує конфіденційність повідомлення шляхом шифрування. Шифрування виконує пряме відображення повідомлення M ($|M| \geq 1$) у шифртекст C , $|C| = |M|$, та обернене відображення шифртексту C у повідомлення M . Вимоги на кратність довжини повідомлення розміру блоку базового перетворення не накладаються. Параметрами

режиму є ключ шифрування K , $|K| = k$ та синхропосилка S , $|S| = l$. Додаткові вимоги щодо синхропосилки не накладаються.

В ході зашифрування повідомлення M ($|M| \geq 1$) подається у вигляді послідовності блоків:

$$M = m_1 \parallel m_2 \parallel \dots \parallel m_n, |m_i| = l,$$

для $i = 1, 2, \dots, n-1, 1 \leq m_n \leq l$.

Початкове значення блока гами γ_0 ($|\gamma_0| = l$) обчислюється як

$$\gamma_0 = T_{l,k}^{(K)}(S). \tag{1}$$

Кожен з блоків шифртексту обчислюється відповідно до співвідношення

$$c_i = m_i \oplus L_{l,|m_i|}(\gamma_{i-1}), \tag{2}$$

для $i = 1, 2, \dots, n$, та

$$\gamma_i = T_{l,k}^{(K)}(\gamma_{i-1}), \tag{3}$$

для $i = 1, 2, \dots, n-1$.

Результатом зашифрування повідомлення є шифртекст $C = c_1 \parallel c_2 \parallel \dots \parallel c_n$.

В ході розшифрування шифртексту C ($|C| \geq 1$) подається у вигляді послідовності блоків:

$$C = c_1 \parallel c_2 \parallel \dots \parallel c_n, |c_i| = l$$

для $i = 1, 2, \dots, n-1, 1 \leq c_n \leq l$.

Початкове значення блока гами γ_0 ($|\gamma_0| = l$) обчислюється як

$$\gamma_0 = T_{l,k}^{(K)}(S).$$

Кожен з блоків повідомлення обчислюється відповідно до співвідношення

$$m_i = c_i \oplus L_{l,|m_i|}(\gamma_{i-1}), \tag{4}$$

для $i = 1, 2, \dots, n$, та

$$\gamma_i = T_{l,k}^{(K)}(\gamma_{i-1}),$$

для $i = 1, 2, \dots, n-1$.

Результатом розшифрування шифртексту є повідомлення $M = m_1 \parallel m_2 \parallel \dots \parallel m_n$.

Схему зашифрування та розшифрування у режимі гамування зі зворотним зв'язком за шифрґамою наведено на рис. 1. Ця схема формально зображує послідовність виконання перетворень (2), (4) за всіма значеннями циклової змінної $i = 1, 2, \dots, n$.

Розглянемо періодичність гами у режимі гамування зі зворотним зв'язком за шифрґамою. Перш за все відзначимо, що, за визначенням, гама складається із початкового значення блоку γ_0 та решти блоків γ_i , які обчислюються за (1), (3) для кожного значення циклової змінної $i = 1, 2, \dots, n-1$. Тобто, задача дослідження полягає саме у визначенні періоду послідовності блоків $\gamma_i, i = 0, 1, \dots, n-1$.

Кожен блок гами γ_i є результатом зашифрування попереднього блоку γ_{i-1} , де початкове значення γ_0 дорівнює результату зашифрування синхропосилки. Якщо скористатися термінологією теорії підстановок [3–5] і представити базове шифрувальне перетворення $T_{l,k}^{(K)}$, ініці-

йоване секретним ключем K , як деяку підстановку s , що діє на множині відкритих текстів, тоді період послідовності блоків шифрми $\gamma_0, \gamma_1, \dots, \gamma_{n-1}$ відповідатиме одному із циклів $s_i = (y, s_i(y), s_i^2(y), \dots, s_i^{l_i-1}(y))$ підстановки s , де початкове значення циклу y дорівнює значенню синхросилки S .

Кожен наступний елемент $s_i^j(y)$ циклу s_i довжини l_i є результатом багаторазового зашифрування синхросилки:

$$\begin{aligned}
 y &= S; \\
 s_i(y) &= T_{l_i, k}^{(K)}(S) = \gamma_0; \\
 s_i^2(y) &= T_{l_i, k}^{(K)}(T_{l_i, k}^{(K)}(S)) = \gamma_1; \\
 &\dots \\
 s_i^{l_i-1}(y) &= \underbrace{T_{l_i, k}^{(K)}(T_{l_i, k}^{(K)} \dots T_{l_i, k}^{(K)}(S))}_{l_i-1 \text{ разів}} = \gamma_{l_i-2}; \\
 s_i^{l_i}(y) &= \underbrace{T_{l_i, k}^{(K)}(T_{l_i, k}^{(K)} \dots T_{l_i, k}^{(K)}(S))}_{l_i \text{ разів}} = \gamma_{l_i-1} = \gamma_0; \\
 &\dots \\
 s_i^n(y) &= \underbrace{T_{l_i, k}^{(K)}(T_{l_i, k}^{(K)} \dots T_{l_i, k}^{(K)}(S))}_{n \text{ разів}} = \gamma_{n-1}.
 \end{aligned}$$

Таким чином, дослідження періодичних властивостей послідовності блоків шифрми $\gamma_i, i=0,1,\dots,n$ полягає у вивченні циклової структури підстановки s , а саме в оцінці розподілу довжин l_i циклів s_i для різних початкових значень $y = S$ базового шифрувального перетворення $T_{l_i, k}^{(K)}$. Такі дослідження дадуть змогу оцінити довжину періоду l_i шифрми для різних $y = S$ та

K або визначити ймовірність формування гами певного періоду для довільного фіксованого значення синхросилки $y = S$ та випадково обраного секретного ключа K .

Розглянемо окремі положення теорії підстановок та їх зв'язок із властивостями БСШ, зокрема, введемо основні поняття та визначення, які пов'язані з певними властивостями симетричних блокових криптоперетворень (розподіли кількості циклів, зростань та інверсій тощо).

3. ОКРЕМІ ПОЛОЖЕННЯ ТЕОРІЇ ПІДСТАНОВОК ТА ЇХ ЗВ'ЯЗОК ІЗ БСШ

За визначенням БСШ «Калина» (його базове перетворення $T_{l_i, k}^{(K)}$) є параметризованою ключем K функцією бієктивного відображення множини відкритих текстів у множини шифртекстів: $V_l \rightarrow V_l, K \in V_k, l, k \in \{128, 256, 512\}$ [1, 2]. Загалом, для довільного l -бітового блокового шифру існує $2^l!$ можливих перестановок відкритого тексту. Ці перетворення, які мають назву підстановок степеня 2^l , утворюють групу відносно операції послідовного виконання перетворень. Така група має назву симетричної групи підстановок степеня 2^n та позначається як S_{2^n} [3]. Практично це означає, що кількість бітів ключа, яку необхідно для отримання всіх можливих перестановок, становить близько $\ln 2^l! \approx l \cdot 2^l$ бітів¹. Однак розмір ключа алгоритму «Калина» приймає значення у 128, 256 або 512 біт, тобто використовується лише невелика частка від повної кількості можливих перестановок. Наприклад, для $l = 128$ ма-

¹ За формулою Стірлінга $\ln(x!) = x \ln(x) - x - O(\ln(x))$

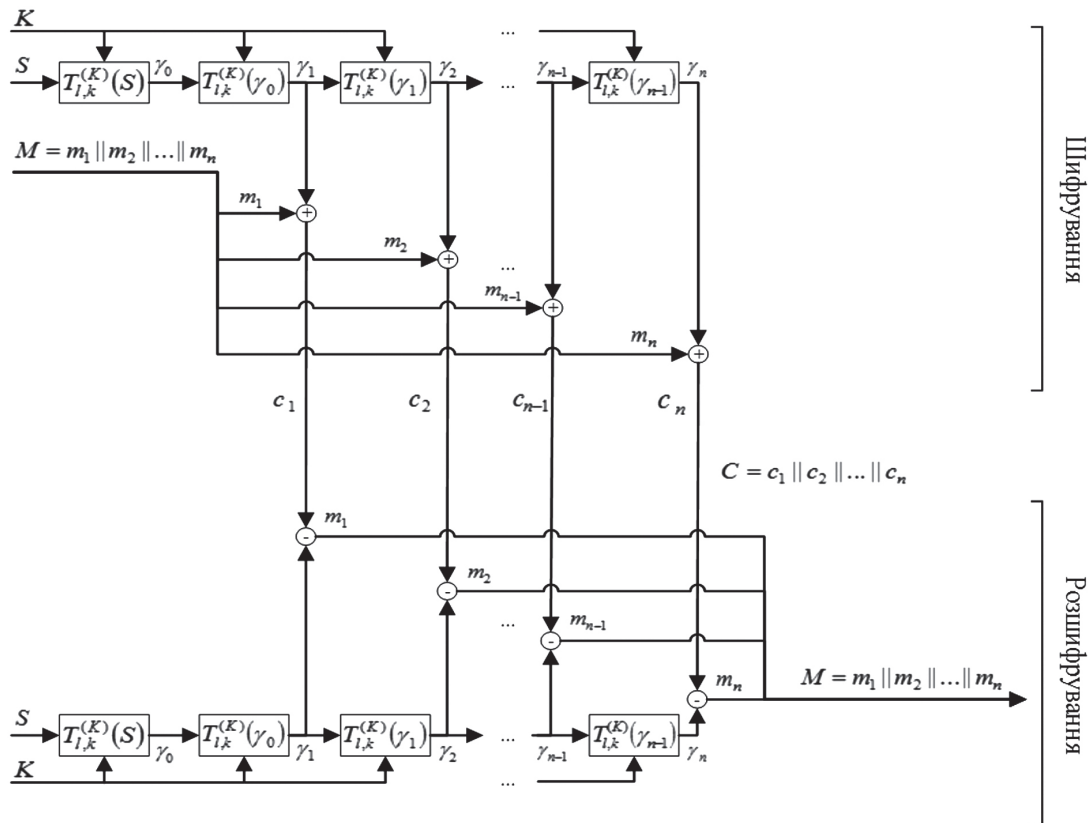


Рис. 1. Схема зашифрування та розшифрування у режимі гамування зі зворотним зв'язком за шифрми

емо $2^{128}! \approx 2^{128 \cdot 2^{128}}$ можливих перестановок 128-бітових блоків, з яких, залежно від довжини ключа, використовуються тільки 2^{128} або 2^{256} перетворень². Таким чином, базове перетворення шифру є по суті деякою підмножиною повної множини всіх можливих підстановок, що діють на множині блоків оброблюваних даних. Основне припущення, яке приймається в ході обґрунтування стійкості симетричного криптоперетворення полягає саме у збереженні ймовірнісних властивостей випадкової підстановки. Тобто припускається, що хоча при шифруванні й застосовується обмежений набір підстановок із S_{2^l} , однак певні розподіли ймовірностей елементів цієї підмножини відповідають властивостям випадково обраної підстановки із всієї множини S_{2^l} [6–9].

Розглянемо основні поняття та визначення теорії підстановок [3] та пов'яжемо їх із цикловими властивостями БСШ. Для цього розглянемо множини всіх бієктивних перетворень множини $Y = \{y_1, y_2, \dots, y_n\}$ саму в себе, що утворюють симетричну групу S_n потужності $n!$ всіх можливих підстановок степеня n . За визначенням симетричної групи [3], кожній підстановці $s \in S_n$ відповідає єдина підстановка $s^{-1} \in S_n$, така, що

$$s^{-1} \cdot s(y) = s \cdot s^{-1}(y) = e(y), \quad y \in Y,$$

де $e(y) \in S_n$ — одинична підстановка, тобто $e(y) = y$ для всіх $y \in Y$.

Скористаємося позначеннями:

$$s \cdot s \cdot \dots \cdot s = s^k, \quad s^{-1} \cdot s^{-1} \cdot \dots \cdot s^{-1} = s^{-k},$$

де добутки містять k множників.

Відповідно маємо

$$s^k \cdot s^{-k} = s^{-k} \cdot s^k = s^0 = e.$$

Множина підстановок степеня n , яка є замкненою відносно операції множення та обчислення оберненого для $s \in S_n$ елементу $s^{-1} \in S_n$, має назву групи підстановок. Кожна така група є підгрупою симетричної групи S_n [3].

Розглянемо деяку підстановку $s \in S_n$, яка діє на множині Y . Визначимо на множині Y бінарне відношення, при цьому вважатимемо $y \sim y'$ для $y, y' \in Y$ якщо існує таке j , що $y' = s^j(y)$. Це бінарне відношення є рефлексивним, симетричним та транзитивним, тобто є відношенням еквівалентності. Дійсно, відповідно до [3] маємо:

— $y \sim y$, оскільки $y = s^0(y) = e(y)$;

— із умови $y \sim y'$ випливає $y' \sim y$, оскільки із

рівності $y' = s^j(y)$ випливає, що $y = s^{-j}(y')$;

— із $y \sim y'$ та $y' \sim y''$ випливає, що $y \sim y''$, бо

з рівностей $y' = s^j(y)$ та $y'' = s^l(y')$ випливає, що $y'' = s^l(s^j(y)) = s^{l+j}(y)$.

Цикл s_i підстановки $s \in S_n$ довжини l_i визначається так:

$$s_i = (y, s_i(y), s_i^2(y), \dots, s_i^{l_i-1}(y)),$$

де $s_i^{l_i}(y) = y$.

² Відповідно до специфікації алгоритму «Калина» для $l = 128$ відповідне k може дорівнювати 128 або 256

Довільну підстановку $s \in S_n$ можна розкласти на відповідні цикли [3]:

$$s = (y_1, s_1(y_1), s_1^2(y_1), \dots, s_1^{l_1-1}(y_1)) \dots \dots (y_k, s_k(y_k), s_k^2(y_k), \dots, s_k^{l_k-1}(y_k)). \quad (5)$$

Елементи y_i та y_{i+1} в підстановці $s \in S_n$ утворюють зростання, якщо $s(y_i) > s(y_{i+1})$, при цьому приймається, що елементу y_1 завжди передують зростання. Пара елементів y_i та y_j в підстановці $s \in S_n$ утворює інверсію, якщо $s(y_i) > s(y_j)$, $i < j$.

Наприклад, підстановка s степеня 4-го виду

$$s = \begin{pmatrix} y_1 & y_2 & y_3 & y_4 \\ s(y_1) & s(y_2) & s(y_3) & s(y_4) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

може бути подана у вигляді розкладу на 3 цикли:

$$s_1 = (y_1) = (1), \quad l_1 = 1;$$

$$s_2 = (y_2, s_2(y_2)) = (2, 4), \quad l_2 = 2;$$

$$s_3 = (y_3) = (3), \quad l_3 = 1,$$

Тобто, маємо такий розклад:

$$s = (y_1)(y_2, s_2(y_2))(y_3) = (1)(2, 4)(3).$$

У цій підстановці є два зростання (елементу $y_1 = 1$ завжди передують одне зростання, та ще одне зростання утворюють елементи $y_1 = 1$ і $y_2 = 2$, бо $s(y_1) = 1 > s(y_2) = 4$) і три інверсії (їх утворюють пари елементів y_2 та y_3 , y_2 та y_4 , y_3 та y_4 , бо виконуються нерівності $s(y_2) > s(y_3)$, $s(y_2) > s(y_4)$, $s(y_3) > s(y_4)$, відповідно).

На множині всіх підстановок симетричної групи S_n задамо рівномірний ймовірнісний розподіл, тобто кожній вибраній підстановці $s \in S_n$ поставимо у відповідність ймовірність її обрання, що дорівнює $1/n!$. За сучасними поглядами симетричної криптографії така множина рівноймовірних відображень відповідає уявленню про «ідеальний» шифр. Адже, якщо випадкове обрання окремої підстановки $s \in S_n$ пов'язати з значенням введеного ключа шифрування, тоді отримане перетворення відповідатиме випадковому і рівномірно вибраному шифртексту для кожного відкритого тексту при будь-якому ключі, тобто на всіх можливих варіантах відображень відкритого тексту у шифрограмму.

Проведемо дослідження ймовірнісних властивостей випадкової підстановки, зокрема, ймовірностей появи циклу певної довжини у випадково обраній підстановці, бо саме ця подія відповідатиме випадку, коли для довільного фіксованого значення синхросилки S буде сформована гама γ_i певного періоду.

4. ОЦІНКА ЙМОВІРНОСТІ ПОЯВИ ЦИКЛУ ПЕВНОЇ ДОВЖИНИ У ВИПАДКОВО ОБРАНІЙ ПІДСТАНОВЦІ

Розглянемо випадкову величину ξ_n , яка дорівнює числу циклів у випадково вибраній підстановці $s \in S_n$. Підстановка $s \in S_n$ належить до циклового класу $\{1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n}\}$, якщо вона містить α_1 циклів довжини 1, α_2 циклів довжини 2 і т. д., тобто:

$$s = (y_1)(y_2)\dots(y_{\alpha_1})(y'_1, y''_1)(y'_2, y''_2)\dots(y'_{\alpha_2}, y''_{\alpha_2})\dots,$$

$$1\alpha_1 + 2\alpha_2 + \dots + n\alpha_n = n.$$

Позначимо через $C(\alpha_1, \alpha_2, \dots, \alpha_n)$ число підстановок у цикловому класі $\{1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n}\}$, а через $C(n, k)$ – число підстановок степеня n , які мають k циклів. Тоді маємо [3]:

$$C(\alpha_1, \alpha_2, \dots, \alpha_n) = \frac{n!}{1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n} \alpha_1! \alpha_2! \dots \alpha_n!},$$

$$C(n, k) = \sum_{\substack{1\alpha_1 + 2\alpha_2 + \dots + n\alpha_n = n \\ \alpha_1 + \alpha_2 + \dots + \alpha_n = k, \alpha_i \geq 0}} \frac{n!}{1^{\alpha_1} 2^{\alpha_2} \dots n^{\alpha_n} \alpha_1! \alpha_2! \dots \alpha_n!} = |s(n, k)|, \quad (6)$$

де $s(n, k)$ – числа Стірлінга першого роду, які визначаються через співвідношення³:

$$(x)_n = x(x-1)\dots(x-n+1) = \sum_{k=0}^n s(n, k) x^k.$$

З формули (6) безпосередньо випливає вираз для точного розподілу ймовірності випадкової події $\xi_n = k$, тобто такого випадку, коли у випадково вибраній підстановці спостерігатиметься точно k циклів (див. вираз (5)).

Скориставшись формулою для обчислення чисел Стірлінга першого роду, маємо [3]:

$$P(\xi_n = k) = \frac{C(n, k)}{n!} = \frac{|s(n, k)|}{n!}, \quad k = 0, 1, \dots, n.$$

В роботі [3] отримано математичне очікування $M\xi_n$ та дисперсію $D\xi_n$ випадкової величини ξ_n :

$$M\xi_n = \sum_{j=1}^n \frac{1}{j} = \ln n + C + o(1),$$

$$D\xi_n = \sum_{j=1}^n \frac{1}{j^2} - \left(\sum_{j=1}^n \frac{1}{j}\right)^2 = \ln n + C + o(1), \quad C = 0,5772\dots,$$

крім того показано, що при $n \rightarrow \infty$ випадкова величина $\xi'_n = (\xi_n - \ln n) / (\ln n)$ розподілена асимптотично нормально з параметрами $(0, 1)$, тобто

$$\lim_{n \rightarrow \infty} P(\xi'_n < u) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^u e^{-y^2/2} dy.$$

Для випадкових величин ζ_n та η_n , які до рівнюють числу зростань та інверсій у випадково обраній підстановці $s \in S_n$, відповідні математичні очікування та дисперсії мають вигляд [3]:

$$M\zeta_n = \frac{n(n-1)}{4}, \quad D\zeta_n = \frac{2n^3 + 3n^2 - 5n}{72},$$

$$M\eta_n = \frac{n}{2}, \quad D\eta_n = \frac{n}{12},$$

при цьому випадкові величини

$$\zeta'_n = (\zeta_n - M\zeta_n) / (D\zeta_n) \quad \text{і} \quad \eta'_n = (\eta_n - M\eta_n) / (D\eta_n)$$

при $n \rightarrow \infty$ також розподілені асимптотично нормально з параметрами $(0, 1)$.

В роботах [6, 9] досліджено емпіричні розподіли ймовірності виникнення певного числа циклів, зростань та інверсій у випадково обраній

³ $(x)_n = x(x-1)\dots(x-n+1)$ – загальноприйняте позначення спадаючого факторіалу (символ Похгаммера)

підстановці із деякої підмножини $V \subset S_n$, елементами якої є підстановки, що реалізуються застосуванням шифрувальної функції на зменшених моделях шифрів⁴. Встановлено, що отримані емпіричні розподіли дуже близькі до розглянутих теоретичних розподілів, тобто можна стверджувати, що зменшені моделі БСШ за цими критеріями подібні властивостям випадкової підстановки із S_n .

Водночас, для оцінки ймовірності формування шифрми γ_i певного періоду для довільного фіксованого значення синхросилки S потрібна інша характеристика випадкової підстановки, а саме розподіл числа циклів заданої довжини. Відповідно до [3], ця характеристика у випадковій підстановці визначається наступним чином.

Позначимо як $\chi_{n,L}$ число циклів довжини L у випадковій рівномірноюбраній підстановці степеня n . Очевидно, що

$$\xi_n = \chi_{n,L=1} + \chi_{n,L=2} + \dots + \chi_{n,L=n}.$$

Розподіл ймовірностей випадкової події $\chi_{n,L} = k$ визначається як [3]:

$$P(\chi_{n,L} = k) = \frac{1}{L^k k!} \sum_{j=0}^{[n/L]-k} \frac{(-1)^j}{L^j j!}, \quad k = 0, 1, \dots, [n/L]. \quad (7)$$

При $n \rightarrow \infty$ випадкова величина $\chi_{n,L}$ має в межі розподіл Пуасона з параметрами $\lambda = 1/L$, тобто

$$\lim_{n \rightarrow \infty} P(\chi_{n,L} = k) = \frac{1}{L^k k!} e^{-1/L}, \quad k = 0, 1, \dots \quad (8)$$

Скористаємося формулою точного розподілу ймовірностей випадкової події $\chi_{n,L} = k$ у вигляді (7) [3]. Значення $n!P(\chi_{n,L} = k)$ відповідає кількості підстановок, які містять k циклів довжини L . Нас цікавить кількість таких підстановок $s \in S_n$, які для довільного фіксованого $y_i \in Y$ обов'язково матимуть цикли $s_i = (y_i, s_i^1(y_i), s_i^2(y_i), \dots, s_i^{l_i-1}(y_i))$ довжини $L = l_i$. Розглянемо випадок, коли $L = 1$, тобто підраховуємо кількість таких підстановок із S_n , які для довільного фіксованого $y_i \in Y$ обов'язково матимуть цикл (y_i) довжини $L = l_i = 1$. У криптографії при розгляді блокових симетричних криптоперетворень такі випадки прийнято називати фіксованими точками підстановки [6].⁵

З урахуванням $L = 1$, формула (7) набуде вигляду

⁴ Обрання підстановки полягало у випадковому і незалежному обранні ключа шифрування, який параметризує шифрувальну функцію і задає конкретний вигляд відображення (підстановку) множини відкритих текстів у множину шифртекстів. При цьому застосовувалися зменшені (16-бітні) моделі шифрів, що реалізують деяку підмножину $V \subset S_{2^{16}}$ підстановок 16-бітних векторів

⁵ Тут ідеться тільки про підстановки, які містять лише конкретну фіксовану точку (цикл) (y_i) , яка відповідає обраному $y_i \in Y$. Зазвичай у відомих джерелах оцінюється загальна кількість підстановок, які містять будь-яку фіксовану точку (y_i) для довільного $i = 1, 2, \dots, n$ на повній множині Y із n елементів

$$P(\chi_{n,L=1} = k) = \frac{1}{k!} \sum_{j=0}^{n-k} \frac{(-1)^j}{j!}, \quad k = 0, 1, \dots, n,$$

причому для кожного $k = 1, \dots, n$ кожен з $n!P(\chi_{n,L=1} = k)$ випадків для довільного фіксованого $y_i \in Y$ спостерігатиметься точно

$$\frac{C_{n-1}^{k-1}}{C_n^k} = \frac{(n-1)!}{(k-1)!(n-k)!} \frac{k!(n-k)!}{n!} = \frac{k}{n} \quad (9)$$

разів, тобто кількість підстановок, що містять одну фіксовану точку конкретного вигляду (цикл (y_i)) визначатиметься за формулою:

$$\begin{aligned} \sum_{k=1}^n n!P(\chi_{n,L=1} = k) \frac{C_{n-1}^{k-1}}{C_n^k} &= \\ &= \sum_{k=1}^n \left(\frac{(n-1)!}{(k-1)!} \sum_{j=0}^{n-k} \frac{(-1)^j}{j!} \right) = (n-1)!, \end{aligned} \quad (10)$$

а відповідна ймовірність появи такої фіксованої точки (для заданого початкового значення $y_i \in Y$) у випадково обраній підстановці степеня n матиме вигляд:

$$\sum_{k=1}^n P(\chi_{n,L=1} = k) \frac{C_{n-1}^{k-1}}{C_n^k} = \frac{(n-1)!}{n!} = \frac{1}{n}. \quad (11)$$

Пояснимо формулу (9). Всього існують точно C_n^k способів одночасного обрання значень $y_i, y_{i_1}, y_{i_2}, \dots, y_{i_{k-1}} \in Y$, $y_i \neq y_{i_1} \neq y_{i_2} \neq \dots \neq y_{i_{k-1}}$, які однозначно визначають цикли $(y_i)(y_{i_1})(y_{i_2}) \dots (y_{i_{k-1}})$ довжиною $L = 1$. Але для кожного фіксованого $y_i \in Y$ існує точно C_{n-1}^{k-1} варіантів обрання решти значень $y_{i_1}, y_{i_2}, \dots, y_{i_{k-1}} \in Y$. Тобто із загальної кількості $n!P(\chi_{n,L=1} = k)$ тих підстановок, які містять k циклів довжини $L = 1$, тільки

$$n!P(\chi_{n,L=1} = k) \frac{C_{n-1}^{k-1}}{C_n^k} = n!P(\chi_{n,L=1} = k) \frac{k}{n}$$

підстановок обов'язково міститимуть цикл (y_i) .

Остання формула (11) може бути отримана значно простіше з тривіальних комбінаторних міркувань. Дійсно, якщо на множині $Y = \{y_1, y_2, \dots, y_n\}$ зафіксувати m елементів, тоді можливі $(n-m)!$ варіантів перестановок решти елементів. Тобто на всій множині підстановок з S_n при їх випадковому рівномірному розподілі ймовірність обрати підстановку з m фіксованими точками дорівнює

$$\frac{(n-m)!}{n!} = \frac{1}{(n-m+1)(n-m+2)\dots n} = \frac{1}{(n)_m}, \quad (12)$$

що при $m = 1$ співпадає з (11).

Формули (9–12) були отримані у роботі [10], в ході дослідження режиму вибіркового гамування із прискореним виробленням імітовставки (Galois/Counter Mode and GMAC – GCM & GMAC), що дозволило оцінити ймовірність виникнення нульового субключа гешування, тобто ймовірність такої події, коли при шифруванні нульового відкритого тексту буде отримано нульове значення шифртексту. Поширимо отриманий раніше результат на довільне значення до-

вжини циклу $L = l_i \in \{1, 2, \dots, n\}$ в ході дослідження періодичних властивостей гаму у режимі OFB.

Розглянемо випадок довільної довжини циклу, тобто підрахуємо кількість таких підстановок s із S_n , які для довільного фіксованого $y_i \in Y$ обов'язково матимуть цикл

$$(y_i, s_i(y_i), s_i^2(y_i), \dots, s_i^{L-1}(y_i))$$

довжини $L = l_i \in \{1, 2, \dots, n\}$.

Для фіксованих довжин та кількостей циклів $(L \text{ і } k)$ всього існує точно C_n^{kL} способів одночасного обрання значень

$$\begin{aligned} &y_i, y_{j_i}, y_{u_i}, \dots, y_{v_i}, \\ &y_{i_1}, y_{j_1}, y_{u_1}, \dots, y_{v_1}, \\ &y_{i_2}, y_{j_2}, y_{u_2}, \dots, y_{v_2}, \\ &\dots, \\ &y_{i_{k-1}}, y_{j_{k-1}}, y_{u_{k-1}}, \dots, y_{v_{k-1}}, \end{aligned} \quad (13)$$

які в сукупності визначають k циклів довжини L кожний:

$$\begin{aligned} &(y_i, y_j = s_i(y_i), y_u = s_i^2(y_i), \dots, y_v = s_i^{L-1}(y_i)), \\ &(y_{i_1}, y_{j_1} = s_{i_1}(y_{i_1}), y_{u_1} = s_{i_1}^2(y_{i_1}), \dots, y_{v_1} = s_{i_1}^{L-1}(y_{i_1})), \\ &(y_{i_2}, y_{j_2} = s_{i_2}(y_{i_2}), y_{u_2} = s_{i_2}^2(y_{i_2}), \dots, y_{v_2} = s_{i_2}^{L-1}(y_{i_2})), \\ &\dots, \\ &(y_{i_{k-1}}, y_{j_{k-1}} = s_{i_{k-1}}(y_{i_{k-1}}), y_{u_{k-1}} = \\ &= s_{i_{k-1}}^2(y_{i_{k-1}}), \dots, y_{v_{k-1}} = s_{i_{k-1}}^{L-1}(y_{i_{k-1}})), \end{aligned} \quad (14)$$

причому всі елементи із (13) є унікальними (неповторними), адже сукупність циклів (14) входить до розкладу однієї і тієї ж підстановки.

Із C_n^{kL} способів одночасного обрання значень (13) для кожного фіксованого набору⁶ $y_i, y_{j_i}, y_{u_i}, \dots, y_{v_i} \in Y$ існує точно C_{n-1}^{kL-1} варіантів обрання решти значень

$$\begin{aligned} &y_{i_1}, y_{j_1}, y_{u_1}, \dots, y_{v_1}, \\ &y_{i_2}, y_{j_2}, y_{u_2}, \dots, y_{v_2}, \\ &\dots, \\ &y_{i_{k-1}}, y_{j_{k-1}}, y_{u_{k-1}}, \dots, y_{v_{k-1}}, \end{aligned}$$

бо обрання набору $y_i, y_{j_i}, y_{u_i}, \dots, y_{v_i} \in Y$ визначається через обрання тільки одного елементу $y_i \in Y$, а з решти $n-1$ елементів можливі різні комбінації по $kL-1$ елементів.

Таким чином, для кожного $k = 0, 1, \dots, [n/L]$ із загальної кількості $n!P(\chi_{n,L} = k)$ тих підстановок, які містять k циклів довжини L , тільки

$$\begin{aligned} n!P(\chi_{n,L} = k) \frac{C_{n-1}^{kL-1}}{C_n^{kL}} &= n!P(\chi_{n,L} = k) \frac{(n-1)!kL!(n-kL)!}{n!(kL-1)!(n-kL)!} = \\ &= n!P(\chi_{n,L} = k) \frac{kL}{n} = (n-1)!kLP(\chi_{n,L} = k) \end{aligned}$$

підстановок обов'язково міститимуть цикл

$$(y_i, s_i(y_i), s_i^2(y_i), \dots, s_i^{L-1}(y_i)).$$

⁶ Цей набір $y_i, y_{j_i}, y_{u_i}, \dots, y_{v_i} \in Y$ складає цикл $(y_i, y_j = s_i(y_i), y_u = s_i^2(y_i), \dots, y_v = s_i^{L-1}(y_i))$, ймовірність появи якого у випадково обраній підстановці і треба визначити

Підсумувавши останній вираз за всіма $k = 0, 1, \dots, \lfloor n/L \rfloor$ із урахуванням (7), отримаємо точну формулу для визначення кількості підстановок s із S_n , які для довільного фіксованого $y_i \in Y$ обов'язково матимуть цикл

$$(y_i, s_i(y_i), s_i^2(y_i), \dots, s_i^{L-1}(y_i))$$

довжини $L = l_i \in \{1, 2, \dots, n\}$:

$$\sum_{k=1}^{\lfloor n/L \rfloor} n! P(\chi_{n,L} = k) \frac{C_{n-1}^{kL-1}}{C_n^{kL}} = \sum_{k=1}^{\lfloor n/L \rfloor} \frac{(n-1)!}{(k-1)! L^{k-1}} \sum_{j=0}^{\lfloor n/L \rfloor - k} \frac{(-1)^j}{L^j j!} = (n-1)!, \quad (15)$$

та відповідну формулу для розрахунку ймовірності випадково обрати підстановку s із S_n з таким циклом:

$$\sum_{k=1}^{\lfloor n/L \rfloor} P(\chi_{n,L} = k) \frac{C_{n-1}^{kL-1}}{C_n^{kL}} = \frac{(n-1)!}{n!} = \frac{1}{n}. \quad (16)$$

Очевидно, що останній аналітичний вираз при $L=1$ повністю збігається з формулою (8) у [10] з відповідним викладенням.

Отриманий аналітичний вираз (16) може розглядатися і як комбінаторна тотожність (спрощена формула) для суми членів формули (7) із відповідними пропорційними коефіцієнтами

$$\frac{C_{n-1}^{kL-1}}{C_n^{kL}} = \frac{kL}{n},$$

або навіть для розподілу Пуасона (8).

Оцінку ймовірності (16) виникнення циклу певної довжини можна, як і в роботі [10], отримати іншим, значно простішим способом, застосовуючи прості комбінаторні міркування.

Зафіксуємо деяке довільне значення y_i із множини $Y = \{y_1, y_2, \dots, y_n\}$. Всього існує $n!$ підстановок на множині Y , з яких лише

$$\frac{n!}{n} = (n-1)!$$

підстановок міститимуть цикл (y_i) довжини $L=1$ у своєму цикловому розкладі.

Крім того, із $n!$ підстановок симетричної групи

$$\frac{n!}{n(n-1)}(n-1) = (n-1)!$$

підстановок міститимуть цикл $(y_i, y_{j \neq i})$ довжини $L=2$,

$$\frac{n!}{n(n-1)(n-2)}(n-1)(n-2) = (n-1)!$$

підстановок міститимуть цикл $(y_i, y_{j \neq i}, y_{u \neq i,j})$ довжини $L=3$ і т.д.

Тобто для довільного фіксованого значення $y_i \in Y$ кількість підстановок із S_n , які містять цикл $(y_i, s_i(y_i), s_i^2(y_i), \dots, s_i^{L-1}(y_i))$, визначається як $(n-1)!$, а відповідна ймовірність випадково обрати підстановку, що містить такий цикл, визначається як

$$\frac{(n-1)!}{n!} = \frac{1}{n},$$

незалежно ані від довжини циклу $L = l_i \in \{1, 2, \dots, n\}$, ані від власного значення y_i із $Y = \{y_1, y_2, \dots, y_n\}$.

Таким чином, ймовірність виникнення циклу певної довжини визначається лише за степенем підстановки n . Наприклад, для $n=4$ із $n! = 24$ підстановок симетричної групи для будь-якого фіксованого y_i із $Y = \{y_1, y_2, y_3, y_4\}$ маємо по $(n-1)! = 6$ підстановок, які обов'язково містять цикли різної довжини (або (y_i) , або $(y_i, y_{j \neq i})$, або $(y_i, y_{j \neq i}, y_{u \neq i,j})$, або $(y_i, y_{j \neq i}, y_{u \neq i,j}, y_{v \neq i,j,u})$, відповідно). Отже ймовірність того, що у випадково обраній підстановці із S_4 міститиметься цикл довжини $L = l_i \in \{1, 2, \dots, 4\}$, дорівнюватиме $1/n = 1/4$ незалежно ані від y_i , ані від $L = l_i$.

Оскільки отримані аналітичні вирази (15) та (16) досить складні та громіздкі, особливо порядок їхнього виведення, проілюструємо приклад розрахунку ймовірностей появи циклу заданої довжини у випадково обраній підстановці із симетричної групи S_4 . Приклад доповнюватимемо поясненнями, що демонструють справедливості отриманих формул та наведених комбінаторних міркувань.

5. ПРИКЛАД ДЛЯ СИМЕТРИЧНОЇ ГРУПИ S_4

Розглянемо приклад усіх бієктивних перетворень множини $Y = \{y_1, y_2, y_3, y_4\}$ саму в себе, тобто множини із $n! = 24$ підстановок степеня $n = 4$.

У таблиці 1 наведено всі підстановки, які складають симетричну групу S_4 (наведено результати кожної підстановки, розклад кожної підстановки на цикли, загальна кількість циклів та розподіл кількості циклів певної довжини. Кожну підстановку для зручності пронумеровано).

У таблиці 2 наведено розподіли кількості величин $\xi_n = k$ та $\chi_{n,L} = k$ для різних k (символом $\#(x)$ позначено число випадків (x) за всіма підстановками із S_4).

5.1 Оцінка ймовірності появи циклу (y_i) . Розглянемо випадок, коли для довільного фіксованого $y_i \in Y$ випадково обрана підстанова s із S_4 обов'язково міститиме цикл (y_i) довжини $L=1$.

Спочатку розглянемо ті підстановки, які містять $k=1$ цикл довжини $L=1$. Маємо 8 таких підстановок (табл. 3)⁷. Але кожне окреме $y_i \in Y$ породжує цикл довжини $L=1$ лише двічі, тобто для кожного довільного фіксованого $y_i \in Y$ існує точно 2 підстановки, які містять цикл довжини $L=1$ виду (y_i) . Наприклад, для $y_1 \in Y$ це 4-та та 5-та підстановки, для $y_2 \in Y$ це 16-та та 21-ша підстанова і т.д. Кількість підстановок, які для довільного фіксованого $y_i \in Y$ містять $k=1$, цикл довжини $L=1$ виду (y_i) підрахуємо наступним чином. Всього існує точно $C_{n-1}^{kL-1} = 4$ способів обрання значення $y_i \in Y$.

⁷ Номера підстановок у таблицях 3–5 відповідають загальній нумерації підстановок із таблиці 1

Множина підстановок із S_4 та їх циклові властивості

№ з/п	Результат підстановки				Розклад підстановки на цикли	Число циклів, ξ_n	Число циклів довжини $L, \chi_{n,L}$			
	$s(y_1)$	$s(y_2)$	$s(y_3)$	$s(y_4)$			$L=1$	$L=2$	$L=3$	$L=4$
1	y_1	y_2	y_3	y_4	$(y_1)(y_2)(y_3)(y_4)$	4	4	0	0	0
2	y_1	y_2	y_4	y_3	$(y_1)(y_2)(y_3, y_4)$	3	2	1	0	0
3	y_1	y_3	y_2	y_4	$(y_1)(y_2, y_3)(y_4)$	3	2	1	0	0
4	y_1	y_3	y_4	y_2	$(y_1)(y_2, y_3, y_4)$	2	1	0	1	0
5	y_1	y_4	y_2	y_3	$(y_1)(y_2, y_4, y_3)$	2	1	0	1	0
6	y_1	y_4	y_3	y_2	$(y_1)(y_2, y_4)(y_3)$	3	2	1	0	0
7	y_2	y_1	y_3	y_4	$(y_1, y_2)(y_3)(y_4)$	3	2	1	0	0
8	y_2	y_1	y_4	y_3	$(y_1, y_2)(y_3, y_4)$	2	0	2	0	0
9	y_2	y_3	y_1	y_4	$(y_1, y_2, y_3)(y_4)$	2	1	0	1	0
10	y_2	y_3	y_4	y_1	(y_1, y_2, y_3, y_4)	1	0	0	0	1
11	y_2	y_4	y_1	y_3	(y_1, y_2, y_4, y_3)	1	0	0	0	1
12	y_2	y_4	y_3	y_1	$(y_1, y_2, y_4)(y_3)$	2	1	0	1	0
13	y_3	y_1	y_2	y_4	$(y_1, y_3, y_2)(y_4)$	2	1	0	1	0
14	y_3	y_1	y_4	y_2	(y_1, y_3, y_4, y_2)	1	0	0	0	1
15	y_3	y_2	y_1	y_4	$(y_1, y_3)(y_2)(y_4)$	3	2	1	0	0
16	y_3	y_2	y_4	y_1	$(y_1, y_3, y_4)(y_2)$	2	1	0	1	0
17	y_3	y_4	y_1	y_2	$(y_1, y_3)(y_2, y_4)$	2	0	2	0	0
18	y_3	y_4	y_2	y_1	(y_1, y_3, y_2, y_4)	1	0	0	0	1
19	y_4	y_1	y_2	y_3	(y_1, y_4, y_3, y_2)	1	0	0	0	1
20	y_4	y_1	y_3	y_2	$(y_1, y_4, y_2)(y_3)$	2	1	0	1	0
21	y_4	y_2	y_1	y_3	$(y_1, y_4, y_3)(y_2)$	2	1	0	1	0
22	y_4	y_2	y_3	y_1	$(y_1, y_4)(y_2)(y_3)$	3	2	1	0	0
23	y_4	y_3	y_1	y_2	(y_1, y_4, y_2, y_3)	1	0	0	0	1
24	y_4	y_3	y_2	y_1	$(y_1, y_4)(y_2, y_3)$	2	0	2	0	0

Таблиця 2

Розподіли кількості величин $\xi_n = k$ та $\chi_{n,L} = k$ за всіма підстановками із S_4

k	0	1	2	3	4
# ($\xi_n = k$)	0	6	11	6	1
# ($\chi_{n,L=1} = k$)	9	8	6	0	1
# ($\chi_{n,L=2} = k$)	15	6	3	0	0
# ($\chi_{n,L=3} = k$)	16	8	0	0	0
# ($\chi_{n,L=4} = k$)	18	6	0	0	0

Таблиця 3

Підстановки, що містять 1 цикл довжини 1 та один цикл довжини 3

№ з/п	Результат підстановки				Розклад підстановки на цикли
	$s(y_1)$	$s(y_2)$	$s(y_3)$	$s(y_4)$	
4	y_1	y_3	y_4	y_2	$(y_1)(y_2, y_3, y_4)$
5	y_1	y_4	y_2	y_3	$(y_1)(y_2, y_4, y_3)$
9	y_2	y_3	y_1	y_4	$(y_1, y_2, y_3)(y_4)$
12	y_2	y_4	y_3	y_1	$(y_1, y_2, y_4)(y_3)$
13	y_3	y_1	y_2	y_4	$(y_1, y_3, y_2)(y_4)$
16	y_3	y_2	y_4	y_1	$(y_1, y_3, y_4)(y_2)$
20	y_4	y_1	y_3	y_2	$(y_1, y_4, y_2)(y_3)$
21	y_4	y_2	y_1	y_3	$(y_1, y_4, y_3)(y_2)$

Цей вибір більш нічим не обмежується, бо для кожного $y_i \in Y$ цикл (y_i) визначається однозначно (за формулою існує $C_{n-1=3}^{kL-1=0} = 1$ варіантів

обрання значення $y_{j \neq i} \in Y$). Тобто загальну кількість підстановок, які містять тільки $k = 1$, цикл довжини $L = 1$ (таких вісім підстановок) треба

помножити на величину $\frac{C_{n-1=3}^{kL-1=0}}{C_{n=4}^{kL=1}} = \frac{1}{4}$. Таким чином, для довільного фіксованого $y_i \in Y$ число підстановок, які містять тільки один цикл (y_i) , дорівнює двом.

Таблиця 4

Підстановки, що містять два цикли довжини 1 та один цикл довжини 2

№ з/п	Результат підстановки				Розклад підстановки на цикли
	$s(y_1)$	$s(y_2)$	$s(y_3)$	$s(y_4)$	
2	y_1	y_2	y_4	y_3	$(y_1)(y_2)(y_3, y_4)$
3	y_1	y_3	y_2	y_4	$(y_1)(y_2, y_3)(y_4)$
6	y_1	y_4	y_3	y_2	$(y_1)(y_2, y_4)(y_3)$
7	y_2	y_1	y_3	y_4	$(y_1, y_2)(y_3)(y_4)$
15	y_3	y_2	y_1	y_4	$(y_1, y_3)(y_2)(y_4)$
22	y_4	y_2	y_3	y_1	$(y_1, y_4)(y_2)(y_3)$

Розглянемо тепер ті підстановки, які містять по $k = 2$ цикли довжини $L = 1$. Маємо 6 підстановок (табл. 4), із них три підстановки у цикловому розкладі містять цикли $(y_1)(y_{i \neq 1})$, три підстановки містять цикли $(y_2)(y_{i \neq 2})$, три підстановки містять цикли $(y_3)(y_{i \neq 3})$ і три підстановки містять цикли $(y_4)(y_{i \neq 4})$. Зрозуміло, що одна і та ж підстановка може рахуватися по-різному, тобто

може за своїм цикловим розкладом відноситися як до підстановок, що містять цикли (y_i) $(y_{j \neq i})$, так і до підстановок, що містять цикли (y_j) $(y_{i \neq j})$. Наприклад, шоста підстановка має цикловий розклад (y_1) (y_2, y_4) (y_3) , вона має рахуватися як із підстановками із циклами (y_1) $(y_{j \neq 1})$, так і з підстановками із циклами (y_3) $(y_{i \neq 3})$ $(y_{j \neq 3})$.

Кількість підстановок, які для фіксованого $y_i \in Y$ містять $k = 2$ цикли (y_i) $(y_{j \neq i})$ довжини $L = 1$, підрахуємо наступним чином. Всього існує точно $C_{n=4}^{kL=2} = 6$ способів одночасного обрання значень $y_i, y_{j \neq i} \in Y$. Але для фіксованого $y_i \in Y$ наявні точно $C_{n=3}^{kL=1} = 3$ варіанти обрання значення $y_{j \neq i} \in Y$. Тобто загальну кількість підстановок, які містять $k = 2$ цикли довжини $L = 1$, треба

помножити на величину $\frac{C_{n=3}^{kL=1}}{C_{n=4}^{kL=2}} = \frac{3}{6}$, отримаємо

шукане значення – для довільного фіксованого значення $y_i \in Y$ число підстановок, містять $k = 2$ цикли (y_i) $(y_{j \neq i})$ довжини $L = 1$, дорівнює трьом. Наприклад, для фіксованого значення $y_1 \in Y$ друга, третя та шоста підстановки містять по $k = 2$ цикли довжини $L = 1$ із цикловими розкладами: (y_1) (y_2) (y_3, y_4) , (y_1) (y_2, y_3) (y_4) та (y_1) (y_2, y_4) (y_3) .

Розглянемо підстановки, які містять $k = 4$ цикли довжини $L = 1$ ($k = 3$ цикли довжини $L = 1$ жодна підстановка мати не може). Маємо одну підстановку – ту, яка наведена першою у табл. 1, її цикловий розклад має вигляд: (y_1) (y_2) (y_3) (y_4) . Застосувавши ту ж саму формулу, маємо $\frac{C_{n=3}^{kL=1}}{C_{n=4}^{kL=4}} = \frac{1}{1} = 1$, тобто загальна кількість підстановок, які містять чотири цикли довжини 1 співпадає із кількістю підстановок із цикловим розкладом (y_i) $(y_{j \neq i})$ $(y_{u \neq i, j})$ $(y_{v \neq i, j, u})$, як це і має бути.

Підрахуємо кількість підстановок із S_4 (табл. 1), які для фіксованого $y_i \in Y$ обов'язково містять цикл (y_i) довжини $L = 1$. Для цього треба підсумувати кількість підстановок, які для фіксованого $y_i \in Y$ у своєму цикловому розкладі містять різну кількість циклів довжини $L = 1$, а саме, це 2 підстановки із $k = 1$ циклом (y_i) , три підстановки із $k = 2$ циклами (y_i) $(y_{j \neq i})$ та одна підстановка із $k = 4$ циклами (y_i) $(y_{j \neq i})$ $(y_{u \neq i, j})$ $(y_{v \neq i, j, u})$. Загалом маємо 6 підстановок із загальної кількості 24 підстановок симетричної групи. Тобто при випадковому рівномірному обранні підстановки із S_4 ймовірність того, що в ній для довільного фіксованого $y_i \in Y$ спостерігатиметься цикл (y_i) довжини $L = 1$ дорівнює $6/24 = 1/4$.

5.2. Оцінка ймовірності появи циклу $(y_i, y_{j \neq i})$. Розглянемо випадок, коли для довільного фіксованого $y_i \in Y$ випадково обрана підстановка s із S_4 обов'язково міститиме цикл $(y_i, y_{j \neq i})$ довжини $L = 2$.

Спочатку розглянемо ті підстановки, які містять $k = 1$ цикл довжини $L = 2$. Маємо 6 таких підстановок, які наведено у таблиці 4 (якщо підстановка із S_4 містить два цикли довжини 1, тоді вона обов'язково містить один цикл до-

вжини 2). Підрахуємо кількість підстановок, які для довільного фіксованого $y_i \in Y$ містять $k = 1$ цикл довжини $L = 2$ виду $(y_i, y_{j \neq i})$. Всього є точно $C_{n=4}^{kL=2} = 6$ способів одночасного обрання значень $y_i, y_{j \neq i} \in Y$. Але для кожного $y_i \in Y$ існує точно $C_{n=3}^{kL=1} = 3$ варіанта обрання значення $y_{j \neq i} \in Y$. Тобто число підстановок, які для довільного фіксованого $y_i \in Y$ у цикловому розкладі містять $k = 2$ цикли (y_i) $(y_{j \neq i})$ довжини $L = 1$, дорівнює $6 \cdot \frac{C_{n=3}^{kL=1}}{C_{n=4}^{kL=2}} = 3$. Наприклад, для $y_1 \in Y$ сьома, п'ятнадцята та двадцять друга підстановки містять по $k = 1$ цикли довжини $L = 2$.

Розглянемо також ті підстановки, які містять по $k = 2$ цикли довжини $L = 2$. Всього в S_n є 3 таких підстановки, це (див. табл. 1):

- восьма підстановка із цикловим розкладом (y_1, y_2) (y_3, y_4) ;
- сімнадцята підстановка із цикловим розкладом (y_1, y_3) (y_2, y_4) ;
- остання, двадцять четверта підстановка із цикловим розкладом (y_1, y_4) (y_2, y_3) .

Кількість підстановок, які для довільного фіксованого $y_i \in Y$ містять $k = 2$ цикли $(y_i, y_{j \neq i})$ та $(y_{u \neq i, j}, y_{v \neq i, j, u})$ довжини $L = 2$, підраховується так само. Всього існує точно $C_{n=4}^{kL=4} = 1$ способів одночасного обрання значень $y_i, y_{j \neq i}, y_{u \neq i, j}, y_{v \neq i, j, u} \in Y$. Цей вибір більш нічим не обмежується, бо для обраних $y_i, y_{j \neq i}, y_{u \neq i, j}, y_{v \neq i, j, u} \in Y$ відповідні $k = 2$ цикли $(y_i, y_{j \neq i})$ та $(y_{u \neq i, j}, y_{v \neq i, j, u})$ визначаються однозначно (за формулою існує $C_{n=3}^{kL=1} = 1$ варіантів). Тобто, число підстановок, які для довільного фіксованого значення $y_i \in Y$ мають цикловий розклад $(y_i, y_{j \neq i})(y_{u \neq i, j}, y_{v \neq i, j, u})$, збігається із загальним числом підстановок із $k = 2$ циклами довжини $L = 2$, тобто дорівнює 3.

Оскільки $k = 3$ та $k = 4$ цикли довжини $L = 2$ жодна підстановка із S_4 мати не може, одразу перейдемо до підрахунку ймовірності виникнення циклу $(y_i, y_{j \neq i})$ у випадково обраній підстановці. Для цього підсумуємо кількість підстановок, які для довільного фіксованого $y_i \in Y$ у своєму цикловому розкладі містять різну кількість циклів довжини $L = 2$, а саме, це 3 підстановки із $k = 1$ циклом $(y_i, y_{j \neq i})$, та три підстановки із $k = 2$ циклами $(y_i, y_{j \neq i})(y_{u \neq i, j}, y_{v \neq i, j, u})$. Загалом маємо 6 підстановок із загальної кількості 24 підстановок симетричної групи, тобто при випадковому обранні підстановки із S_4 ймовірність того, що в ній для довільного фіксованого $y_i \in Y$ спостерігатиметься цикл $(y_i, y_{j \neq i})$ довжини $L = 2$ дорівнює $6/24 = 1/4$.

5.3. Оцінка ймовірності появи циклу $(y_i, y_{j \neq i}, y_{u \neq i, j})$. Аналогічно до розглянутого вище, підрахуємо кількість підстановок, які для довільного фіксованого $y_i \in Y$ мають цикл $(y_i, y_{j \neq i}, y_{u \neq i, j})$. У довільній підстановці $s \in S_4$ може бути не більше одного такого циклу, тобто випадки із $k > 1$ неможливі. Кожен цикл довжини $L = 3$ у розкладанні підстановки поєднується із циклом

довжини 1, тобто всі 8 таких підстановок наведено табл. 3.

Підрахуємо кількість тих підстановок, які для довільного фіксованого $y_i \in Y$ обов'язково містять цикл $(y_i, y_{j \neq i}, y_{u \neq i, j})$. Всього наявні точно $C_{n=4}^{kL=3} = 4$ способи одночасного обрання значень $y_i, y_{j \neq i}, y_{u \neq i, j} \in Y$. Але для кожного $y_i \in Y$ існує точно $C_{n=3}^{kL=2} = 3$ варіанта обрання значень $y_{j \neq i}, y_{u \neq i, j} \in Y$. Тобто число підстановок, які для довільного фіксованого значення $y_i \in Y$ обов'язково мають цикл $(y_i, y_{j \neq i}, y_{u \neq i, j})$, визначається як $8 \cdot \frac{C_{n=3}^{kL=2}}{C_{n=4}^{kL=3}} = 6$. Наприклад, для $y_1 \in Y$ це 6 підстановок (№ 9, 12, 13, 16, 20, 21) із цикловими розкладами (див. табл. 3): $(y_1, y_2, y_3) (y_4)$, $(y_1, y_2, y_4) (y_3)$, $(y_1, y_3, y_2) (y_4)$, $(y_1, y_3, y_4) (y_2)$, $(y_1, y_4, y_2) (y_3)$ та $(y_1, y_4, y_3) (y_2)$.

Отже, ймовірність того, що для довільного фіксованого $y_i \in Y$ у випадково обраній підстановці $s \in S_4$ спостерігатиметься цикл $(y_i, y_{j \neq i}, y_{u \neq i, j})$ довжини $L = 3$ дорівнює $6/24 = 1/4$.

5.4. Оцінка ймовірності появи циклу $(y_i, y_{j \neq i}, y_{u \neq i, j}, y_{v \neq i, j, u})$. У будь-якій підстановці $s \in S_4$ може бути тільки один цикл довжини $L = 4$. Такі підстановки наведено у таблиці 5.

Таблиця 5

Підстановки, що містять один цикл довжини 4

№ з/п	Результат підстановки				Розклад підстановки на цикли
	$s(y_1)$	$s(y_2)$	$s(y_3)$	$s(y_4)$	
10	y_2	y_3	y_4	y_1	(y_1, y_2, y_3, y_4)
11	y_2	y_4	y_1	y_3	(y_1, y_2, y_4, y_3)
14	y_3	y_1	y_4	y_2	(y_1, y_3, y_4, y_2)
18	y_3	y_4	y_2	y_1	(y_1, y_3, y_2, y_4)
19	y_4	y_1	y_2	y_3	(y_1, y_4, y_3, y_2)
23	y_4	y_3	y_1	y_2	(y_1, y_4, y_2, y_3)

Очевидно, що всі такі підстановки обов'язково мають у своєму єдиному циклі всі елементи із множини $Y = \{y_1, y_2, y_3, y_4\}$, тобто, для кожного $y_i \in Y$ у кожній підстановці із табл. 5 існуватиме цикл $(y_i, y_{j \neq i}, y_{u \neq i, j}, y_{v \neq i, j, u})$. Перевіримо застосовану вище формулу: $\frac{C_{n=4}^{kL=3}}{C_{n=4}^{kL=4}} = 1$, тобто дійсно, всі підстановки із таблиці 5 обов'язково міститимуть цикл $(y_i, y_{j \neq i}, y_{u \neq i, j}, y_{v \neq i, j, u})$ для кожного довільного фіксованого $y_i \in Y$. Отже, ймовірність появи циклу $(y_i, y_{j \neq i}, y_{u \neq i, j}, y_{v \neq i, j, u})$ у випадково обраній підстановці $s \in S_4$ дорівнює $6/24 = 1/4$.

6. ІНТЕРПРЕТАЦІЯ ОТРИМАНИХ РЕЗУЛЬТАТІВ ДО ВЛАСТИВОСТЕЙ БСШ

Отримані аналітичні вирази (15) та (16) дозволяють оцінити кількість підстановок із симетричної групи, які для визначеного елемента множини перетворень обов'язково містять цикл певної довжини із цим елементом, та відповідну ймовірність випадково обраної підстановки із таким циклом.

Скористаємося цими формулами для дослідження періодичних властивостей гами у режимі OFB. При цьому вважатимемо, що ймовірнісні властивості підстановок, які утворюються шифрувальною функцією, відповідають певним властивостям випадкової підстановки, тобто відповідають нашим уявленням про такий «ідеальний» БСШ, який при будь-якому введеному ключі шифрування випадково і рівномірно зіставляє будь-який шифртекст будь-якому відкритому тексту. Таким чином l -бітний БСШ реалізовуватиме деяку підмножину симетричної групи підстановок степеня 2^l , обрання конкретної підстановки s із S_{2^l} пов'язується із введеним ключем шифрування. На всій множині ключів шифру ймовірність обрати таку підстановку, яка для довільного фіксованого $y_i = S \in Y = \{y_1, y_2, \dots, y_{2^l}\}$ обов'язково має цикл $(y_i, s_i(y_i), s_i^2(y_i), \dots, s_i^{L-1}(y_i))$ довжини $L = l_i \in \{1, 2, \dots, n\}$, визначатиметься за (16).

Практично це означає, що ймовірність виникнення циклу будь-якої довжини у випадково вибраній підстановці з симетричної групи S_{2^l} для довільного фіксованого елемента множини не залежить ні від цього елемента, ні від довжини циклу. Вона залежить лише від порядку $n = 2^l$ підстановок симетричної групи S_n і визначається як зворотна величина, тобто дорівнює $1/n$. Для будь-якого фіксованого значення введеної синхросилки $y = S$ ймовірність того, що відповідна шифрграма $\gamma_i, i = 0, 1, \dots, n-1$, яка формується у режимі OFB, матиме період довжини $L = l_i \in \{1, 2, \dots, n\}$, не залежить ані від значення цієї синхросилки, ані від довжини періоду. Вона визначається лише ступенем підстановки, тобто, у даному випадку, розрядністю шифру і дорівнює 2^{-l} .

Визначимо ймовірність того, що період формованої шифрграми буде не меншим за 2^m блоків, тобто ймовірність такої події, коли для фіксованого значення введеної синхросилки $y_i = S$ відповідна шифрграма не повторюватиметься під час виконання 2^m ітерацій за формулами (1), (3) при формуванні блоків гами γ_i :

$$P(\forall i, j \in \{1, 2, \dots, 2^m\} : \gamma_i \neq \gamma_j |_{i \neq j}) = 1 - \sum_{L=1}^{2^m} \sum_{k=1}^{\lfloor 2^l/L \rfloor} P(\chi_{2^l, L} = k) \frac{C_{2^l-1}^{kL-1}}{C_{2^l}^{kL}} = \sum_{L=2^m+1}^{2^l} \sum_{k=1}^{\lfloor 2^l/L \rfloor} P(\chi_{2^l, L} = k) \frac{C_{2^l-1}^{kL-1}}{C_{2^l}^{kL}} \quad (17)$$

Враховуючи (16), отримаємо:

$$P(\forall i, j \in \{1, 2, \dots, 2^m\} : \gamma_i \neq \gamma_j |_{i \neq j}) = 1 - \sum_{L=1}^{2^m} 2^{-l} = \sum_{L=2^m+1}^{2^l} 2^{-l} = 1 - 2^{m-l} \quad (18)$$

Таким чином, в ході виконання припущення щодо відповідності певних ймовірнісних власти-

востей шифру властивостям випадкової підстановки ймовірність неповторення ґами на визначеній довжині є функцією від цієї довжини. Цей факт зумовлює основні обмеження на застосування режиму гамування зі зворотним зв'язком за шифрґамою, що безпосередньо впливає із отриманих результатів досліджень. Так, що стосується відповідного режиму застосування БСШ «Калина», специфікацію якого наведено у [1, 2], основним обмеженням на використання режиму OFB є вказані в додатку Г.2 «Обмеження на сумарну довжину повідомлень, що захищаються з використанням одного ключа», а саме:

- при розмірі блоку 128 біт рекомендується обмежити кількість блоків, що захищаються на одному ключі величиною 2^{60} (16 млн ТБ);
- при розмірі блоку 256 біт рекомендується обмежити кількість блоків, що захищаються на одному ключі величиною 2^{124} ;
- при розмірі блоку 512 біт рекомендується обмежити кількість блоків, що захищаються на одному ключі величиною 2^{251} .

Оскільки, як це показано у розділі 2, сутність захисту інформаційного повідомлення за специфікацією режиму OFB полягає у додаванні до нього шифрґами, тоді обмеження, вказані у додатку Г.2 стосуються саме обмежень на довжину шифрґами, яка формується багаторазовим шифруванням одного і того ж несекретного блоку ініціалізації (синхроросилки) за формулами (1), (3). Тобто, виконання обмежень, які рекомендовано специфікацією проекту національного стандарту, забезпечує певні ймовірнісні показники неперіодичності шифрґами, а саме:

- при розмірі блоку $l = 128$ біт і при виконанні рекомендованого обмеження кількості блоків, що захищаються на одному ключі величиною $2^m = 2^{60}$, буде забезпечено ймовірність неповторення ґами $1 - 2^{m-l} = 1 - 2^{-68} > 1 - 2^{-64}$;
- при розмірі блоку $l = 256$ біт і при виконанні рекомендованого обмеження кількості блоків, що захищаються на одному ключі величиною $2^m = 2^{124}$, буде забезпечено ймовірність неповторення ґами $1 - 2^{m-l} = 1 - 2^{-132} > 1 - 2^{-128}$;
- при розмірі блоку $l = 512$ біт і при виконанні рекомендованого обмеження кількості блоків, що захищаються на одному ключі величиною $2^m = 2^{251}$, буде забезпечено ймовірність неповторення ґами $1 - 2^{m-l} = 1 - 2^{-261} > 1 - 2^{-256}$.

Частіше в теорії захисту інформації застосовують зворотну величину – ймовірність того, що сформована шифрґама із довжиною, що не перевищує певну межу, матиме хоча б одне повторення. Враховуючи (17) та (18) цю ймовірність визначимо як:

$$P_{l,m} = 1 - P(\forall i, j \in \{1, 2, \dots, 2^m\} : \gamma_i \neq \gamma_j |_{i \neq j}) = \sum_{L=1}^{2^m} \sum_{k=1}^{\lfloor 2^l/L \rfloor} P(\chi_{2^l, L} = k) \frac{C_{2^l-1}^{kL-1}}{C_{2^l}^{kL}} = 2^{m-l}. \quad (19)$$

На рис. 2 зображено залежність $P_{l,m}$ від m для різних l .

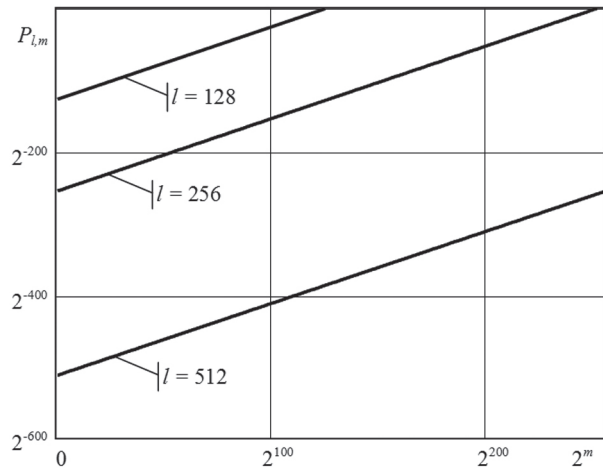


Рис. 2. Залежності ймовірності того, що у шифрґами $\gamma_i, i = 0, 1, \dots, n-1$ довжиною не більше $2^m = 2^{60}$ блоків буде хоча б одне повторення

Із залежностей, які наведено на рис. 2, видно, що підвищення довжини шифрґами веде до зростання ймовірності будь-якої кількості повторень блоків ґами. Ці графіки можна застосовувати для обґрунтування певних обмежень, наприклад, якщо потрібно зменшити ймовірність будь-якої кількості повторень ґами необхідно зменшити її довжину.

ВИСНОВКИ

На підставі отриманих результатів можна зробити такі важливі у практичному значенні висновки.

1. Властивості сучасних симетричних криптоперетворень залежать не лише від характеристик БСШ, але й від режимів його застосування. Тому у проекті національного стандарту ДСТУ «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення» передбачено 10 режимів криптоперетворення: проста заміна (базове перетворення), гамування, гамування зі зворотним зв'язком за шифртекстом, вироблення імітовставки, зчеплення шифрблоків, гамування зі зворотним зв'язком за шифрґамою, вибіркоче гамування із прискореним виробленням імітовставки, вироблення імітовставки і гамування, індексованої заміни, захисту ключових даних.

2. У режимі OFB, який застосовується для забезпечення послуги конфіденційності, вихідне повідомлення захищається шляхом додавання шифрґами, яка формується багаторазовим шифруванням одного і того ж несекретного блоку ініціалізації (синхроросилки). Якщо прийняти припущення про відповідність властивостей шифру певним властивостям випадкової підстановки, тоді періодичність ґами визначатиметься наявністю циклів у випадково обраній підстановці із симетричної групи, причому обрання підстановки задається значенням секретного ключа.

3. Дослідження властивостей випадково обраної підстановки s з симетричної групи S_n показали, що ймовірність виникнення циклу $s_i = (y_i, s_i(y_i), s_i^2(y_i), \dots, s_i^{l_i-1}(y_i))$ будь-якої довжини $L = l_i$ для довільного фіксованого елемента y_i з множини $Y = \{y_1, y_2, \dots, y_n\}$ не залежить ані від цього елемента y_i , ані від довжини циклу $L = l_i$. Ця ймовірність залежить лише від порядку n підстановок симетричної групи S_n і визначається як зворотна величина, тобто дорівнює $1/n$.

4. Таким чином, періодичні властивості гама у режимі гамування зі зворотним зв'язком за шифргамою визначаються за розподілом ймовірностей кількості циклів випадкової підстановки. Обрання секретного ключа, який параметризує шифрувальну функцію, відповідає обранню конкретної підстановки із симетричної групи, обрання значення синхросилки відповідає обранню елемента y_i з множини елементів $Y = \{y_1, y_2, \dots, y_n\}$, над якими здійснюється підстанова. Але ані власне значення синхросилки, ані довжина періоду гама не впливають на ймовірність отримання гама певного періоду. Ця ймовірність визначається лише степенем підстановки $n = 2^l$, тобто за розрядністю l базового шифрувального перетворення.

5. З точки зору практичного застосування симетричних криптоперетворень до шифргама висуваються вимоги неповорності на довжині, що не перевищує встановленої межі. Ймовірність такої події визначається як $1 - 2^{m-l}$, де 2^m – обмеження довжини шифргама. Наприклад, для 128-розрядного шифру «Калина» при обмеженні довжини гама до 2^m у режимі OFB ймовірність того, що блоки гама жодного разу не співпадають, дорівнює $1 - 2^{m-l} = 1 - 2^{-68}$, тобто значно більше за $1 - 2^{-64}$. Зворотна величина $P_{l,m}$, тобто ймовірність того, що на довжині не більше 2^m блоки шифргама в режимі OFB співпадають бодай один раз, дорівнюватиме $P_{l,m} = 2^{m-l}$. Ця залежність може використовуватися для обґрунтування обмежень на довжину шифргама, коли встановлена верхня межа ймовірності $P_{l,m}$.

6. Специфікацією БСШ «Калина» [1, 2] рекомендовано певні обмеження на сумарну довжину повідомлень, що захищаються з використанням одного ключа. Стосовно режиму гамування зі зворотним зв'язком за шифргамою такі обмеження слід розглядати як вимоги до максимальної довжини гама, яка з певною ймовірністю не повторюватиметься. Наведені рекомендації носять принциповий характер, бо саме виникнення повторення гама є найбільш небезпечним випадком в ході застосування режиму OFB, адже в цьому разі зловмисник майже напевно порушить встановлений режим конфіденційності повідомлень. Наприклад, якщо допустима ймовірність повторення блоків гама складає 2^{-64} , тоді довжина гама для $l = 128$ бітного БСШ «Калина» не

має перевищувати 2^{64} блоків (у проекті стандарту це обмеження більш жорсткіше і складає 2^{60}).

7. Отримані оцінки ймовірності формування гама певного періоду можна розглядати і як критерій обрання криптографічних примітивів, або критерій статистичного тестування. Дійсно, якщо досліджуваний криптопримітив у режимі OFB з рівною ймовірністю формує гама будь-якого періоду і ця ймовірність визначається зворотною до степеня підстановки, тоді за циклічними властивостями досліджуваний криптопримітив відповідає ймовірнісним властивостям випадкової підстановки і за цим критерієм може бути прийнятий до застосування. Власне проведення таких досліджень, зокрема, на нелінійних вузлах заміну або на зменшених моделях БСШ є перспективним напрямком подальших робіт. Перспективним також є поширення отриманих результатів на інші режими гамування, зокрема, на режими гамування зі зворотним зв'язком за шифртекстом, вибіркового гамування із прискореним виробленням імітовставки, вироблення імітовставки і гамування тощо.

Література

- [1] ДСТУ. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення [Текст]. - Проект стандарту друга (остаточна) редакція. - Київ: Держспоживстандарт України, 2014. - 238 с.
- [2] Розробка нового блокового симетричного шифру: звіт за перший етап НДР «Алгоритм» (проміжний) / АТ «ІТ»; кер. І.Д. Горбенко – Харків, 2014. - Том 4. - 304 с.
- [3] Сачков В.Н. Введение в комбинаторные методы дискретной математики. - М.: Наука. Гл. ред. физ.-мат. лит., 1982. - 384 с.
- [4] Тронин С.Н. Введение в теорию групп. - Казань: Казанский государственный университет, 2006. - 100 с.
- [5] Александров П.С. Введение в теорию групп. - М.: Наука, - 1980. - 145 с.
- [6] Долгов В.И., Лисицкая И.В., Руженцев В.И. Анализ циклических свойств блочных шифров // Прикладная радиоэлектроника - 2007. - Т. 6, № 2. - С. 257–263.
- [7] Кузнецов А.А., Лисицкая И.В., Исаев С.А. Линейные свойства блочных симметричных шифров, представленных на украинский конкурс // Прикладная радиоэлектроника. - 2011. - Т. 10, №2 - С. 135–140.
- [8] Сорока Л.С., Кузнецов А.А., Московченко И.В., Исаев С.А. Исследование дифференциальных свойств блочно-симметричных шифров. // Системы обработки информации. - X: ХУПС. -2010 - Вип. 6(87). - С. 286–294.
- [9] Долгов В.И., Родинко М.Ю. Блочные симметричные шифры – случайные подстановки. Комбинаторные показатели // Прикладная радиоэлектроника - 2013. - Т.12, №2 - С. 236–239.
- [10] Кузнецов О. О. Анализ коллизионных властивостей режиму вироблення імітовставок із вибірко-

вим ґамуванням / О. О. Кузнецов, Д. В. Іваненко, Є.П. Колованова // Вісник Харківського національного університету ім. В. Н. Каразіна серія «Математичне моделювання. Інформаційні технології. Автоматизовані системи управління». — 2014. — № 1097, Т. 23. — С. 55–71.

Надійшла до редколегії 2.09.2014

Кузнецов Олександр Олександрович, фото та відомості про автора див. на стор. 207.



Горбенко Юрій Іванович, кандидат технічних наук, технічний директор АТ «ІТ». Наукові інтереси: криптографічні системи та протоколи, проектування та розробка систем, комплексів та засобів криптографічного захисту інформації.

Колованова Євгенія Павлівна, фото та відомості про автора див. на стор. 207.

УДК 004.056.55

Периодические свойства шифрґаммы в режиме Output Feedback / А.А. Кузнецов, Ю.И. Горбенко, Е.П. Колованова // Прикладная радиоэлектроника: научн.-техн. журнал. — 2014. — Том 13. — № 3. — С. 239–251.

Исследуются свойства режима ґаммирования с обратной связью по шифрґамме (англоязычное обозначение — Output Feedback). С применением матема-

тического аппарата теории подстановок исследуются периодические свойства ґаммы, в частности проводится оценка вероятности появления ґаммы определенного периода при условии соответствия свойств шифра определенным свойствам случайной подстановки. Разрабатываются практические рекомендации по применению режима ґаммирования с обратной связью по шифрґамме, обосновываются требования и ограничения, вытекающие из полученных оценок периодических свойств ґаммы.

Ключевые слова: режим шифрования, периодичность ґаммы, случайная подстановка, Output Feedback. Табл.: 5. Ил.: 2. Библиогр.: 10 назв.

UDC 004.056.55

Periodic properties of the Output Feedback mode / A.A. Kuznetsov, Yu.I. Gorbenko, E.P. Kolovanova // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 239–251.

The properties of the Output Feedback mode are investigated in this paper. Periodic properties are investigated using the mathematical apparatus of permutations theory. In particular, estimating the probability of occurrence of a specified period ґamma is performed, when the properties of the cipher meet certain properties of a random permutation. Practical recommendations for using the Output Feedback mode are developed. Requirements and restrictions arising from of the above estimates of the periodic ґamma properties are justified.

Keywords: encryption mode, sequence period, random permutation, Output Feedback.

Tab.: 5. Fig.: 2. Ref.: 10 items.