УДК 004.056.55: 519.248

КЛАСИФІКАЦІЯ ПЕРЕСТАНОВОК ЗІ СПЕЦІАЛЬНИМИ ВЛАСТИВОСТЯМИ ТА ОЦІНКА ПОТУЖНОСТЕЙ КЛАСІВ

М. К. Бурлака[1, a]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

Анотація

Розглядаються перестановки, які використовуються у якості ключів шифрування у роторних шифраторах. Введено поняття характеристики перестановки, яка визначає ефективність їх застосування у роторних шифрувальних машинах, та за характеристиками виділено різні класи перестановок. Приводяться результати статистичного моделювання для оцінок частки перестановок отриманих класів серед усіх перестановок різного порядку.

Ключові слова: перестановка, криптографія, класифікація, ключ шифрування, роторний шифратор, статистичне моделювання, оцінка імовірності

Вступ

Важливою складовою стійкості криптосистеми є визначення множини задовільних ключів шифрування. Для роторних шифраторів ключем являється початковий стан роторів та перестановки в кожному з декількох послідовних роторів, в залежності від яких перетворення відкритого тексту у шифротекст може виявитися більш або менш ефективним. Так як кожен з роторів класичного роторного шифратора, у якого три ротори, виконує моноалфавітну підстановку, а розташування самих роторів може змінюватися, то загальна кількість ключів на англійскому алфавіті становить 3!·26!. Проте не всі ключі є застосовними (наприклад, ті, які кожну літеру відкритого тексту переводять саму у себе).

Метою даної роботи є визначення застосовності перестановки у якості підключа шифрування у роторних шифраторах за допомогою аналізу криптографічних властивостей перестановки і оцінки кількості перестановок із заданими характеристиками за допомогою методу статистичного моделювання з генеруванням випадкових перестановок.

1. Характеристики перестановок та їх властивості

Нехай є множина $\{0, 1, \dots, n-1\}$ і деяка її перестановка $(i_0, i_1, \dots, i_{n-1})$. За правилом

$$\begin{array}{c|cccc} \boxplus & 0 & 1 & \dots & n-1 \\ & i_0 & i_1 & \dots & i_{n-1} \\ \hline & j_0 & j_1 & \cdots & j_{n-1} \end{array}$$

отримуємо послідовність $(j_0, j_1, \dots, j_{n-1})$ лишків покоординатної суми $k + i_k$ за модулем n. Усі $j_t, t = \overline{0, n-1}$ належать множині $\{0, 1, \dots, n-1\}$ і не обов'язково є різними. Нехай k_0 – кількість нулів серед $(j_0, j_1, \dots, j_{n-1})$, k_1 – кількість одиниць, …, k_{n-1} – кількість $n-1$. Перепишемо мультимножину $\{j_0, j_1, \dots, j_{n-1}\}$ у вигляді:

$$\{0^{k_0}, 1^{k_1}, \dots, (n-1)^{k_{n-1}}\}.$$

Нескладно бачити, що для $\{k_0, k_1, \dots, k_{n-1}\}$ має виконуватися

$$\sum_{j=0}^{n-1} k_j = n.$$

Характеристикою перестановки $(i_0, i_1, \dots, i_{n-1})$ множини $\{0, 1, \dots, n-1\}$ з відповідним набором $\{k_0, k_1, \dots, k_{n-1}\}$ будемо називати послідовність $(\alpha_0, \alpha_1, \dots, \alpha_n)$, де α_i – кількість чисел k_j, що зустрічаються i разів.

Для характеристик перестановок справедлива наступна рівність:

$$\sum_{i=0}^{n} i\alpha_i = n.$$

Криптографічна якість перестановки для реалізації шифру залежить від характеристики даної перестановки. Чим більше значення другої позиції характеристики перестановки (тобто чим більше унікальних лишків суми за модулем n), тим краще ця перестановка для використання у якості підключа шифрування у роторних шифраторах. Якщо характеристики кількох перестановок співпадають, то ці перестановки мають однакові криптографічні властивості для роторних систем, та, відповідно, криптоаналіз систем, побудованих із використанням таких перестановок, має складність одного порядку.

[a] maria.k.burlaka@gmail.com

2. Оцінки потужності класів та ймовірності перестановок з різними характеристиками

Перестановка $(i_0, i_1, \ldots, i_{n-1})$ множини $\{0, 1, \ldots, n-1\}$ називається перестановкою «без паралельних перепайок», якщо

$$\forall k, l \in \{0, 1, \ldots, n-1\} :$$
$$(k + i_k) \not\equiv (l + i_l) \,(\mathrm{mod} n) \text{ при } k \neq l.$$

Назва таких перестановок пов'язана з конструкцією класичних роторів, в яких контакти правої та лівої сторони ротора з'єднувалися дротами без паралельних пар. Таким ротором реалізується найкращий для застосування вид перестановок – перестановка «без паралельних перепайок».

Так як для перестановки «без паралельних перепайок» усі залишки $j_t, t = \overline{0, n-1}$, є унікальними, то характеристика такої перестановки – це послідовність виду $(0, n, 0, \ldots, 0)$.

Методом повного перебору перестановок порядку $n = 11$ та обчислення їх характеристик були отримані усі класи перестановок та встановлена потужність кожного класу, в тому числі і класу перестановок без «паралельних перепайок». У табл. 1 наведені деякі класи з точною імовірністю отримати перестановку з цих класів при випадковому виборі.

Табл. 1. Точна імовірність появи перестановок з наведеними характеристиками для $n = 11$

N	α_0	α_1	α_2	α_3	α_4	$\ldots$	α_{12}	P_n
1	4	4	2	1	0	0	0	0.206735
2	5	3	2	0	1	0	0	0.050532
3	0	11	0	0	0	0	0	0.000948
4	8	0	0	1	2	0	0	0.000076
5	10	0	0	0	0	0	1	$3 \cdot 10^{-7}$

Отримана імовірність для класу перестановок без «паралельних перепайок» порядку $n = 11$ ($N = 3$, табл. 1) повністю збігається з приведеною у статті [1]. Аналогічні результати були отримані при застосуванні статистичного моделювання і генерації 10^7 випадкових перестановок. Наведені у табл. 1 та 2 дані дуже близькі, що свідчить про ефективність методу для оцінки потужностей класів перестановок.

Також статистичним моделюванням були отримані класи перестановок для $n = 11 - 19, 25, 35, 45, 155$. У табл. 3 наведені деякі з класів для $n = 45$.

Табл. 2. Статистично змодельована імовірність появи перестановок з наведеними характеристиками для $n = 11$

N	α_0	α_1	α_2	α_3	α_4	$\ldots$	α_{12}	P_n
1	4	4	2	1	0	0	0	0.206749
2	5	3	2	0	1	0	0	0.050543
3	0	11	0	0	0	0	0	0.000951
4	8	0	0	1	2	0	0	0.000076
5	10	0	0	0	0	0	1	$14 \cdot 10^{-7}$

Перестановкою множини довжини n з виродженою характеристикою будемо називати перестановку з характеристикою виду $\{n-1, 0, \ldots, 0, 1\}$. Фактично це означає, що усі лишки суми за модулем n є однаковими, що значно спрощує криптоаналіз шифру.

Табл. 3. Статистично змодельована імовірність появи перестановок з наведеними характеристиками для $n = 45$

N	α_0	α_1	α_2	α_3	α_4	$\ldots$	α_{46}	P_n
1	15	18	9	3	0	0	0	0.028728
2	14	21	8	0	2	0	0	0.001085
3	21	8	11	5	0	0	0	0.000357
4	26	5	5	6	3	0	0	$1 \cdot 10^{-7}$
5	0	45	0	0	0	0	0	0

Частка перестановок із виродженою характеристикою серед усіх можливих перестановок множини дуже мала ($N = 5$, табл. 1, 2 та 3). В результаті проведених експериментів для $n = 11 - 19, 25, 35, 45, 155$ найбільша їх кількість була отримана при $n = 11$ ($P_{11} = 0.0000014$). При статистичному моделюванні перестановок з іншими значеннями n зустічалася лише одна перестанока з виродженою характеристикою або не зустрічалися зовсім, тобто їх імовірності при випадковому виборі близькі до нуля.

На відміну від перестановок без паралельних перепайок, які є найбільш вдалими для застосування у роторних шифраторах, перестановки з виродженою характеристикою є зовсім не застосовними.

Висновки

У роботі введено поняття характеристики перестановок, які використовуються як підключі у роторних шифрувальних машинах. Оскільки характеристика перестановки впливає на ефективність та стійкість при їх застосування у роторних шифрувальних машинах, то актуальною задачею є оцінка потужності різних класів перестановок. Проведено статистичне моделювання та наведено результати експериментів для знаходження оцінок потужності виділених класів перестановок різного порядку. Показано, що імовірність випадково вибрати перестановку з високими криптографічними властивостями швидко зменшується з ростом порядку перестановки. Для використання в криптографічних системах необхідно розробляти ефективні алгоритми для генерування перестановок з різними криптографічними характеристиками. У подальших дослідженнях необхідно виявити та описати інші класи і побудувати довірчі інтервали для оцінок їх потужностей за допомогою апроксимації розподілу Бернулі до нормального розподілу та розподілу Пуассона.

Перелік використаних джерел

1. Cooper C., Gilchrist R., Kovalenko I. N., Novacovic D. Deriving the number of good permutations with applications to cryptography // Кибернетика и системный анализ. — 1999. — № 5. — С. 10–16.