DOI: 10.18372/2410-7840.22.14661
УДК 004.056.55:512.643

ВЕРХНІ ОЦІНКИ ЗНАЧЕНЬ ІНДЕКСУ РОЗГАЛУЖЕННЯ МАТРИЦЬ НАД КІЛЬЦЯМИ ЛИШКІВ ЗА МОДУЛЕМ СТЕПЕНЯ ДВІЙКИ

Олег Курінний, Сергій Яковлєв

Індекс розгалуження – один з найважливіших криптографічних параметрів лінійних перетворень у блокових шифрах, який суттєво впливає на стійкість до диференціального та лінійного криптоаналізу. Добре відомі методи побудови у матричній формі лінійних перетворень над скінченними полями, які мають максимально можливе значення індексу розгалуження (MDS-матриці). У той же час важливе криптографічне значення мають операції у кільці лишків за модулем степеня двійки, оскільки вони ефективно реалізуються у сучасних обчислювальних архітектурах і при цьому підвищують стійкість криптоперетворень до алгебраїчних атак. Відомі методи побудови MDS-матриць незастосовні для кілець лишків за непростим модулем. У даній роботі доведено, що матриця над будь-яким кільцем лишків за парним модулем не може мати максимальний індекс розгалуження. Також доведено, що індекс розгалуження матриць над кільцем лишків за модулем степеня двійки є інваріантом при зведенні матриці за модулем 2, а тому для даного класу матриць будуть справедливі усі відомі аналітичні результати, одержані для класу двійкових матриць – зокрема, верхні обмеження на індекс розгалуження. Сформульовано умови для двійкових матриць, необхідні для високого значення індексу розгалуження. Одержані результати дозволяють будувати блокові шифри із потенційно підвищеною стійкістю до алгебраїчних та інтегральних атак, зберігаючи при цьому обґрунтовану стійкість до диференціального та лінійного криптоаналізу.

Ключові слова: *індекс розгалуження, кільце лишків, двійкові матриці, диференціальний криптоаналіз, лінійний криптоаналіз.*

1. Вступ

Стратегія широкого шляху, запропонована Йоном Деменом у 1998 році [6], постулює, що стійкість симетричних шифрів до відомих методів криптоаналізу визначається не тільки якістю нелінійних перетворень (S-блоків), а й властивостями лінійних перемішуючих перетворень шифрів. Основним параметром криптографічної якості лінійного перетворення є так званий *індекс розгалуження*. У рамках запропонованої стратегії для побудови шифрів SQUARE та Rijndael (пізніше стандартизованого як AES) використовувались спеціальні конструкції, запозичені з теорії лінійних кодів – *MDS-матриці* над скінченними полями, які мають максимально можливий індекс розгалуження для матриць заданого розміру. Саме завдяки цій властивості вдалось довести як практичну [5], так і теоретичну [8, 11] 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 та/або ефективності реалізації. У даній роботі розглядаються матричні перетворення над кільцями лишків за модулем 2^n. Подібні структури зазвичай забезпечують високу швидкість при реалізації за рахунок наявності модульного додавання серед стандартних інструкцій процесорів; в той же час алгебраїчні властивості додавання забезпечують 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; також сформульовано декілька необхідних умов на матриці із високим значенням індексу розгалуження. Як наслідок, запропоновано простий спосіб підвищення стійкості SP-мереж типу ARIA або Midori до криптоаналітичних атак за рахунок переходу на інші алгебраїчні операції у лінійних перетвореннях.

2. Необхідні теоретичні відомості

Підстановочно-перестановочна мережа, або просто SP-мережа, – це ітеративна схема блокового шифрування, раунди якої складаються із послідовних замішування з ключем, нелінійного перетворення, зазвичай реалізованого у вигляді серії паралельних S-блоків невеликого розміру, та лінійного перетворення, яке перемішує виходи з S-блоків між собою. Більшість існуючих блокових шифрів зі структурою SP-мережі реалізує лінійного перетворення у матричному вигляді. Як правило, матриці розглядаються над однією з трьох таких алгебраїчних структур:

1) скінченне поле $GF(2^n)$ із відповідними операціями додавання та множення над двійковими векторами як елементами поля;

2) кільце лишків Z_{2^n} із операціями додавання та множення над двійковими векторами як зображеннями чисел за модулем 2^n у двійковій системі числення;

3) лінійний векторний простір $V_n = \{0,1\}^n$ із операцією побітового додавання двійкових векторів та множенням на скаляри 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, наприклад, для алгоритмів легкої криптографії, призначених для реалізації у малопотужних пристроях.

Для деякого вектору x довжини m над заданим кільцем *вага вектору* $wt(x)$ дорівнює кількості ненульових координат у векторі. Для двійкових векторів введена таким чином вага співпадає із більш звичною вагою Хемінга (кількістю одиниць у векторі). Через $nz(x)$ позначимо кількість нульових координат вектору x; таким чином, $\mathrm{wt(x)} + \mathrm{nz(x)} = \mathrm{m}$. Зауважимо, що усі вектори далі розглядаються як вектори-стовпчики у операціях множення матриці на вектор.

Індекс розгалуження (англ. *branch number*) квадратної матриці A розміру $m \times m$ – це величина

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

Іншими словами, індекс розгалуження дорівнює мінімально можливій кількості ненульових координат на вході та на виході лінійного перетворення $f(x) = A \cdot x$ для усіх ненульових входів.

Аналітичні оцінки стійкості SP-мереж до диференціального та лінійного криптоаналізу обчислюються через відповідні параметри S-блоків та значення індексу розгалуження лінійних перетворень [8, 11]; в цілому чим більший індекс, тим стійкіший шифр до обох зазначених методів аналізу.

Неважко показати, що для невироджених матриць індекс розгалуження змінюється в діапазоні $2 \le BN(A) \le m+1$. Матриця зветься *MDS-матрицею*, якщо її індекс розгалуження сягає максимального значення $m+1$. Для MDS-матриць існує простий критерій [8]: матриця є MDS-матрицею тоді і тільки тоді, коли всі її квадратні підматриці є невиродженими.

Для побудови MDS-матриць над скінченними полями існує ряд конструкцій, таких як матриці лінійних кодів, матриця Вандермонда або матриця Коші, але на кільця лишків ці структури з тих чи інших причин не переносяться [1]. Також для скінченних полів одержано ряд результатів щодо побудови MDS-матриць з додатковими властивостями (інволютивність, циркулянтність тощо), а також побудови MDS-матриць з матриць меншого розміру, що дозволяє оптимізувати ресурси, необхідні для реалізації криптосистеми [9]. Для кілець лишків такі конструкції також не переносяться, тому проблема побудови матриць з високим індексом розгалуження та іншими бажаними 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 добутку такої матриці на вектор зводиться до деякої кількості побітових додавань координат даного вектору). Так, у японських шифрах Camellia [2] та E2 [7] використовуються $(0,1)$-матриці розміру 8×8 з індексом розгалуження 5, у корейському шифрі ARIA [10] – матриця розміру 16×16 з індексом розгалуження 8, у нещодавно запропонованому легкому шифрі Midori [3] – матриця розміру 4×4 з індексом розгалуження 3. Втім, доведено, що $(0,1)$-матриці не можуть бути MDS; більш того, має місце така оцінка [4]: для квадратної $(0,1)$-матриці A розміру $m \times m$ виконується нерівність

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

З даного результату випливає, що при m = 2, 3 або 4 можуть існувати $(0,1)$-матриці із майже максимальним значенням індексу розгалуження $\mathrm{BN(A)} = \mathrm{m}$; при більших розмірах максимально можливе значення індексу розгалуження пропорційно 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 спеціально сконструйовані матриці розміру 16×16 над кільцем лишків Z_{256} (тобто, над байтами) із індексом розгалуження 5 [12]. Однак для матриць загального виду над кільцями лишків не опубліковано аналітичних оцінок для індексу розгалуження.

3. Основні результати

Нехай R – деяке кільце, $M_m(R)$ – кільце матриць розміру $m \times m$ над R. У якості кільця R будемо розглядати кільце лишків за парним модулем. У першу чергу розглянемо кільце лишків за довільним парним модулем.

Твердження. Над кільцем Z_{2n}, $n \in N$, не існує MDS-матриць.

Доведення. Якщо $A \in M_m(Z_{2n})$ є MDS-матрицею, то усі її квадратні підматриці повинні бути невироджені (тобто, їх визначник повинен належати Z_{2n}^* і, відповідно, бути непарним лишком). Зокрема, це стосується і підматриць розміру 1×1, тобто кожного елементу матриці. Таким чином, кожен елемент матриці A повинен бути непарним лишком.

Розглянемо ліву верхню 2×2-підматрицю матриці A: $\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$. Визначник цієї матриці дорівнює $a_{11}a_{22} - a_{12}a_{21}$ (усі операції за модулем $2n$) і є парним лишком. Таким чином, дана квадратна підматриця є виродженою, а тому A не є MDS-матрицею. Доведення завершене.

Оскільки над кільцями лишків за парним модулем не існує MDS-матриць, виникає питання про максимально можливе досяжне значення індексу розгалуження. Відповідь на це питання вдалось знайти для випадку, коли модуль є степенем двійки; цей випадок становить найбільший інтерес для криптографічних застосувань.

Між кільцями лишків Z_{2^n} та Z_2 існує «природний» гомоморфізм $\varphi_0(x) = x \bmod 2$; в коректності цього гомоморфізму нескладно переконатись стандартною перевіркою. Цей гомоморфізм можна узагальнити й на кільце матриць над Z_{2^n}: гомоморфізмом кілець є відображення

$$\varphi : M_m(Z_{2^n}) \to M_m(Z_2),$$
$$\varphi : A \mapsto A \bmod 2,$$

де $A \bmod 2$ – матриця, отримана застосуванням гомоморфізму φ_0 до кожного елементу матриці A. Дійсно, нехай $A, B \in M_m(Z_{2^n})$, $A = \|a_{ij}\|$, $B = \|b_{ij}\|$ – довільні матриці, а їх добуток $C = A \cdot B = \|c_{ij}\|$. Тоді $c_{ij} = \sum_{k=1}^{m} a_{ik} b_{kj}$ та, відповідно,

$$\varphi_0(c_{ij}) = \varphi_0\left(\sum_{k=1}^{m} a_{ik} b_{kj}\right) = \sum_{k=1}^{m} \varphi_0(a_{ik})\varphi_0(b_{kj}).$$

Оскільки це співвідношення виконується для кожної пари індексів (i, j), то маємо $\varphi(AB) = \varphi(A)\varphi(B)$. Аналогічно перевіряється, що $\phi(\mathrm{A} + \mathrm{B}) = \phi(\mathrm{A}) + \phi(\mathrm{B})$. Отже, описане відображення φ є гомоморфізмом.

Для вектору $x = (x_1, x_2, ..., x_m)^T \in (Z_{2^n})^m$ будемо за аналогією позначати $\phi(\mathrm{x}) = (\phi_0(\mathrm{x}_1), ..., \phi_0(\mathrm{x}_m))^{\mathrm{T}}$. Неважко переконатись, що для довільних векторів $\varphi(x + y) = \varphi(x) + \varphi(y)$.

Основний результат про індекси розгалуження матриць над кільцем лишків Z_{2^n} сформулюємо у вигляді такої теореми.

Теорема. Для введеного вище гомоморфізму кілець матриць φ та довільної матриці $A \in M_m(Z_{2^n})$ виконується рівність $BN(A) = BN(\varphi(A))$.

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

Для довільного вектору $x \in (Z_{2^n})^m$ виконується нерівність $wt(x) \geq wt(\varphi(x))$. Дійсно, при застосуванні до вектору x відображення φ вага вектору не може збільшитись: всі непарні координати вектору x стануть одиницями, а всі парні стануть нулями, тобто кількість нулів може лише зрости. Ті ж міркування справедливі й для вектору $y = Ax$. Таким чином,

$$\mathrm{wt(x)} + \mathrm{wt(Ax)} \geq \mathrm{wt}(\phi(\mathrm{x})) + \mathrm{wt}(\phi(\mathrm{Ax})) \geq$$
$$\geq \min_{\mathrm{z} \neq 0} \{\mathrm{wt}(\phi(\mathrm{z})) + \mathrm{wt}(\phi(\mathrm{Az})) \geq \mathrm{BN}(\phi(\mathrm{A})).$$

Оскільки в цій нерівності x – довільний вектор над Z_{2^n}, то й для вектору, на якому досягається мінімальне значення виразу ліворуч (яке дорівнює $BN(A)$), дана нерівність буде справедливою. Таким чином, $BN(A) \geq BN(\varphi(A))$.

Доведемо тепер, що $BN(A) \leq BN(\varphi(A))$.

Довільному ненульовому двійковому вектору-стовпчику $z = (z_1, z_2, ..., z_m)^T \in (Z_2)^m$ поставимо у відповідність вектор-стовпчик $\mathrm{x} = (\mathrm{x}_1, \mathrm{x}_2, ..., \mathrm{x}_m)^{\mathrm{T}} \in (\mathrm{Z}_{2^n})^{\mathrm{m}}$ за таким правилом:

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

Нескладно показати, що вектор x також ненульовий і виконуються співвідношення $\varphi(x) = z$, $wt(x) = wt(z)$ та $\phi(\mathrm{A}) \cdot \mathrm{z} = \phi(\mathrm{A}) \cdot \phi(\mathrm{x}) = \phi(\mathrm{Ax})$.

Покажемо, що $wt(Ax) = wt(\varphi(Ax))$. Для цього необхідно показати, що кількість ненульових координат у векторі $y = Ax$ дорівнює кількості ненульових координат у векторі $\varphi(y) = \varphi(Ax)$. Оскільки для $y_i \neq 0$ завжди $\varphi_0(y_i) \neq 0$ і навпаки, а для $y_i = 0$ завжди $\varphi_0(y_i) = 0$, фактично необхідно показати, що з $\varphi_0(y_i) = 0$ випливає $y_i = 0$. Зрозуміло, що рівність $\varphi_0(y_i) = 0$ еквівалентна рівності $\sum_{j=1}^{m} \varphi_0(a_{ij})\varphi_0(x_j) \equiv 0 \pmod 2$. Кожен доданок цієї суми дорівнює 0 або 1, причому кількість доданків, які дорівнюють 1, парна. Розглянемо усі випадки, коли $\varphi_0(a_{ij})\varphi_0(x_j) = 0$.

1) Якщо $\varphi_0(a_{ij})$ довільне, а $\varphi_0(x_j) = 0$, то $x_j = 0$ та, відповідно, $a_{ij}x_j = 0$.

2) Якщо $\varphi_0(a_{ij}) = 0$ та $\varphi_0(x_j) = 1$, то $a_{ij} \equiv 2k \pmod{2^n}$, $x_j = 2^{n-1}$ та, відповідно, $a_{ij}x_j \equiv 2k \cdot 2^{n-1} \equiv 0 \pmod{2^n}$.

Таким чином, у сумі $y_i = \sum_{j=1}^{m} a_{ij}x_j$ ненульові доданки відповідають тим значенням *j*, для яких $\varphi_0(a_{ij})\varphi_0(x_j) = 1$. Але тоді усі відповідні a_{ij} є непарними лишками, $x_j = 2^{n-1}$ і кількість таких доданків парна. Тому $\sum_{j=1}^{m} a_{ij}x_j = 2^{n-1}\sum_{j=1}^{m} a_{ij} \equiv 0 \pmod{2^n}$, оскільки сума парної кількості непарних чисел є парним числом.

Таким чином, з $\varphi_0(y_i) = 0$ випливає $y_i = 0$, а тому $wt(Ax) = wt(\varphi(Ax))$. Отже,

$$BN(A) \le wt(x) + wt(Ax) = wt(z) + wt(\varphi(A)z),$$

причому ця нерівність виконується для довільного вектору z, включно з тим, на якому досягається мінімум виразу праворуч, який дорівнює $BN(\varphi(A))$.

Отже, $BN(A) \le BN(\varphi(A))$ та одночасно $BN(A) \ge BN(\varphi(A))$, а отже, індекси розгалуження матриць A та $\varphi(A)$ співпадають. Доведення теореми завершено.

Наслідок. Для довільної матриці $A \in M_m(Z_{2^n})$ виконується нерівність:

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

Нерівність випливає з наведеної у попередньому розділі оцінки індексу розгалуження для квадратних $(0,1)$-матриць.

Питання побудови матриць над кільцем Z_{2^n} із високим індексом розгалуження залишається відкритим. Наразі невідомо аналітичних конструкцій матриць, які б гарантували значення індексу розгалуження; відповідно, побудова таких матриць зводиться до певної задачі комбінаторної оптимізації. Доведена теорема показує, що пошук можна починати з побудови $(0,1)$-матриці із високим індексом розгалуження, а потім вибору необхідної матриці над Z_{2^n} з множини прообразів знайденої матриці відносно відображення φ. Сформулюємо умови на стовпчики $(0,1)$-матриці, необхідні для досягання високого значення індексу розгалуження.

Лема 1. Якщо деякий стовпчик матриці $A \in M_m(Z_2)$ має вагу не більш ніж $\frac{m}{2}$, то $BN(A) \le \frac{m}{2} + 1$.

Дійсно, якщо *i*-тий стовпчик A має вагу $\le \frac{m}{2}$, то для вектору e_i, в якому тільки *i*-та координата дорівнює 1, маємо $wt(e_i) + wt(Ae_i) \le 1 + \frac{m}{2}$. Відповідно, індекс розгалуження не може перевищувати дану величину.

Лема 2. Якщо у матриці $A \in M_m(Z_2)$ щонайменше два стовпчики мають вагу не меншу за $\frac{3m}{4}$, то $BN(A) \le \frac{m}{2} + 2$.

Дійсно, позначимо ці стовпчики як вектори a_i та a_j, і нехай $x = e_i \oplus e_j$. Тоді

$$wt(x) + wt(Ax) = 2 + wt(A(e_i \oplus e_j)) \le$$
$$\le 2 + nz(Ae_i) + nz(Ae_j) \le 2 + \tfrac{m}{4} + \tfrac{m}{4} = 2 + \tfrac{m}{2}.$$

Таким чином, для побудови квадратної $(0,1)$-матриці із високим індексом розгалуження необхідно обирати її стовпчики серед векторів, вага яких не менша за половину довжини, але не більше одного такого стовпчика повинно мати вагу, більшу за три чверті довжини.

4. Можливі застосування одержаних результатів

Одним із застосувань доведеної теореми про індекс розгалуження 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 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 16×16 з індексом розгалуження 8 [10]. Із теореми випливає, що можна замінити цю матрицю на її довільний прообраз відносно гомоморфізму φ і перейти в обчислення у кільці лишків за модулем 2^n. При такій досить «природній» заміні індекс розгалуження матриці зберігається, але загалом підвищується криптостійкість. Вибір елементів прообразу може диктуватись додатковими міркуваннями; скажімо, коефіцієнти матриці не повинні бути великими (наприклад, 1, 2, 3 та 4) для збереження ефективності обчислення, але не повинні співпадати між собою для ускладнення інтегрального криптоаналізу.

У специфікації шифру Midori розглядається в якості лінійного перетворення три матриці на вибір, дві з яких задовольняють властивості інволютивності [3]; дві з цих матриць – це матриці над Z_{2^n}, а третя – $(0,1)$-матриця, яка одержана з однієї з попередніх фактично застосуванням гомоморфізму φ. 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 існують шляхи модифікації шифрів (зокрема, 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 не повинен втратити свою стійкість до диференціального та лінійного криптоаналізу, а ретельний підбір відповідної матриці може підвищити стійкість до алгебраїчних та інтегральних атак. Втім зауважимо, що через перехід до інших алгебраїчних операцій все одно слід проводити повне оцінювання стійкості модифікованого шифру; однак форма та порядок відомих аналітичних оцінок до криптографічних атак в багатьох випадках зберігаються.

5. Висновки

У даній роботі розглянуто матриці над кільцями лишків за модулем степеня двійки. Основним результатом є доведення факту, що індекс розгалуження таких матриць зберігається при заміні усіх парних лишків на 0, а непарних на 1. Це дозволяє застосовувати для даного класу матриці відомі оцінки на індекс розгалуження для двійкових матриць та, зокрема, будувати матриці над кільцем лишків із високим індексом розгалуження через проміжний пошук «гарних» двійкових матриць. Також сформульовано декілька необхідних умов на двійкові матриці із високим індексом розгалуження, які спрощують задачу перебору при побудові таких матриць. Наприкінці обговорюється, яким чином одержані результати можуть бути використані для підсилення криптографічної стійкості блокових шифрів від алгебраїчних та інтегральних атак при потенційному збереженні стійкості до диференціального та лінійного криптоаналізу.

ЛІТЕРАТУРА

[1]. В. Дідан, "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», С. 89-90, 2016.

[2]. K. Aoki, T. Ichikawa, M. Kanda et al. "Camellia: a 128-Bit block cipher suitable for multiple platforms – design and analysis", *SAC 2000*, *LNCS*, vol. 2012, pp. 39-56, 2001.

[3]. S. Banik, A. Bogdanov, T. Isobe et al., "Midori: A Block Cipher for Low Energy", *Cryptology ePrint Archive*, Report 2015/1142. https://eprint.iacr.org/2015/1142.pdf.

[4]. J. Choy, K. Khoo, "New Applications of Differential Bounds of the SDS Structure", *Cryptology ePrint Archive*, Report 2008/395. https://eprint.iacr.org/2008/395.pdf.

[5]. J. Daemen, V. Rijmen, "The Rijndael Block Cipher", *AES Proposal*, 1998.

[6]. J. Daemen, V. Rijmen, "The Wide Trail Design Strategy", *Cryptography and Coding,* pp. 222-238, 2001. http://jda.noekeon.org/JDA_VRI_Wide_2001.pdf.

[7]. M. Kanda et al., "A New 128-bit Block Cipher E2", *Technical Report of IEICE*. ISEC98-12.

[8]. J. Kang et al, "Practical and Provable Security against Differential and Linear Cryptanalysis for Substitution-Permutation Networks", *ETRI Journal*, Vol. 23, No. 4, Dec, 2001.

[9]. T. Kranz, G. Leander, K. Stoffelen, F. Wiemer, "Shorter Linear Straight-Line Programs for MDS Matrices", *Cryptology ePrint Archive*, Report 2017/1151. https://eprint.iacr.org/2017/1151.pdf.

[10]. D. Kwon, J. Kim, S. Park et al., "New Block Cipher: ARIA", *ICISC 2003: Information Security and Cryptology - ICISC 2003*, pp. 432-445. http://www.math.snu.ac.kr/~jinhong/04Aria.pdf.

[11]. S. Park, S. Sung, S. Chee et al., "On the security of Rijndael-like structures against differential and linear cryptanalysis", *Advances in Cryptology – ASIACRYPT,* LNCS, vol. 2501, pp. 176-191, *2002*.

[12]. G. Piret, J. Quisquater, "Integral Cryptanalysis on reduced-round Safer++", *Cryptology ePrint Archive*, Report 2003/033. https://eprint.iacr.org/2003/033.pdf.

ВЕРХНИЕ ОЦЕНКИ ЗНАЧЕНИЙ ИНДЕКСА ВЕТВЛЕНИЯ МАТРИЦ НАД КОЛЬЦАМИ ВЫЧЕТОВ ПО МОДУЛЮ СТЕПЕНИ ДВОЙКИ

Индекс ветвления – один из важнейших криптографических параметров линейных преобразований в блочных шифрах, который существенно влияет на стойкость к дифференциальному и линейному криптоанализу. Хорошо известны методы построения в матричной форме линейных преобразований над конечными полями, которые имеют максимально возможное значение индекса ветвления (MDS-матрицы). В то же время важное криптографическое значение имеют операции в кольцах вычетов по модулю степени двойки, поскольку они эффективно реализуются в современных вычислительных архитектурах и при этом повышают стойкость криптопреобразований к алгебраическим атакам. Известные методы построения MDS-матриц неприменимы для колец вычетов по непростому модулю. В данной работе доказано, что матрица над любым кольцом вычетов по чётному модулю не может иметь максимальный индекс ветвления. Также доказано, что индекс ветвления матрицы над кольцом вычетов по модулю степени двойки инвариантен при сведении матрицы по модулю 2, поэтому для данного класса матриц будут справедливы все известные аналитические результаты, полученные для класса двоичных матриц – в частности, верхние ограничения на индекс ветвления. Сформулированы условия для двоичных матриц, необходимые для высокого значения индекса ветвления. Полученные результаты позволяют строить блочные шифры с потенциально повышенной стойкостью к алгебраическим и интегральным атакам, сохраняя при этом обоснованную стойкость к дифференциальному и линейному криптоанализу.

Ключевые слова: индекс ветвления, кольцо вычетов, двоичные матрицы, дифференциальный криптоанализ, линейный криптоанализ.

UPPER BOUNDS FOR A BRANCH NUMBER OF MATRICES OVER A RING OF INTEGERS MODULO POWER OF TWO

Branch number is a very important cryptographic parameter of linear mappings used in block ciphers. It significantly affects security against differential and linear cryptanalysis due to "wide trail strategy" of block cipher design. Many techniques are well known to generate linear mappings with maximal possible branch number in matrix form over finite fields (so-called MDS-matrices). In the same time operations over integers modulo power of two are important for cryptographic purposes. They are very efficient in modern computing architectures and increase security of cryptographic functions against algebraic attacks. But known techniques of MDS-matrix generating are not applicable to a ring of integers modulo composite number. In this work we proved that any square matrix over a ring of integers modulo even number cannot have a maximal branch number. We proved that the branch number of any square matrix over a ring of integers modulo power of two is invariant under reduction modulo 2. Thus, any analytic result known for binary matrices is valid for matrices modulo power of two, including upper bounds for the branch number. Consequently, the branch number of this type of matrix cannot exceed about two thirds of a matrix size. Also we formulated some requirements for binary matrices to obtain high value of the branch number; we show that such matrices cannot have both sparse (low weight) and dense (high weight) columns. At the end we shortly consider how the security of binary ciphers (e.g. ARIA or Midori) against linear and integral cryptanalysis can be increased by replacing binary matrix with matrix over a ring of integers modulo power of two in linear layer. The results of this work allow to create block ciphers with potentially improved security against algebraic and integral attacks and reasonable security against differential and linear cryptanalysis.

Keywords: branch number, ring of integers modulo n, binary matrices, differential cryptanalysis, linear cryptanalysis.

Курінний Олег Вікторович, студент Фізико-технічного інституту Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».
E-mail: ol.kurinnoy@gmail.com.
Orcid ID: 0000-0002-8866-3823.
Куринной Олег Викторович, студент Физико-технического института Национального технического университета Украины «Киевский политехнический институт имени Игоря Сикорского».
Kurinnyi Oleh, student of Institute of Physics and Technology, National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute».

Яковлєв Сергій Володимирович, кандидат технічних наук, доцент кафедри математичних методів захисту інформації Фізико-технічного інституту Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».
E-mail: yasv@rl.kiev.ua.
Orcid ID: 0000-0002-5647-5043.
Яковлев Сергей Владимирович, кандидат технических наук, доцент кафедры математических методов защиты информации Физико-технического института Национального технического университета Украины «Киевский политехнический институт имени Игоря Сикорского».
Yakovliev Serhii, Ph. D., assistant professor of Department of mathematical methods of information security, Institute of Physics and Technology, National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute».