# Ланцюги Підпросторів Калина-Подібних Шифрів

Коляда Марія, Яковлєв Сергій
кафедра математичних методів захисту інформації
Фізико-технічний інститут
НТУУ «Київський політехнічний інститут імені І.Сікорського»
Київ, Україна
kolyadamariya1710@gmail.com, yasv@rl.kiev.ua

# Subspace Trails of Kalyna-Like Block Ciphers

Mariya Kolyada, Serhii Yakovliev
dept. of Mathematical Methods of Information Security
Institute of Physics and Technology
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
Kyiv, Ukraine
kolyadamariya1710@gmail.com, yasv@rl.kiev.ua

***Анотація*—У даній роботі наведено типи та приклади ланцюгів підпросторів для одного, двох, трьох та чотирьох раундів «Калина»-подібних шифрів.**

***Abstract*—We present types and examples of subspace trails for one, two, three and four rounds of "Kalyna"-type block ciphers.**

***Ключові слова—симетрична криптографія; блокові шифри; «Калина»; ланцюги підпросторів.***

***Keywords—symmetric cryptography; block ciphers; Kalyna cipher; subspace trails***

## I. Вступ

Наявність у блоковому шифрі характеристик із нерівноімовірним розподілом дозволяє будувати ефективні стастистичні атаки відновлення раундових ключів або ключа шифрування загалом. Пошук та аналіз поведінки таких нерівномірних статистик є постійно актуальною криптографічною задачею.

Дослідження ланцюгів підпросторів було вперше запропоноване у 2011 році для криптоаналізу шифру PRINTcipher [3], після чого ідея такого аналізу була ефективно застосована для шифру AES [1]. Для проведення такого аналізу у [1] запропонована техніка використання спеціальним чином підібраних вхідних даних, поведінку яких можна спрогнозувати після декількох раундів шифрування; при цьому від шифру не вимагається наявність спеціальних симетрій або констант.

У даній роботі ми розглянемо ланцюги підпросторів, які можна побудувати для блокових шифрів із структурою алгоритму шифрування «Калина» (ДСТУ 7624:2014 [2]), та покажемо, як можна застосувати техніку аналізу ланцюгів підпросторів для «Калина»-подібних шифрів.

## II. Короткий опис блокового шифру «Калина»

Симетричний блоковий шифр «Калина» [3] був стандартизований як національний стандарт ДСТУ 7624 у 2014 році та введений у дію з 2015 року [4] (зауважимо, що попередня опублікована версія шифру «Калина» під такою ж назвою має суттєві структурні відмінності [5]). Структура шифру «Калина» подібна до структури шифру *Rijndael*, але орієнтована на 64-бітні обчислювальні архітектури. Кількість раундів залежить від довжини відкритого тексту та довжини ключа. Відкритий текст подається у вигляді матриці розміром a×8, де $a \in \{2,4,8\}$. Базові перетворення для шифрування:

$$E_{l,k}^{K} = AddKey^{K'} \circ MixColumns \circ ShiftRows \circ SubBytes \circ$$
$$\circ \prod_{i=1}^{t-1} ( AddKey^{Ki} \circ MixColumns \circ ShiftRows \circ SubBytes ) \circ$$
$$\circ AddKey^{K0'}$$

де $l$ – розмір внутрішнього стану блокового шифру (у бітах), $K$ – ключ шифрування, $k$ – довжина ключа шифрування (у бітах), $AddKey^{K'}$ – функція додавання раундового ключа $K$ за модулем $2^{64}$, *MixColumns* – лінійне перетворення (множення матриці лінійного перетворення на матрицю внутрішнього стану над скінченним полем), *ShiftRows* – перестановка елементів $g_{i,j} \in GF(2^8)$ внутрішнього стану (циклічний зсув рядків вправо при матричному поданні), *SubBytes* (*SB*) – шар нелінійного бієктивного відображення, який виконує обробку векторів,

заданих над $V_8$ (байтова підстановка), $AddKey^K$ функція додавання циклового ключа $K$ за модулем 2.

Позначимо через R одне раундове перетворення, тобто послідовне виконання процедур *SubBytes*, *ShiftRows* та *MixColumns*, а також додавання із ключем. Через $R^{(i)}$ будемо позначати процедуру, яка складається з виконання послідовних $i$ раундів (включно із додаванням проміжних раундових ключів).

Процедура *ShiftRows* (*SR*) виконує циклічний зсув вправо рядків матриці стану $g_{i,j} \in GF(2^8)$. Кількість елементів зсуву залежить від номеру рядку $i \in \{0,1,\ldots,7\}$, розміру блоку $l \in \{128\ 256,\ 512\}$, та обчислюється за формулою $\delta_i = \left|\frac{i*l}{512}\right|$.

Процедура *MixColumns* (*MC*) виконує множення кожного стовпчику матриці стану на спеціально підібрану матрицю. Кожен елемент $g_{i,j}$, матриці внутрішнього стану $G=(g_{i,j})$ розглядається як елемент скінченного поля $GF(2^8)$, яке утворене незвідним поліномом $\vartheta(x) = x^8 + x^4 + x^3 + x^2 + 1$. Відповідно, кожен елемент результуючої матриці стану $W=(w_{i,j})$ одержується як результат множення векторів довжини 8 над скінченним полем $GF(2^8)$ за формулою $w_{i,j} = v >>> i \otimes G_j$, де $\upsilon$ = (0x01, 0x01, 0x05, 0x01, 0x08, 0x06, 0x07, 0x04) – вектор, що утворює циркулянтну матрицю МДР-коду і складається з послідовності байтових констант у шістнадцятковому поданні, які інтерпретуються як елементи поля $GF(2^8)$, при цьому циклічний зсув виконується відносно елементів вектора над скінченним полем.

Більш детальну інформацію про структуру та особливості блокового шифру ДСТУ 7624:2014 «Калина» можна одержати у [3, 4].

## III. Ланцюги підпросторів ітеративних блокових шифрів

Нехай $F$ – раундова функція в ітеративному блочному шифрі:

$$E_K(m) = k_n \oplus F(\ldots F(k_1 \oplus F(k_0 \oplus m))),$$

де $k_i$ – раундові ключі, отримані з основного ключа $K$ за допомогою певного ключового розкладу. Вхідні повідомлення $m$ розглядаються як бітові вектори із лінійного простору всіх бітових векторів відповідної довжини. Підпростір $V$ лінійного простору вхідних повідомлень є інваріантним відносно $F$, якщо $F(V) = V$; однак наявність таких підпросторів для сучасних блокових шифрів є малоімовірною.

Нехай для підпростору $V$ існують класи суміжності $V \oplus a$ та $V \oplus a'$ такі, що $F(V \oplus a) = V \oplus a'$; тоді, якщо раундовий ключ K міститься в $V \oplus (a \oplus a')$, то $F(V \oplus a) \oplus K = V \oplus a$ і клас суміжності $V \oplus a$ є інваріантним відносно $F$. Якщо для довільного $a$, існує унікальне $b$ таке, що $F(V \oplus a) \oplus K = V \oplus b$, то будемо казати, що підпростір $V$ *зберігає інваріантність відносно* $F$. Це значить, що для довільного початкового підпростору $V \oplus a$ ми можемо поставити в відповідність інший підпростір $V \oplus b$, де $b$ залежить від $a$ та від раундового ключа. У більш загальному випадку ми розглядаємо пару підпросторів $V_1$ та $V_2$ таких, що для довільного вектору a існує унікальний вектор b (який залежить від $a$ та ключа) повинне виконуватись співвідношення $F(V_1 \oplus a) \oplus K \subseteq V_2 \oplus b$, тобто F переводить кожен клас суміжності у якийсь інший клас суміжності.

*Ланцюгом підпросторів довжини r* назвемо простий кортеж з $r+1$ підпросторів $(V_1, V_2, \ldots, V_{r+1})$, для яких виконуються співвідношення

$$F(V_i \oplus a_i) \oplus K \subseteq V_{i+1} \oplus a_{i+1}.$$

Позначимо через $E=\{e_{0,0}, \ldots, e_{a,8}\}$, $a \in \{2,4,8\}$, простір початкових станів шифру «Калина», де $e_{i,j}$ – окремі байти (8-бітові рядки), $a$ – кількість стовпчиків. Визначимо чотири сімейства підпросторів $E$:

діагональний простір,

інверсно-діагональний простір,

стовпчиковий простір,

змішаний простір.

У шифрі «Калина» передбачено 3 різні форми вхідних даних, в залежності від їх довжини; опис підпросторів буде наведено для всіх можливих довжин блоків.

*Стовпчиковий простір* $C_i$ визначимо як $C_i = \langle e_{0,i}, e_{1,i}, e_{2,i}, e_{3,i}, e_{4,i}, e_{5,i}, e_{6,i}, e_{7,i} \rangle$. Наприклад, $C_0$ для випадку 8*8 буде мати вид, наведений на рис. 1:

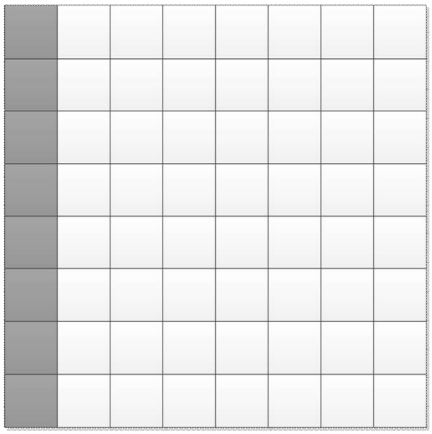

Рис. 1. Схематичний вид простору $C_0$ розміром 8*8. Сірим позначено ненульові координати елементів простору.

*Діагональний простір* $D_i$ визначимо таким чином:

Для випадку 8x8: $D_i = SR^{-1}(C_i) = \langle e_{7,i}, e_{6,i+1}, e_{5,i+2}, e_{4,i+3}, e_{3,i+4}, e_{2,i+5}, e_{1,i+6}, e_{0,i+7} \rangle$, де індекс $i+j$ обчислюється за модулем 8, $i \in \{0,\ldots,7\}$. Наприклад, $D_0$ буде мати вид, наведений на рис. 2:

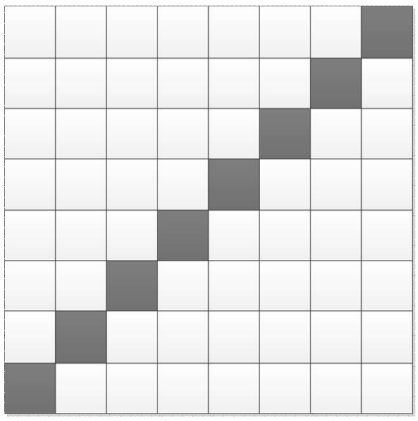

Рис. 2. Схематичний вид простору $D_0$ розміром 8*8. Сірим позначено ненульові координати елементів простору.

Для випадку 4x8: $D_i = SR^{-1}(C_i) = \langle e_{7,i}, e_{6,i}, e_{5,i+1}, e_{4,i+1}, e_{3,i+2}, e_{2,i+2}, e_{1,i+3}, e_{0,i+3} \rangle$, де індекс $i+j$ обчислюється за модулем 4, $i \in \{0,1,2,3\}$.

Для випадку 2x8: $D_i = SR^{-1}(C_i) = \langle e_{7,i}, e_{6,i}, e_{5,i}, e_{4,i}, e_{3,i+1}, e_{2,i+1}, e_{1,i+1}, e_{0,i+1} \rangle$ , де індекс $i+j$ обчислюється за модулем 2, $i \in \{0,1\}$.

*Інверсно-діагональний простір* $ID_i$ визначимо таким чином:

Для випадку 8*8: $ID_i = SR(C_i) = \langle e_{0,i}, e_{1,i+1}, e_{2,i+2}, e_{3,i+3}, e_{4,i+4}, e_{5,i+5}, e_{6,i+6}, e_{7,i+7} \rangle$ ,де індекс $i+j$ обчислюється за модулем 8, $i \in \{0,\ldots,7\}$. Наприклад, $ID_0$ буде мати вид, наведений на рис. 3:

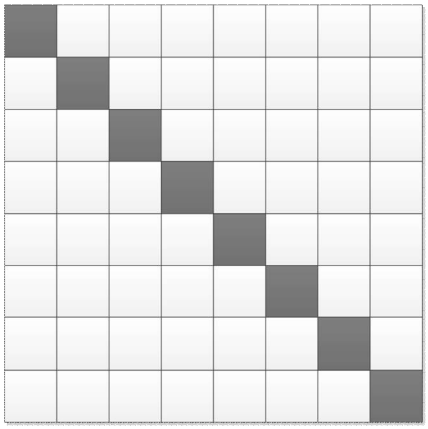

Рис. 3. Схематичний вид простору $ID_0$ розміром 8*8. Сірим позначено ненульові координати елементів простору.

Для випадку 4*8: $ID_i = SR(C_i) = \langle e_{0,i}, e_{1,i}, e_{2,i+1}, e_{3,i+1}, e_{4,i+2}, e_{5,i+2}, e_{6,i+3}, e_{7,i+3} \rangle$ ,де індекс $i+j$ розраховується за модулем 4, $i \in \{0,1,2,3\}$.

Для випадку 2*8: $ID_i = SR(C_i) = \langle e_{0,i}, e_{1,i}, e_{2,i}, e_{3,i}, e_{4,i+1}, e_{5,i+1}, e_{6,i+1}, e_{7,i+1} \rangle$ ,де індекс $i+j$ розраховується за модулем 2, $i \in \{0,1\}$.

*Змішаний простір* $M_i$ визначимо таким чином:

$$M_i = MC(ID_i).$$

## IV. Ланцюги підпросторів для одного та двох раундів шифру «Калина»

Побудуємо ланцюги підпросторів для двох, трьох та чотирьох раундів шифру «Калина-512» (вхідні дані трактуються як матриця 8x8). Для шифрів «Калина-256» та «Калина-128» (вхідні дані трактуються як матриці 4x8 та 2x8 відповідно) існують аналогічні ланцюги, які описуються таким само чином.

Опишемо деякі ланцюги підпросторів для одного раунду шифрування.

1) Нехай $I \subseteq \{0,1,2,3,4,5,6,7\}$, де $0 < |I| < 8$ та $a \in D_I^{\perp}$, тоді існує унікальне $b \in C_I^{\perp}$, таке що

$$R_K(D_I \oplus a) = C_I \oplus b .$$

2) Нехай $I \subseteq \{0,1,2,3,4,5,6,7\}$, де $0<|I|<8$, та $a \in C_I^{\perp}$, тоді існує унікальне $b \in M_I^{\perp}$, таке, що

$$R_K(C_I \oplus a) = M_I \oplus b .$$

Процес проходження підпросторів, які розглядались у випадках 1) та 2), наведено на рис. 4.

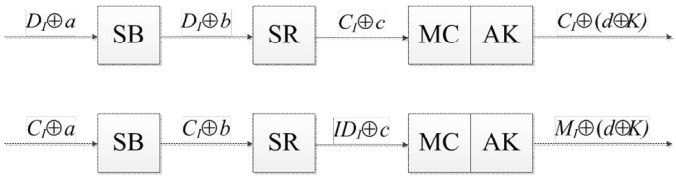


Рис. 4. Візуальне представлення ланцюгів підпросторів для одного раунду.

Нехай $R^{(2)}$ визначає процедуру зашифрування двох раундів «Калини» з раундовими ключами $K_1$, $K_2$. Опишемо ланцюги підпросторів для них.

3) Якщо відкритий текст належав класу суміжності діагонального підпростору, то результат його шифрування буде належати класу суміжності змішаного підпростору. Зокрема, після 2-х раундів шифрування з фіксованим ключем отримаємо:

$$Pr(R^{(2)}(u) \oplus R^{(2)}(v) \in M_I \mid u \oplus v \in D_I) = 1 \ \text{™}\sum u \neq v .$$

4) Якщо два відкритих тексти належать різним класам суміжності діагонального простору, то результат їх шифрування буде належати різним класам суміжності змішаного простору. Інакше

$$Pr(R^{(2)}(u) \oplus R^{(2)}(v) \in M_I \mid u \oplus v \notin D_I) = 0 , \ \text{™}\sum u \neq v .$$

5) З відкритого тексту, який належить класу суміжності діагонального простору, неможливо за два раунди

шифрування одержати шифртекст із класу суміжності діагонального простору:

$$Pr(R^{(2)}(u) \oplus R^{(2)}(v) \in D_J \mid u \oplus v \in D_I) = 0\ ,\ ™\sum u \neq v\ .$$

6) З відкритого тексту, який належить класу суміжності змішаного простору, неможливо за два раунди шифрування одержати шифртекст із класу суміжності змішаного простору:

$$Pr(R^{(2)}(u) \oplus R^{(2)}(v) \in M_J \mid u \oplus v \in M_I) = 0\ ,\ \text{де}\ u \neq v\ .$$

Ці властивості використовуються як відмінна риса для криптоаналізу двох раундів шифрування. Візьмемо два відкритих тексти з $D_I$, з $I \subseteq \{0,1,2,3,4,5,6,7\}$, де $0 < |I| < 8$; з імовірністю 1 після двох раундів вони потраплять у підпростір $M_I$. Якщо замість «Калини» застосувати до цих текстів випадкову перестановку (ідеальний шифр), то ймовірність того, що вони потраплять в однаковий підпростір $M_I$ дорівнює $(2^8)^{-64+8*|I|}$. Таким чином, достатньо однієї пари, щоб відрізнити випадкову перестановку від двох раундів шифрування «Калиною».

## V. Ланцюги підпросторів для трьох та чотирьох раундів шифру «Калина»

Опишемо ланцюги підпросторів для трьох раундів шифрування «Калини».

Для довільних $M_I$ та $C_J$ маємо:

$$Pr(x \in C_j | x \in M_I) = (2^8)^{-8|I|+|I||J|}.$$

Відповідно, клас суміжності простору $M_I$ можна представити як об'єднання класів суміжності простору $C_J$:

$$M_I \oplus a = \bigcup_{x \in M_I \oplus a \setminus C_J} C_J \oplus x\ .$$

Відмітимо, що кількість векторів $x \in M_I \oplus a \setminus C_J$ точно дорівнює $(2^8)^{8|I|-|I||J|}$.

Розглянемо два елементи з одного класу суміжності $D_I$. Після двох раундів они будуть належати одному класу суміжності простору $M_I$. Клас суміжності $M_I$ може бути представлений у вигляді об'єднання $N = (2^8)^{8|I|-|I||J|}$ класів суміжності $A_1, A_2, \ldots, A_N$ простору $C_J$. Імовірність, що ці два елементи належать одному класу суміжності $C_J$ після двох раундів шифрування, дорівнює $(2^8)^{-8|I|+|I||J|}$. Відповідно, після третього раунду шифрування ці два елементи перейдуть у один клас суміжності змішаного простору (див. рис. 5).

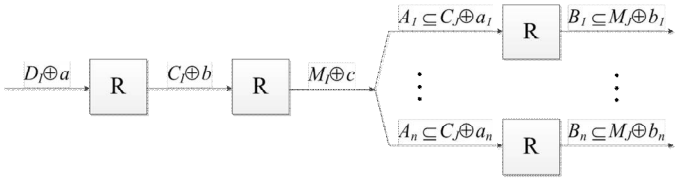


Рис. 5. Візуальне представлення ланцюгів підпросторів для трьох раундів шифрування.

Позначимо через $p_1$ ймовірність того, що випадкових відкритих тексти після трьох раундів шифрування належатимуть одному класу суміжності простору $M_J$, а через $p_2$ – ймовірність того, що у один клас суміжності $M_J$ після трьох раундів потраплять два відкритих тексти, які належать одному класу суміжності простору $D_I$. Дані ймовірності обчислюються за формулами

$$p_1 = C_8^{|J|}\,(2^8)^{-64+8*|J|},\ p_2 = C_8^{|J|}\,(2^8)^{-8*|I|+|I||J|}.$$

Легко помітити, що ймовірність одержати колізію у другому варианті вища, ніж при випадковому виборі. Зокрема, для $|J|=7$ та $|I|=1$ маємо $p_2 = 2^{-5}$, в той час коли $p_1 = 2^{-61}$. Звернемо увагу, що $I$ та $J$ підкоряються умові: $0<|I|+|J|\leq 7$.

Для чотирьох раундів можна побудувати ланцюги підпросторів, використовуючи просту композицію властивостей ланцюгів підпросторів для двох раундів, описану у пунктах 3) та 6) попереднього розділу. Маємо:

$$Pr(R^{(4)}(u) \oplus R^{(4)}(v) \in M_J \mid u \oplus v \in D_I) = 0\ ,\ \text{де}\ u \neq v\ .$$

Іншими словами, за чотири раунди шифрування тексти, які належать одному класу суміжності діагонального простору, не можуть потрапити у один клас суміжності змішаного простору. Це також дає змогу побудувати розпізнавач для чотирираундової «Калини». Інший шлях для побудови чотирираундових ланцюгів – розбиття класу суміжності змішаного простору на сукупність класів суміжності діагональних просторів та застосування техніки, аналогічної для побудови трираундових ланцюгів.

## VI. Висновки

У даній роботі було побудовано декілька ланцюгів підпросторів для перших чотирьох раундів шифрування шифру «Калина» та проведено їх попередній аналіз. Дані результати залежать лише від структури матриці стану шифру та його лінійних перетворень, а тому переносяться на довільні «Калина»-подібні шифри.

В подальшому на основі проведеного аналізу планується побудувати атаки розпізнавання на «Калина»-подібні шифри із зменшеною кількістю раундів.

## Література References


[1] Gregor Leander, Mohamed Ahmed Abdelraheem, Hoda AlKhzaimi, and Erik Zenner. A Cryptanalysis of PRINTcipher: The Invariant Subspace Attack. In *Advances in Cryptology* – CRYPTO 2011: 31st Annual Cryptology Conference,Santa Barbara, CA, USA, 2011. Proceedings, pages 206–221, 2011.

[2] Lorenzo Grassi, Christian Rechberger and Sondre Ronjom, "Subspace Trail Cryptanalysis and its Applications to AES" [Online] – http://eprint.iacr.org/2016/592

[3] Roman Oliynykov, Ivan Gorbenko, Oleksandr Kazymyrov et al. "A New Encryption Standard of Ukraine: The Kalyna Block Cipher" [Online]. – http://eprint.iacr.org/2015/650

[4] Інформаційні технології. Криптографічний захист інфомації. Алгоритм симетричного блокового перетворення: ДСТУ 7624:2014. – К.: Держспоживстандарт України, 2015. – 238 с.

[5] І.Д. Горбенко, Перспективний блоковий шифр "Калина" – основні положення та специфікація / І.Д. Горбенко, О.С. Тоцький, С.В. Казьміна та ін. // Прикладна радіоелектроніка. – 2007. – Т.6, №2. – С.195-208