

# Індекси Розгалуження Матриць над Кільцями Лишків

Олег Курінний, Сергій Яковлєв  
кафедра математичних методів захисту інформації  
Фізико-технічний інститут  
Національний технічний університет України «Київський політехнічний інститут ім. Ігоря Сікорського»  
Київ, Україна  
[ol.kurinnoy@gmail.com](mailto:ol.kurinnoy@gmail.com), [yasv@rl.kiev.ua](mailto:yasv@rl.kiev.ua)

## The Branch Number of Matrices over Residue Rings

Oleh Kurinnyi, Serhii Yakovliev  
Department of Mathematical Methods of Information Security  
Institute of Physics and Technology  
National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”  
Kyiv, Ukraine  
[ol.kurinnoy@gmail.com](mailto:ol.kurinnoy@gmail.com), [yasv@rl.kiev.ua](mailto:yasv@rl.kiev.ua)

**Анотація**—Доведено, що індекс розгалуження матриці над кільцем лишків за модулем  $2^n$  зберігається при гомоморфному відображенні у  $(0, 1)$ -матрицю над двійковим лінійним простором. Грунтуючись на цьому, були запропоновані шляхи підсилення криптографічної стійкості таких блокових шифрів, як ARIA та Midori, за рахунок переходу до операцій у кільці лишків під час шифрування.

**Abstract**—We prove that branch number of a matrix over residue ring modulo  $2^n$  is an invariant under homomorphic mapping to  $(0, 1)$ -matrix over binary linear space. With this result we propose some ways to increase cryptographic security of ciphers like ARIA or Midori at the expense of modular operations usage within encryption.

**Ключові слова**—індекс розгалуження, матриці над кільцями лишків,  $(0,1)$ -матриці, шифр ARIA, шифр Midori.

**Keywords**—branch number, matrices over residue rings,  $(0,1)$ -matrices, ARIA cipher, Midori cipher.

### I. ВСТУП

Стратегія широкого шляху, запропонована Йоном Деменом у 1998 році [7], постулює, що стійкість симетричних шифрів до відомих методів криптоаналізу визначається не лише і не тільки якістю нелінійних перетворень (S-блоків), але й властивостями лінійних перемішуючих перетворень шифрів – зокрема, максимально можливих лавинних ефектів. У рамках даної стратегії для побудови шифрів SQUARE та Rijndael (пізніше стандартизованого як AES) використовувались спеціальні конструкції, так звані *MDS-матриці* над

скінченними полями, які мають максимальний індекс розгалуження. Саме завдяки цій властивості вдалось довести як практичну [8], так і теоретичну [9] стійкість AES до диференціального та лінійного криптоаналізу.

У сучасних блокових шифрах лінійні перетворення можуть визначатись матрицями над довільними алгебраїчними структурами, які надають ті чи інші переваги з точки зору криптостійкості або ефективності реалізації. У даній роботі розглядаються матричні перетворення над кільцями лишків за модулем  $2^n$ . Подібні структури зазвичай забезпечують високу швидкість при реалізації та певний рівень стійкості від різних криптоаналітичних атак.

На відміну від матриць над скінченними полями, для матриць над кільцями лишків не було опубліковано аналітичних оцінок на значення індексу розгалуження. У даній роботі буде показано, що матричні перетворення над кільцями лишків мають властивості, подібні до  $(0,1)$ -матриць над полем  $F_2$  і, таким чином, для оцінки їх індексу розгалуження можна застосувати відомі результати, одержані для двійкових матриць [1]. Як наслідок, запропоновано простий спосіб підвищення стійкості SP-мереж типу ARIA або Midori до диференціального та лінійного криптоаналізу за рахунок переходу на інші алгебраїчні операції у лінійному шарі.

### II. ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

Більшість існуючих блокових шифрів зі структурою SP-мережі використовуює в якості лінійного шару матричне

перетворення. Як правило, матриці розглядаються над однією з трьох таких алгебраїчних структур:

1) скінченне поле  $GF(2^n)$  із відповідними операціями додавання та множення у полі;

2) кільце лишків  $Z_2^n$  із операціями додавання та множення за модулем  $2^n$ ;

3) лінійний векторний простір  $V_n = \{0, 1\}^n$  із операцією побітового додавання та множенням на скалярі 0 та 1.

Останній випадок описує використання  $(0, 1)$ -матриць. Відмова від (можливої) операції множення координат вхідних векторів направлена на підвищення швидкості виконання обчислень, що є важливим для алгоритмів легкої криптографії, призначених для реалізації у малопотужних пристроях.

Для деякого вектору  $x$  вага вектору  $wt(x)$  дорівнює кількості ненульових координат у векторі. Для двійкових векторів введена таким чином вага співпадає із більш звичною вагою Хеммінга.

Індексом розгалуження квадратної матриці розміру  $m \times m$  називається величина

$$BN(A) = \min_{x \neq 0} \{wt(x) + wt(Ax)\}.$$

Аналітичні оцінки стійкості SP-мереж до диференціального та лінійного криптоаналізу обчислюються через значення індексу розгалуження лінійних перетворень, які використовуються: чим більший індекс, тим стійкіший шифр.

Для невироджених матриць індекс розгалуження змінюється в діапазоні  $2 \leq BN(A) \leq m + 1$ . Матриця зветься *MDS-матрицею*, якщо її індекс розгалуження сягає максимального значення  $m + 1$ . Для MDS-матриць існує простий критерій [9].

**Твердження.** Матриця є MDS-матрицею тоді і тільки тоді, коли всі її квадратні підматриці є невиродженими.

Для отримання MDS-матриць над скінченними полями існує ряд таких конструкцій, як матриця Вандермонда або матриця Коші, але на кільця лишків ці структури з тих чи інших причин не переносяться [4]. Також для скінченних полів одержано ряд результатів щодо побудови MDS-матриць з додатковими властивостями (інволютивність, циркулянтність тощо), що дозволяє оптимізувати ресурси, необхідні для побудови криптосистеми, а також ряд результатів, які дозволяють з MDS-матриць отримувати MDS-матриці більшого розміру [6]. Для кілець лишків такі конструкції також не переносяться, тому проблема побудови матриць з високим індексом розгалуження та іншими криптографічними властивостями є актуальною.

$(0, 1)$ -матриці є популярною конструкцією для побудови блокових шифрів через дуже просту реалізацію з використанням елементів комп'ютерної низькорівневої архітектури (обчислення зводиться до деякої кількості побітових додавань координат вхідного вектору). Так, у шифрі E2 використовується  $(0, 1)$ -матриця розміру 8 на 8 з індексом розгалуження 5 [10], у шифрі ARIA – матриця

розміру 16 на 16 з індексом розгалуження 8 [2], у шифрі Midori – матриця розміру 4 на 4 з індексом розгалуження 3 [3]. Втім, доведено, що  $(0, 1)$ -матриці не можуть бути MDS; більш того, має місце така оцінка.

**Теорема 1 ([1]).** Для квадратної  $(0, 1)$ -матриці  $A$  розміру  $m \times m$  виконується нерівність

$$BN(A) \leq \frac{2m + 4}{3}.$$

З теореми 1 випливає, що при  $m=2, 3$  або 4 можуть існувати  $(0, 1)$ -матриці із майже максимальним значенням індексу розгалуження  $BN(A) = m$ ; при більших розмірах максимально можливе значення індексу розгалуження відносно зменшується.

Матриці над кільцями лишків використовуються через просту реалізацію, доступну на рівні інструкцій процесору, та різке ускладнення деяких криптоаналітичних атак (зокрема, лінійного криптоаналізу та його модифікацій). Наприклад, у сімействі шифрів SAFER використовуються матриці розміру 16 на 16 над кільцем лишків  $Z_{256}$  (тобто, над байтами) [5]. Для матриць над кільцями лишків не опубліковано оцінок для індексу розгалуження, але показано, що такі матриці не можуть бути MDS-матрицями [11].

### III. ОЦІНКИ ІНДЕКСУ РОЗГАЛУЖЕННЯ МАТРИЦЬ НАД КІЛЬЦЯМИ ЛИШКІВ

Між кільцями лишків  $Z_2^n$  та  $\{0, 1\}$  існує «природний» гомоморфізм  $\varphi_0(x) = x \bmod 2$ . В коректності цього гомоморфізму нескладно переконавшись стандартною перевіркою. Аналогічним чином можна визначити гомоморфізм над множинами матриць. Нехай  $M_m(Z_2^n)$  – множина квадратних матриць розміру  $m$  над кільцем лишків  $Z_2^n$ , тоді відображення  $\varphi: M_m(Z_2^n) \rightarrow M_m(\{0, 1\})$  таке, що  $\varphi(A) = A \bmod 2$ , де  $A \bmod 2$  – це матриця, отримана застосуванням гомоморфізму  $\varphi_0$  до кожного елементу матриці  $A$  (для вектору розміру  $m$  гомоморфізм  $\varphi$  визначається аналогічним чином, тому не будемо вводити додаткове позначення). Переконаємось у правильності цього факту. Нехай  $A, B$  – це матриці над  $Z_2^n$ , тоді елемент добутку цих двох матриць з індексом  $i$  та  $j$  буде знаходитись за формулою:

$$(AB)_{ij} = \sum_{k=1}^m A_{ik} B_{kj}$$

Тепер знайдемо образ цього елементу після застосування відображення  $\varphi_0$ :

$$\varphi_0((AB)_{ij}) = \varphi_0\left(\sum_{k=1}^m A_{ik} B_{kj}\right) = \sum_{k=1}^m \varphi_0(A_{ik}) \varphi_0(B_{kj})$$

Оскільки це співвідношення виконується для кожної пари індексів  $i$  та  $j$ , то для відображення  $\varphi$  воно теж виконується:

$$\varphi(AB) = \varphi(A)\varphi(B)$$

Аналогічним чином перевіряється, що, застосувавши відображення до суми матриць, отримаємо суму відображень відповідних матриць:

$$\varphi(A_{ij} + B_{ij}) = \varphi(A_{ij}) + \varphi(B_{ij})$$

Отже, запропоноване відображення матриць  $\varphi$  є гомоморфізмом.

Сформулюємо і доведемо теорему, яке пов'язує індекс розгалуження  $(0, I)$ -матриць з індексом розгалуження матриць над кільцем лишків.

**Теорема 2.** Для довільної матриці  $A$  над кільцем лишків  $\mathbb{Z}_2^n$  виконується рівність:

$$BN(A) = BN(\varphi(A))$$

де  $\varphi$  – описаний вище «природний» гомоморфізм.

**Доведення.** Покажемо спочатку, що  $BN(A) \geq BN(\varphi(A))$ .

Розглянемо деякий вектор  $x$  довжини  $m$  над  $\mathbb{Z}_2^n$  і будемо для нього досліджувати вираз виду  $wt(x) + wt(Ax)$ .

Очевидно, що  $wt(x) \geq wt(\varphi(x))$ . Дійсно, при застосуванні гомоморфізму до вектору  $x$  його вага не може збільшитись: всі непарні елементи вектору  $x$  стануть одиницями, а всі парні стануть нулями, тобто кількість нулів може збільшитись, але ніяк не може зменшитись.

Покажемо тепер, що  $wt(Ax) \geq wt(\varphi(Ax))$ . Нехай  $Ax=y$ , де  $y=(y_1, \dots, y_m)$  та  $y_i = \sum_{j=1}^m a_{ij}x_j$ , де  $i = \overline{1, m}$ . Після застосування гомоморфізму до вектору  $y$  отримуємо вектор  $\varphi(y) = \varphi(Ax)$ . Для того, щоб довести нерівність  $wt(y) \geq wt(\varphi(y))$ , необхідно показати, що  $y_i \geq \varphi_0(y_i)$ ,  $i = \overline{1, m}$ , тобто не може виникнути ситуації, коли  $y_i=0$ , а  $\varphi_0(y_i)=1$  для деякого  $i$ . Іншими словами, треба показати, що з  $y_i=0$  випливає  $\varphi_0(y_i)=0$ . Нехай  $y_i=0$ , тоді  $\sum_{j=1}^m a_{ij}x_j = 0 \pmod{2^n}$ , що, за властивостями конгруенцій, еквівалентно рівності  $\sum_{j=1}^m a_{ij}x_j = k2^n$ . Застосуємо до цього виразу гомоморфізм і отримуємо  $\varphi_0(\sum_{j=1}^m a_{ij}x_j) = \varphi_0(k2^n) = 0$ . Тому виконується  $wt(Ax) \geq wt(\varphi(Ax))$ .

Отже, було доведено, що для деякого вектора  $x$  виконується:  $wt(x) + wt(Ax) \geq wt(\varphi(x)) + wt(\varphi(Ax))$ . Тоді

$$\begin{aligned} wt(x) + wt(Ax) &\geq wt(\varphi(x)) + wt(\varphi(Ax)) \geq \\ &\geq \min_{y \neq 0} \{ wt(\varphi(y)) + wt(\varphi(Ay)) \} \geq BN(\varphi(A)) \end{aligned}$$

Оскільки в цій нерівності  $x$  – довільний вектор над  $\mathbb{Z}_2^n$ , то й для вектору, на якому досягається мінімальне значення ліворуч, дана нерівність буде справедливою. Таким чином,  $BN(A) \geq BN(\varphi(A))$ .

Покажемо тепер, що  $BN(A) \leq BN(\varphi(A))$ . Нехай матриця  $B$  є елементом  $M_m(\{0, 1\})$ , а  $z$  – деякий вектор над  $\{0, 1\}$

довжини  $m$ . Розглянемо повний прообраз цієї матриці відносно гомоморфізму  $\varphi$ , тобто множину

$$\varphi^{-1}(B) = \{ C \in M_m(\mathbb{Z}_2^n) : \varphi(C) = B \}$$

Очевидно, що ця множина є не пустою, оскільки  $\varphi$  – сюр'єктивне відображення. Виберемо з цієї множини довільну матрицю  $A$ . Довільному двійковому вектору  $z=(z_1, \dots, z_m)$  поставимо у відповідність вектор  $x=(x_1, \dots, x_m)$  над  $\mathbb{Z}_2^n$  за таким правилом:

$$x_i = \begin{cases} 2^{n-l}, & \text{якщо } z_i = 1 \\ 0, & \text{якщо } z_i = 0 \end{cases}$$

Очевидно, що  $\varphi(x)=z$  та  $wt(x)=wt(z)=wt(\varphi(x))$ . Нескладно також показати, що в силу гомоморфізму виконується рівність  $\varphi(A) \cdot z = \varphi(A)\varphi(x) = \varphi(Ax)$ .

Покажемо, що  $wt(Ax) \leq wt(\varphi(Ax))$ . Ця нерівність буде виконуватись лише тоді, коли кількість ненульових елементів у векторі  $Ax=y$  менша, ніж у векторі  $\varphi(Ax)=\varphi(y)$ , тобто коли неможлива така ситуація:  $y_i \neq 0$ , але  $\varphi_0(y_i)=0$ . Таким чином, потрібно довести, що з твердження  $\varphi_0(y_i)=0$  випливає  $y_i=0$ . Зрозуміло, що  $\varphi_0(y_i)=0$  еквівалентно

рівності  $\sum_{j=1}^m \varphi_0(a_{ij})\varphi_0(x_j) = 0 \pmod{2}$ . Ця сума складається з доданків або  $\varphi_0(a_{ij})\varphi_0(x_j)=1$ , або  $\varphi_0(a_{ij})\varphi_0(x_j)=0$ . Очевидно, що кількість доданків, які дорівнюють одиниці, парна, інакше би значення суми за модулем 2 не дорівнювало б нулю. Але ситуація, коли  $\varphi_0(a_{ij})\varphi_0(x_j)=0$ , розпадається ще на три випадки в залежності від значень координат вектору  $x$ .

Розглянемо всі випадки детальніше.

1. Якщо  $\varphi_0(a_{ij})$  – довільне та  $\varphi_0(x_j)=0$ , то в силу побудованого гомоморфізму  $\varphi$  і конструкції вектору  $x$  маємо, що  $x_j=0$ . Тоді  $a_{ij}x_j = a_{ij} \cdot 0 = 0 \pmod{2^n}$ , і нульовий доданок в суму  $\sum_{j=1}^m a_{ij}x_j$  нічого не вносить.

2. Якщо  $\varphi_0(a_{ij})=0$  та  $\varphi_0(x_j)=1$ , то  $a_{ij}=2k \pmod{2^n}$  і  $x_j=2^{n-l}$ . Тоді  $a_{ij}x_j = (2k) \cdot 2^{n-l} = 2^n \cdot k = 0 \pmod{2^n}$ , і нульовий доданок в суму  $\sum_{j=1}^m a_{ij}x_j$  нічого не вносить.

3. Якщо  $\varphi_0(a_{ij})=1$  та  $\varphi_0(x_j)=1$ , то  $a_{ij}=(2k+1) \pmod{2^n}$  і  $x_j=2^{n-l}$ . Тоді  $\sum_{j=1}^m a_{ij}x_j = 2^{n-l} \sum_{j=1}^m a_{ij}$ ; але сума парної кількості

непарних чисел є парним числом, тому  $\sum_{j=1}^m a_{ij} = 2l$  та

$$\sum_{j=1}^m a_{ij}x_j = 2^{n-l} \sum_{j=1}^m a_{ij} = 2^{n-l} \cdot 2l = 2^n l = 0 \pmod{2^n}$$

Отже,  $\sum_{j=1}^m a_{ij}x_j = 0 \pmod{2^n}$ , а тому з рівності  $\varphi_0(y_i)=0$  випливає  $y_i=0$ . Таким чином,  $wt(Ax) \leq wt(\varphi(Ax))$ .

Отже,  $wt(x)+wt(Ax) \leq wt(\varphi(x))+wt(\varphi(Ax))$  і використовуючи міркування, аналогічні попередньому випадку, отримуємо, що  $BN(A) \leq BN(\varphi(A))$ .

З обох доведених нерівностей одержуємо рівність  $BN(A)=BN(\varphi(A))$ , яку й треба було довести.

З теореми 2 та відомих результатів для  $(0,1)$ -матриць впливають такі наслідки.

**Наслідок 1.** Над кільцем лишків  $Z_2^n$  не існує MDS-матриць.

**Наслідок 2.** Для довільної матриці  $A$  розміру  $m \times m$  над  $Z_2^n$  виконується наступна нерівність:

$$BN(A) \leq \frac{2m+4}{3}$$

#### IV. ЗАСТОСУВАННЯ ТЕОРЕМИ ПРО ЗБЕРЕЖЕННЯ ІНДЕКСУ РОЗГАЛУЖЕННЯ ДЛЯ ПОБУДОВИ МАТРИЦЬ НАД КІЛЬЦЯМИ ЛИШКІВ

Одним із застосувань доведеної теореми про гомоморфізм є побудова матриць над кільцями лишків на основі  $(0,1)$ -матриць. Мотивація такої побудови полягає в тому, що диференціальний та лінійний криптоаналіз блокових шифрів суттєво ускладнюються із переходом на кільце лишків, де операції виконуються за модулем  $2^n$ , через складний характер впливу різних алгебраїчних операцій на різниці та лінійні відносно побітового додавання апроксимації.

Наприклад, у шифрі ARIA, як було зазначено, використовується  $(0,1)$ -матриця розміру  $16$  на  $16$  з індексом розгалуження  $8$  [2]. Із доведення теореми 2 випливає, що можна замінити цю матрицю на її довільний прообраз відносно гомоморфізму  $\varphi$  і перейти в обчислення над кільцями лишків. При такій досить «природній» заміні індекс розгалуження матриці зберігається, але загалом підвищується криптостійкість. Вибір елементів прообразу може диктуватись іншими міркуваннями; скажімо, коефіцієнти матриці не повинні бути великими (наприклад,  $1, 2, 3$  та  $4$ ) для збереження ефективності обчислення, але не повинні співпадати для запобігання інтегральному криптоаналізу.

У специфікації шифру Midori розглядається в якості лінійного перетворення три матриці на вибір, дві з яких задовільняють властивості інволютивності [3]. Також дві з них – це матриці над  $Z_2^n$ , а третя –  $(0,1)$ -матриця, яка одержана з однієї з попередніх застосуванням описаного гомоморфізму. Відповідно, ці матриці мають однаковий індекс розгалуження, що дозволяє будувати оцінки стійкості до відомих методів криптоаналізу уніфікованим чином. Втім, розробники віддали перевагу  $(0,1)$ -матриці через властивості інволютивності та орієнтацію на реалізації у малопотужних архітектурах.

Два наведених приклада демонструють, що можна запропонувати шлях модифікації шифру, а саме його лінійного перетворення, для підвищення криптографічної стійкості. Для цього достатньо замінити  $(0,1)$ -матриці, які

використовуються, на певні матриці-прообрази над кільцями лишків. При такій заміні індекс розгалуження зберігається, тому шифр зазвичай не втрачає свою стійкість до диференціального та лінійного криптоаналізу, а ретельний підбір відповідної матриці може підвищити стійкість до алгебраїчних атак. Зауважимо, що через перехід до інших алгебраїчних операцій все одно слід проводити оцінювання стійкості модифікованого шифру; однак форма та порядок оцінок в багатьох випадках зберігаються.

#### ВИСНОВКИ

У даній роботі було доведено, що індекси розгалуження матриць над кільцями лишків за модулем  $2^n$  зберігаються при гомоморфному відображенні у  $(0,1)$ -матриці над двійковими лінійними просторами. Це дало змогу застосувати для оцінки значень індексу розгалуження матриць над кільцями лишків результати, відомі для  $(0,1)$ -матриць. Грунтуючись на одержаних результатах, було запропоновано деякі шляхи пошуку криптографічно сильних матриць над кільцями лишків та підсилення криптографічної стійкості таких шифрів, як ARIA та Midori, шляхом заміни їх лінійних перетворень на перетворення над кільцями лишків.

#### ЛІТЕРАТУРА REFERENCES

- [1] J. Chloy, K. Khoo, “New Applications of Differential Bounds of the SDS Structure” [Online]. Available: <https://eprint.iacr.org/2008/395.pdf>
- [2] D. Kwon, J. Kim, S. Park and others, “New Block Cipher: ARIA” [Online]. Available: <http://www.math.snu.ac.kr/~jinhong/04Aria.pdf>
- [3] S. Banik, A. Bogdanov, T. Isobe and others, “Midori: A Block Cipher for Low Energy” [Online]. Available: <https://eprint.iacr.org/2015/1142.pdf>
- [4] Дідан В.В., Методи побудови MDS-матриць над скінченними полями та кільцями // Матеріали XIV Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (26-28 травня 2016 р., Київ). – К.: Видавництво «Політехніка», 2016. – стор. 89-90.
- [5] J. Massey, “On the Optimality of SAFER+ Diffusion” [Online]. Available: [http://mpcs.sci.am/filesimages/volumes/volume\\_44/14.pdf](http://mpcs.sci.am/filesimages/volumes/volume_44/14.pdf)
- [6] T. Kranz, G. Leander, K. Stoffelen, F. Wiemer, “Shorter Linear Straight-Line Programs for MDS Matrices” [Online]. Available: <https://eprint.iacr.org/2017/1151.pdf>
- [7] J. Daemen, V. Rijmen, “The Wide Trail Design Strategy” [Online]. Available: [http://jda.noekeon.org/JDA\\_VRI\\_Wide\\_2001.pdf](http://jda.noekeon.org/JDA_VRI_Wide_2001.pdf)
- [8] J. Daemen and V. Rijmen, “The Rijndael Block Cipher,” AES Proposal, 1998.
- [9] Ju-Sung Kang et al, “Practical and Provable Security against Differential and Linear Cryptanalysis for Substitution-Permutation Networks”, ETRI Journal, Vol.23, No.4, Dec. 2001.
- [10] M. Kanda et al. “A New 128-bit Block Cipher E2” Technical Report of IEICE. ISEC98-12
- [11] С.В. Яковлев, В.В. Дідан, «Про неіснування матриць максимального індексу розгалуження над кільцем лишків за модулем» // Міжнародна науково-практична конференція «Інформаційні технології та комп'ютерне моделювання 2016» (23-28 травня 2016 р., Івано-Франківськ – Яремче). – Івано-Франківськ: Супрун В.П., 2016. – стор. 116-117.