УДК 004.056.55:519.2

ВИКОРИСТАННЯ АЛЬТЕРНАТИВНИХ АЛГЕБРАЇЧНИХ ОПЕРАЦІЙ ДЛЯ ДИФЕРЕНЦІАЛЬНОГО КРИПТОАНАЛІЗУ SP-МЕРЕЖ

С. О. Сергеєв[1, a]

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

Анотація

В даній роботі досліджуються такі випадки, коли блоковий шифр, стійкий до класичного диференціального криптоаналізу, може бути атакований при використанні інших альтернативних, побудованих спеціальним чином операцій, заданих на просторі повідомлень. Кальдеріні та Сала показали [3], як можна ефективно обчислювати альтернативні операції на векторному просторі, який може слугувати простором повідомлень для блокових шифрів. В даній роботі була обчислена кількість можливих операцій заданого вигляду.

Ключові слова: блоковий шифр, диференціальний криптоаналіз, альтернативні операції

Вступ

Диференціальний криптоаналіз [1] відноситься до так званих атак останнього раунду, оскільки основною метою проведення аналізу є встановлення раундового ключа останнього раунду. Стійкість шифрів до класичного диференціального криптоаналізу визначається максимумом диференціальної ймовірності. Відповідно, існує клас блокових шифрів, які є стійкими. Однак у [2] досліджена можливість проведення диференціальної атаки з альтернативними алгебраїчними, побудованими спеціальним чином операціями, на блокові шифри, які є стійкими до класичного диференціального криптоаналізу. Спочатку було визначено клас таких операцій, потім побудувано тестовий 15-бітовий шифр на SP-мережі. Порівнювалась його стійкість до класичного диференціального криптоаналізу та до атаки, яка використовує альтернативні операції. Актуальність даної роботи зумовлена можливістю застосовувати диференціальний криптоаналіз до стійких до нього шифрів. Задача даної роботи полягає у знаходженні кількості таких операцій.

1. Необхідні терміни та визначення

Нехай $V_n = \{0,1\}^n$, де $n = u \cdot m, m \geq 2$. Векторний простір V_n – це пряма сума

$$V_n = V_1 \oplus \ldots \oplus V_m,$$

де кожний підпростір V_i має розмірність u. $\forall v \in V_n$ будемо писати, що $v = v_1 \oplus \ldots \oplus v_m$, де $v_i \in V_i$.

Будемо позначати: $Sym(V_n)$ – група лінійних перетворень, що діє на V_n. $AGL(V_n), GL(V_n)$ – це, відповідно, афінна та лінійна група на V_n.

Нехай G – скінченна група, що діє на V_n. Будемо позначати дію перестановки $g \in G$ на вектор $v \in V_n$ як vg.

Визначення. Група G називається регулярною, якщо $\forall x, y \in V_n, \exists! g \in G : xg = y$. [3]

Нехай $T_\oplus$ – група трансляцій на просторі V_n, тобто $T_\oplus = \{K(X,a) | a \in V_n\}$, причому функція K діє на вектор X точно так, як і функція додавання з ключем діє на повідомлення X, тобто $K(X,k) = X \oplus k$. Отже, будемо вважати, що $\forall a, b \in V_n$ функція K така, що $K(a,b) = a \oplus b$. З огляду на це, SP-мережі можна також називати трансляційними шифрами. Щоб представити додавання з ключем як дію групи трансляцій на векторний простір V_n, автори роботи [2] означили, що $T_\oplus$ – абелева регулярна група, кожен елемент якої має порядок 2.

Далі, якщо ми визначимо, що $\forall a, b \in V_n : a \circ b = K(a,b)$, легко побачити, що $(V_n, \circ)$ – це адитивна група і що операції $\circ$ індукує структуру векторного простору на V_n, якій відповідає група трансляцій $T_\circ = T$.

Зауважимо, що операція $\circ$ має блокову структуру, тобто $\forall x, y \in V_n : x \circ y = (x_1 \circ y_1, \ldots, x_m \circ y_m)$, це дозволяє вивчати кожен S-блок незалежно від інших.

Нехай $\circ$ – нова операція, та $T_\circ$ є підгрупою $AGL_\oplus$, де $AGL_\oplus$ – це група всіх афінних функцій на векторному просторі $(V_n, \oplus)$.

$AGL_\circ$ – група афінних функцій на $(V_n, \circ)$.

В контексті вищевведених позначень визначимо *підпростір слабких ключів*, як:

$$W_\circ = \{k | k \in V_n, \forall x \in V_n : x \circ k = x \oplus k\}.$$

$W_\circ$ є векторним підпросторм як простору $(V_n, \oplus)$, так і простору $(V_n, \circ)$. Таким чином, кожний $k \in W_\circ$ представляє собою ключ, який можна додати до тексту незалежно від операції. В цьому контексті ми називаємо такі вектори *слабкими ключами*.

$Span\{e_{n-d+1}, \ldots, e_n\}$ – лінійна оболонка векторів $e_{n-d+1}, \ldots, e_n$.

Теорема 1.1. [2] Нехай $T_\circ$ – абелева регулярна підгрупа групи $AGL_\oplus$, кожний елемент групи $T_\circ$ має

[a] stas_sergeev@ukr.net

порядок 2. Тоді $W_\circ$ нетривіальний підпростір простору V_n. Більше того,

$$2 - (n \mod 2) \leq dim(W_\circ) \leq n - 2.$$

2. Ідея атаки

Ідею атаки розглянемо на прикладі 15-бітового блокового шифру, побудованого на SP-мережі, на просторі $V_{15} = \oplus_{i=1}^{5} \mathbb{F}_{2^3}$[2].

Нехай операція $\circ$ визначена наступними матрицями:

$$M_{e_1} = \begin{pmatrix} \mathbb{1}_2 & 0 & 0 & \dots & 0 \\ & 1 & 0 & \dots & 0 \\ \mathbb{O}_{13,2} & & & & \mathbb{1}_{13} \end{pmatrix},$$

$$M_{e_2} = \begin{pmatrix} \mathbb{1}_2 & 1 & 0 & \dots & 0 \\ & 0 & 0 & \dots & 0 \\ \mathbb{O}_{13,2} & & & & \mathbb{1}_{13} \end{pmatrix},$$

$M_{e_i} = \mathbb{1}_{15}, 3 \leq i \leq 15$. Операція $\circ$ визначена таким чином, що $dim(W_\circ) = 13$.

Розглянемо r-раундовий шифр, i-ий раунд якого визначається за формулою $\varphi_{i,k} = \gamma \ \lambda \ \sigma_{k_i}$, де:

- γ діє на кожний блок, як s-блок γ', визначений наступним чином:
  $\gamma' : F_{2^3} \to F_{2^3}$, який афінно еквівалентний функції $x \to x^3$.

x	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x
$x\ \gamma'$	0_x	6_x	2_x	1_x	5_x	7_x	4_x	3_x

- λ – матриця, визначена ось так:

$$\lambda = \begin{pmatrix} 1&0&1&0&1&0&0&0&1&0&1&0&1&0&1 \\ 0&1&1&0&1&0&1&0&0&0&1&0&1&0&1 \\ 0&0&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&1&0&1&0&1&0&0&0&0&0 \\ 0&0&0&0&0&1&1&0&1&0&1&1&0&1&0 \\ 0&0&1&1&1&0&0&0&0&0&0&1&0&1&0 \\ 0&0&1&0&0&1&0&0&1&0&1&0&1&1&0 \\ 0&0&0&0&1&0&0&0&1&1&1&0&0&1&1 \\ 0&0&1&1&1&0&1&1&0&0&1&0&1&1&1 \\ 0&0&1&1&1&0&1&0&0&1&1&1&1&1&0 \\ 0&0&1&1&0&0&0&0&0&0&1&1&1&0&1 \\ 0&0&0&0&0&1&1&1&0&1&0&0&1&0&1 \\ 0&0&0&0&1&0&0&0&0&1&0&0&1&1&1 \\ 0&0&1&1&1&0&0&1&1&1&0&1&1&1&1 \\ 0&0&0&1&1&1&0&0&0&0&1&0&1&0&0 \end{pmatrix}$$

- σ_{k_i} – функція додавання з раундовим ключем k_i. Ключі k_i випадкові, рівномірно розподілені на V_n.

Експериментальні обчислення показують, що найкращий 5-раундовий диференціал – це $(\delta_{I_\oplus}, \delta_{O_\oplus}) = (0007_x, 1301_x)$ має ймовірність $2^{-14.567}$, де різниця – це класична $\oplus$-різниця. Використовуючи $\circ$-різницю, було знайдено найкращий 5-раундовий диференціал, – $(\delta_{I_\circ}, \delta_{O_\circ}) = (3000_x, 019D_x)$ з ймовірністю $2^{-14.296}$. З урахуванням отриманих ймовірностей, автори роботи [2] знайшли, що більше ніж в половині випадків диференціал не проходить для $\oplus$-різниці, отже основна диференціальна атака не буде успішною. Використовуючи $\circ$-диференціал, різниця з'являється принаймні один раз на 56% ключів. Отже, це приклад шифру, який є стійким до класичного диференціального аналізу, та для якого розглядається операція, що відрізняється від тієї, яка використовується для додавання ключів, та дає успішну диференціальну атаку.

3. Оцінка кількості операцій

Введемо на просторі повідомлень V_n клас нових групових операцій $\circ$, відносно яких блокові шифри, побудовані на SP-мережі, які є стійкими до класичного диференціального криптоаналізу, будуть нестійкими. Після цього знайдемо кількість операцій такого типу.

Структура матриць, які задають операцію

Теорема 3.1. Нехай $T_\circ$ – абелева регулярна підгрупа групи $AGL_\oplus$ така, що $T_\oplus$ є підгрупою $AGL_\circ$ та $W_\circ = Span\{e_{n-d+1}, \dots, e_n\}$. Тоді для $\forall a \in V_n, \exists$ матриця $E_a \in (F_2)^{(n-d)\times d}$ така, що

$$M_a = \begin{pmatrix} \mathbb{1}_{n-d} & E_a \\ \mathbb{O}_{d,n-d} & \mathbb{1}_d \end{pmatrix}.$$

Більше того, канонічні вектори $\{e_i\}_{i=1}^n$ також є базисом для $(V_n, \circ)$.

Отже, як показано у теоремі 3.1, фіксація такої операції еквівалентна визначенню матриці $E_{e_i} \forall i, 1 \leq i \leq n$. Позначимо останні d компонентів j-го рядка матриці M_{e_i} як $b_{i,j}$ таким чином, щоби ми могли представити

$$M_{e_i} = \begin{pmatrix} \mathbb{1}_{n-d} & E_{e_i} \\ \mathbb{O}_{d,n-d} & \mathbb{1}_d \end{pmatrix} = \begin{pmatrix} & b_{i,1} \\ \mathbb{1}_{n-d} & \vdots \\ & b_{i,n-d} \\ \mathbb{O}_{d,n-d} & \mathbb{1}_d \end{pmatrix}.$$

Оскільки $W_\circ = Span\{e_{n-d+1}, \dots, e_n\}$, ми маємо, що $E_{e_i} =$ для всіх $n - d + 1 \leq i \leq n$. Більше того, оскільки $T_\circ$ – група, в якій кожний елемент має порядок 2, то для кожного $1 \leq i \leq n - d$ ми маємо $e_i \circ e_i = 0$, це означає, що $b_{i,i} = 0$. До того ж, оскільки для $1 \leq i, j \leq n - d$ ми маємо $e_i \circ e_j = e_j \circ e_i$, то $b_{i,j} = b_{j,i}$. Також легко показати, що $\forall a, b, c \in V_n$ маємо $(a \oplus b) \circ c = a \circ c \oplus b \circ c \oplus c$, тому якщо записати, що $a = \sum_{i=1}^n \xi_i e_i$ (тут і надалі в даній роботі знак суми означає операцію $\oplus$), то отримаємо

$$a \circ b = \begin{cases} \sum_{\xi_i \neq 0} \ b \circ e_i, & \text{якщо } wt(a) \text{ непарне}, \\ (\sum_{\xi_i \neq 0} \ b \circ e_i) \oplus b, & \text{якщо } wt(a) \text{ парне}, \end{cases}$$

де $wt(a)$ – вага Хеммінга вектора a, тобто кількість ненульових координат вектора a. З цього випливає, що значення $a \circ b$ може бути обчислене за поліноміальний час.

Обчислення кількості операцій

Оскільки кожна операція $\circ$ задається n матрицями $M_{e_i}, i = \overline{1,n}$, то, обчисливши кількість таких матриць, ми зможемо обчислити кількість всіх можливих операцій.

Спочатку знайдемо кількість матриць M_{e_1}, які мають наступний вигляд:

$$M_{e_1} = \begin{pmatrix} & b_{1,1} \\ & b_{1,2} \\ \mathbb{1}_{n-d} & b_{1,3} \\ & \vdots \\ & b_{1,n-d} \\ \mathbb{O}_{d,n-d} & \mathbb{1}_d \end{pmatrix}.$$

Оскільки рядок $b_{1,1} = 0$, то ми можемо обирати лише решту $n - d - 1$ бітових рядків, кожен з яких

містить d елементів. Таким чином, існує $2^{(n-d-1)\cdot d}$ матриць M_{e_1}.

Матриці M_{e_2} мають такий вигляд:

$$M_{e_2} = \begin{pmatrix} & b_{2,1} \\ & b_{2,2} \\ \mathbb{1}_{n-d} & b_{2,3} \\ & \vdots \\ & b_{2,n-d} \\ \mathbb{O}_{d,n-d} & \mathbb{1}_d \end{pmatrix}.$$

Оскільки рядок $b_{2,2} = 0$ та $b_{1,2} = b_{2,1}$, то ми можемо обирати лише решту $n-d-2$ бітових рядків, кожен з яких містить d елементів. Таким чином, існує $2^{(n-d-2)\cdot d}$ матриць M_{e_2}.

Знайдемо кількість матриць M_{e_3}, які мають наступний вигляд:

$$M_{e_3} = \begin{pmatrix} & b_{3,1} \\ & b_{3,2} \\ \mathbb{1}_{n-d} & b_{3,3} \\ & \vdots \\ & b_{3,n-d} \\ \mathbb{O}_{d,n-d} & \mathbb{1}_d \end{pmatrix}.$$

Оскільки рядок $b_{3,3} = 0$ та $b_{1,3} = b_{3,1}, b_{2,3} = b_{3,2}$, то ми можемо обирати лише решту $n-d-3$ бітових рядків, кожен з яких містить d елементів. Таким чином, існує $2^{(n-d-3)\cdot d}$ матриць M_{e_3}.

Аналогічним чином знаходимо кількість матриць $M_{e_i}, 4 \le i \le n-d$. Остання матриця $M_{e_{n-d}}$ задається однозначно та має наступний вигляд:

$$M_{e_{n-d}} = \begin{pmatrix} & b_{n-d,1} \\ & b_{n-d,2} \\ \mathbb{1}_{n-d} & b_{n-d,3} \\ & \vdots \\ & b_{n-d,n-d} \\ \mathbb{O}_{d,n-d} & \mathbb{1}_d \end{pmatrix},$$

де $b_{n-d,1} = b_{1,n-d}, b_{n-d,2} = b_{2,n-d}, b_{n-d,3} = b_{3,n-d}, \ldots, b_{n-d,n-d-1} = \overline{b_{n-d-1,n-d}}$ та $b_{n-d,n-d} = 0$.

Матриці $M_{e_i}, i = \overline{n-d+1, n}$ є одиничними, оскільки, як було зазначено, $E_{e_i} = \mathbb{O}$ для всіх $n-d+1 \le i \le n$.

Оскільки матриці обираються послідовно, то щоб обчислити кількість операцій (тобто, обрати набір матриць $M_{e_i}, i = \overline{1,n}$), треба скористатися правилом добутку:

$$2^{(n-d-1)\cdot d} \cdot 2^{(n-d-2)\cdot d} \cdot \ldots \cdot 2^{(n-d-(n-d))\cdot d} =$$
$$= 2^{0\cdot d} \cdot 2^{1\cdot d} \cdot 2^{2\cdot d} \cdot \ldots 2^{(n-d-2)\cdot d} \cdot 2^{(n-d-1)\cdot d} =$$
$$= 2^{d+2\cdot d+3\cdot d+\ldots+(n-d-2)\cdot d+(n-d-1)\cdot d} =$$
$$= 2^{d\cdot(1+2+3+\ldots+(n-d-2)+(n-d-1))} =$$
$$= 2^{\frac{d\cdot(n-d)\cdot(n-d-1)}{2}}$$

Таким чином, існує $2^{\frac{d\cdot(n-d)\cdot(n-d-1)}{2}}$ різних операцій.

Зауважимо, що оскільки $2 - (n \mod 2) \le d = dim(W_\circ) \le n-2$, то для непарних n кількість операцій при $d=1$ дорівнює $2^{\frac{(n-1)\cdot(n-2)}{2}}$, а для парних n при $d=2$ кількість операцій дорівнює $2^{(n-2)\cdot(n-3)}$. Длях віск n кількість операцій при $d = n-2$ дорівнює 2^{n-2}.

Висновки

Отже, у даній роботі розглядалася можливість застосовувати диференціальний криптоаналіз до блокових шифрів, які є стійкими до класичного диференціального криптоаналізу, використовуючи альтернативні алгебраїчні операції. Було обчислено кількість усіх можливих операцій запропонованого виду та показано, що вона обернено експоненційно залежить від розмірності простору слабких ключів.

Перелік використаних джерел

1. С. В. Яковлєв. Аналітичні оцінки стійкості немарковських симетричних блочних шифрів до диференціального криптоаналізу — 2014. — 160 с.
2. Céline Blondeau and Roberto Civino and Massimiliano Sala. Differential Attacks: Using Alternative Operations — 2017. — 12 с. — Режим доступу: `https://eprint.iacr.org/2017/610.pdf`.
3. M. Calderini, M. Sala. Elementary abelian regular subgroups as hidden sums for cryptographic trapdoors. — 2017. — 33 с. — Режим доступу: `https://arxiv.org/pdf/1702.00581.pdf`.