

Описание инвариантных подпространств матриц Адамара

Давыдов С.А.¹, Костарев С.В.²

¹АО «НПК «Криптонит»

²ФСР БИТ

s.davydov@kryptonite.ru, k0starevSV@yandex.ru

XSL-алгоритмы:

- 1 Наложение ключа по модулю 2 *XOR*
- 2 Нелинейное преобразование (параллельное действие S-блоков)
(*S, S, ..., S*)
- 3 Линейное рассеивающее преобразование *L*

Примеры XSL-алгоритмов блочного шифрования

- Кузнечик (ГОСТ Р 34.12-2015)
- AES
- Khazad
- LED
- и др.

Инварианты раундовой функции

Определение

Пусть $F: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ — подстановка. **Инвариантом** подстановки F называется такая булева функция $g: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$, что функция

$$g + g \circ F$$

является константой.

В этом случае $F(S_g) \in \{S_g, \mathbb{F}_2^n \setminus S_g\}$, где $S_g = \{x \in \mathbb{F}_2^n \mid g(x) = 1\}$.



Инварианты функции F ищут среди булевых функций определённого вида

¹Todo, Y., Leander, G., Sasaki, Y. «Nonlinear invariant attack: Practical attack on full SCREAM, iSCREAM, and Midori64», 2016.

²Буров Д. А., «О существовании нелинейных инвариантов специального вида для раундовых преобразований XSL-алгоритмов», 2021.

Метод криптоанализа на основе инвариантных подпространств

Если g является функцией-индикатором множества $W + \alpha$, где $W < \mathbb{F}_2^n$, $\alpha \in \mathbb{F}_2^n$, то говорят о методе криптоанализа на основе инвариантных подпространств. В этом случае $F(W + \alpha) = W + \alpha$.

Метод успешно применен к блочным шифрам PRINT³, Robin, iSCREAM, Zorro⁴, SCREAM, Midori64⁵, Khazad⁶.

³Leander, G., Abdelraheem, M.A., AlKhazaimi, H., Zenner, E. (2011). A Cryptanalysis of PRINTcipher: The Invariant Subspace Attack. Advances in Cryptology – CRYPTO 2011.

⁴Leander, G., Minaud, B., Rønjom, S. «A generic approach to invariant subspace attacks: Cryptanalysis of Robin, iSCREAM and Zorro», 2015.

⁵Todo, Y., Leander, G., Sasaki, Y. «Nonlinear invariant attack: Practical attack on full SCREAM, iSCREAM, and Midori64», 2016.

⁶Burov D. A., B. A. Pogorelov, «An attack on 6 rounds of Khazad», 2016.

Метод криптоанализа на основе инвариантных подпространств

Как искать инвариантные подпространства раундовой функции F XSL-схемы?

- Инвариантные подпространства $\mathbf{S} = (S, S, \dots, S)$
- Инвариантные подпространства L

Инвариантные подпространства матриц, используемых в L-слое

- Рекурсивные матрицы (Кузнечик^{7 8 9}, LED, PHOTON).
- Циркулянтные матрицы^{9 10} (AES, SM4, Whirlpool).
- Матрицы Адамара¹⁰ (Khazad, Anubis, CLEFIA).
- И др.

⁷Denis Fomin. «On the Impossibility of an Invariant Attack on Kuznyechik» 10-th Workshop on Current Trends in Cryptology (CTCrypt 2021). Pre-proceedings.

⁸Д. А. Буров, «О существовании нелинейных инвариантов специального вида для раундовых преобразований XSL-алгоритмов», Дискрет. матем., 33:2 (2021), 31–45.

⁹С.А. Давыдов, «Об инвариантных подпространствах матриц-циркулянтов и рекурсивных матриц», Дискрет. матем., 36:4 (2024), 44–63.

¹⁰А. В. Волгин, Г. В. Крючков, «Характеризация линейных преобразований, задающихся матрицами Адамара над конечным полем и циркулянтными матрицами», ПДМ. Приложение, 2017, № 10, 10–11.

Определение

Квадратная матрица H порядка 2^k над полем $\mathbb{F}_{2^s}$ называется матрицей Адамара (FFH-матрицей), если

$$H = \begin{pmatrix} U & V \\ V & U \end{pmatrix}, \quad (1)$$

где U, V FFH-матрицы размера $2^{k-1} \times 2^{k-1}$.

Инвариантные подпространства FFH-матрицы были использованы для построения атаки на **6 раундов** алгоритма **Khazad**¹¹.

¹¹Burov D.A., Pogorelov B.A., «An attack on 6 rounds of Khazad», 2016.

$$W^{(1)} = \{(a, a, b, b, e, e, d, d) | a, b, e, d \in \mathbb{F}_{28}\},$$

$$W^{(2)} = \{(a, b, a, b, e, d, e, d) | a, b, e, d \in \mathbb{F}_{28}\},$$

$$W^{(3)} = \{(a, b, b, a, e, d, d, e) | a, b, e, d \in \mathbb{F}_{28}\},$$

$$W^{(4)} = \{(a, b, e, d, a, b, e, d) | a, b, e, d \in \mathbb{F}_{28}\},$$

$$W^{(5)} = \{(a, b, e, d, b, a, d, e) | a, b, e, d \in \mathbb{F}_{28}\},$$

$$W^{(6)} = \{(a, b, e, d, e, d, a, b) | a, b, e, d \in \mathbb{F}_{28}\},$$

$$W^{(7)} = \{(a, b, e, d, d, e, b, a) | a, b, e, d \in \mathbb{F}_{28}\},$$

$$U^{(1)} = \{(a, a, a, a, b, b, b, b) | a, b \in \mathbb{F}_{28}\},$$

$$U^{(2)} = \{(a, a, b, b, a, a, b, b) | a, b \in \mathbb{F}_{28}\},$$

$$U^{(3)} = \{(a, a, b, b, b, b, a, a) | a, b \in \mathbb{F}_{28}\},$$

$$U^{(4)} = \{(a, b, a, b, a, b, a, b) | a, b \in \mathbb{F}_{28}\},$$

$$U^{(5)} = \{(a, b, a, b, b, a, b, a) | a, b \in \mathbb{F}_{28}\},$$

$$U^{(6)} = \{(a, b, b, a, a, b, b, a) | a, b \in \mathbb{F}_{28}\},$$

$$U^{(7)} = \{(a, b, b, a, b, a, a, b) | a, b \in \mathbb{F}_{28}\},$$

$$Z^{(1)} = \{(a, a, a, a, a, a, a, a) | a \in \mathbb{F}_{28}\}.$$

Инвариатные подпространства L-слоя с нетривиальной группой автоморфизмов

Определение

Группой автоморфизмов квадратной матрицы A порядка n над полем $\mathbb{F}_{2^s}$ назовем группу

$$\text{Aut}_d(A) = \{g = (g_1, g_2) \in S_n \times S_n \mid A^g = A\},$$

где $A^g = (a_{g_1(i), g_2(j)})$.

- Циркулянты и FFH-матрицы имеют нетривиальную группу автоморфизмов¹².
- Матрицы с нетривиальной группой автоморфизмов имеют собственные инвариатные подпространства¹².
- Полученные в работе¹² инвариатные подпространства FFH-матриц в точности соответствуют (2).

¹²Буров Д.А., Костарев С.В. «Группы автоморфизмов максимально рассеивающих матриц», CTCrypt 2025.

Жорданова форма матрицы Адамара

Теорема (А. В. Волгин, Г. В. Крючков¹⁰)

Пусть подматрица V матрицы Адамара H (1) обратима. Тогда каноническая форма матрицы $Ex + H$ равна

$$K(Ex + H) = \text{diag}(1, \dots, 1, (x + r)^2, \dots, (x + r)^2),$$

где r — сумма элементов строки матрицы H .

Следствие

Жорданова форма матрицы Адамара H равна

$$J(H) = \begin{pmatrix} r & 1 & 0 & 0 & \dots & \dots & 0 & 0 \\ 0 & r & 0 & 0 & \dots & \dots & 0 & 0 \\ 0 & 0 & r & 1 & \dots & \dots & 0 & 0 \\ 0 & 0 & 0 & r & \dots & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & \dots & r & 1 \\ 0 & 0 & 0 & 0 & \dots & \dots & 0 & r \end{pmatrix}$$

Инвариантные подпространства матриц Адамара

Матрица $J(H)$ подобна матрице T следующего вида:

$$P^{-1}J(H)P = T_{2^k \times 2^k} = \begin{pmatrix} R_{2^{k-1} \times 2^{k-1}} & E_{2^{k-1} \times 2^{k-1}} \\ O_{2^{k-1} \times 2^{k-1}} & R_{2^{k-1} \times 2^{k-1}} \end{pmatrix},$$

где O — нулевая матрица, E — единичная матрица, а $R = \text{diag}(r, r, \dots, r)$ — скалярная матрица соответствующих размеров.

Пример

Матрица $T_{8 \times 8}$ равна:

$$T_{8 \times 8} = \begin{pmatrix} r & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & r & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & r & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & r & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & r & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & r & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & r & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & r \end{pmatrix}.$$

Инвариантные подпространства матриц Адамара

Как найти инвариантные подпространства матрицы Адамара H ?

- Найти матрицу перехода (подобия) между матрицей Адамара и матрицей T .
- Описать инвариантные подпространства матрицы T .

Теорема

Пусть в (1) матрица V обратима. Тогда **решением** уравнения подобия $X^{-1}TX = H$ является матрица C такая, что

$$C = \begin{pmatrix} O & E \\ V & U + R \end{pmatrix}$$

и

$$C^{-1} = \begin{pmatrix} V^{-1}(U + R) & V^{-1} \\ E & O \end{pmatrix}.$$

Следствие

Для **максимально рассеивающей** матрицы H условия теоремы выполнены и матрица C является решением уравнения подобия.

Определение

- 1 **Прямой суммой** подпространств $Y, W < \mathbb{F}_{2^s}^m$ называется подпространство $(Y \dot{+} W) < \mathbb{F}_{2^s}^m$, содержащее всевозможные суммы $y + w$ элементов $y \in Y, w \in W$, при этом каждый элемент представляется в виде указанной суммы единственным образом.
- 2 **Внешней прямой суммой** подпространств $Y, W < \mathbb{F}_{2^s}^m$ называется подпространство $(Y \oplus W) < \mathbb{F}_{2^s}^m$, состоящее из элементов декартова произведения множеств Y, W с операциями сложения и умножения на элементы поля, выполняемыми независимо для каждой координаты — элемента подпространства Y или W .

Теорема

Подпространство $W < \mathbb{F}_{2^s}^{2^k}$ является **инвариантным** подпространством преобразования T тогда и только тогда, когда W есть прямая сумма подпространств

$$W = W_e \dot{+} B,$$

где W_e — подпространство **собственных векторов** преобразования T , $W_e = \langle \theta \rangle \oplus (W_e)_R$, $B = (B_L, B_R)$ и $B_L < (W_e)_R < \mathbb{F}_{2^s}^{2^{k-1}}$.

$$T_{8 \times 8} = \begin{pmatrix} r & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & r & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & r & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & r & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & r & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & r & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & r & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & r \end{pmatrix}$$

$$W^{(1)} = \{(a, a, b, b, e, e, d, d) | a, b, e, d \in \mathbb{F}_{28}\},$$

$$W^{(2)} = \{(a, b, a, b, e, d, e, d) | a, b, e, d \in \mathbb{F}_{28}\},$$

$$W^{(3)} = \{(a, b, b, a, e, d, d, e) | a, b, e, d \in \mathbb{F}_{28}\},$$

$$W^{(4)} = \{(a, b, e, d, a, b, e, d) | a, b, e, d \in \mathbb{F}_{28}\},$$

$$W^{(5)} = \{(a, b, e, d, b, a, d, e) | a, b, e, d \in \mathbb{F}_{28}\},$$

$$W^{(6)} = \{(a, b, e, d, e, d, a, b) | a, b, e, d \in \mathbb{F}_{28}\},$$

$$W^{(7)} = \{(a, b, e, d, d, e, b, a) | a, b, e, d \in \mathbb{F}_{28}\},$$

$$U^{(1)} = \{(a, a, a, a, b, b, b, b) | a, b \in \mathbb{F}_{28}\},$$

$$U^{(2)} = \{(a, a, b, b, a, a, b, b) | a, b \in \mathbb{F}_{28}\},$$

$$U^{(3)} = \{(a, a, b, b, b, b, a, a) | a, b \in \mathbb{F}_{28}\},$$

$$U^{(4)} = \{(a, b, a, b, a, b, a, b) | a, b \in \mathbb{F}_{28}\},$$

$$U^{(5)} = \{(a, b, a, b, b, a, b, a) | a, b \in \mathbb{F}_{28}\},$$

$$U^{(6)} = \{(a, b, b, a, a, b, b, a) | a, b \in \mathbb{F}_{28}\},$$

$$U^{(7)} = \{(a, b, b, a, b, a, a, b) | a, b \in \mathbb{F}_{28}\},$$

$$Z^{(1)} = \{(a, a, a, a, a, a, a, a) | a \in \mathbb{F}_{28}\}.$$

Пример

Подпространство $W^{(1)}$ задаётся *четырьмя векторами*:

$$W^{(1)} = \langle \vec{C}_7 + \vec{C}_6, \vec{C}_5 + \vec{C}_4, \vec{C}_3 + \vec{C}_2, \vec{C}_1 + \vec{C}_0 \rangle,$$

которые определяются следующими подпространствами теоремы:

$$W_e = \langle (0, 0, 0, 0, 1, 1, 0, 0), (0, 0, 0, 0, 0, 0, 1, 1) \rangle;$$

$$B = \langle (1, 1, 0, 0, 0, 0, 0, 0), (0, 0, 1, 1, 0, 0, 0, 0) \rangle.$$

Подпространство $Z^{(1)}$ задаётся *вектором*:

$$Z^{(1)} = \langle \vec{C}_3 + \vec{C}_2 + \vec{C}_1 + \vec{C}_0 \rangle.$$

Замечание

Из теоремы следует, что матрица Адамара размера 8×8 над полем $\mathbb{F}_{2^8}$ имеет по крайней мере $2^{32} - 1$ собственных векторов, в то время как в $\mathbb{F}_6$ представлено единственное подпространство, содержащее собственные векторы — $Z^{(1)}$, в него входит 255 собственных векторов.

⁶ Burov D.A., Pogorelov B.A., «An attack on 6 rounds of Khazad», 2016.

Определение

Подпространство W пространства $\mathbb{F}_{2^s}^m$, инвариантное относительно любого преобразования $\mathbf{S} = (S, \dots, S)$, $S \in \text{Sym}(\mathbb{F}_{2^s})$, будем называть подпространством *вида 1*.

Гипотеза (1)

Инвариантные подпространства *вида 1* матрицы Адамара H исчерпываются инвариантными подпространствами из теоремы 6 работы ¹² при условии, что H является *максимально рассеивающей матрицей*.

Гипотеза (2)

Инвариантные подпространства *вида 1* матрицы Адамара H исчерпываются инвариантными подпространствами из теоремы 6 работы ¹² при условии, что *подматрица V матрицы H обратима*.

¹² Буров Д.А., Костарев С.В. «Группы автоморфизмов максимально рассеивающих матриц», СТСrypt 2025.

Определение

Циркулянтной матрицей размера $m \times m$ над полем $\mathbb{F}_{2^s}$ будем называть матрицу, у которой каждая строка $\vec{C}_i$ есть циклический сдвиг влево строки $\vec{C}_{i-1}, i \in \overline{1, m-1}$.

$$C_{m \times m} = \text{Circ}_{2^s}(c_{m-1}, \dots, c_0) = \begin{pmatrix} c_0 & c_{m-1} & \dots & c_2 & c_1 \\ c_1 & c_0 & \dots & c_3 & c_2 \\ \dots & & & & \\ c_{m-2} & c_{m-3} & \dots & c_0 & c_{m-1} \\ c_{m-1} & c_{m-2} & \dots & c_1 & c_0 \end{pmatrix}.$$

Пусть $\mathbb{P} = \mathbb{F}_{2^s}$, $C = \text{Circ}_{2^s}(c_{2^k-1}, \dots, c_0) \in \mathbb{P}_{2^k, 2^k}$ и

$$B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{\otimes k} \in \mathbb{P}_{2^k, 2^k},$$

где $\otimes$ — кронекерова степень матрицы.

Тогда $B^{-1}CB = T$, где $T \in \mathbb{P}_{2^k, 2^k}$ — *верхнетреугольная матрица Тёплица* вида:

$$T = \begin{pmatrix} t_0 & t_1 & t_2 & \dots & t_{2^k-1} \\ 0 & t_0 & t_1 & \dots & t_{2^k-2} \\ \dots & & & & \\ 0 & 0 & \dots & t_0 & t_1 \\ 0 & 0 & 0 & \dots & t_0 \end{pmatrix}, \quad t_i = \sum_{j \preceq (2^k-1-i)} c_{(j+1 \bmod 2^k)},$$

где $j \preceq (2^k - 1 - i)$ означает что каждый разряд в двоичной записи числа j не превосходит соответствующего разряда в двоичной записи числа $2^k - 1 - i$.

⁹ С.А. Давыдов, «Об инвариантных подпространствах матриц-циркулянтов и рекурсивных матриц», Дискрет. матем., 36:4 (2024), 44–63.

Утверждение

Матрица Адамара H (1) с обратимой матрицей V подобна циркулянтной матрице

$$C_{2^k \times 2^k} = \text{Circ}_{2^k}(0, \dots, 0, 1, 0, \dots, 0, r + 1),$$

где r есть сумма элементов строки матрицы Адамара H , а единица расположена на позиции 2^{k-1} .