УДК 512.643.8 DOI 10.17223/2226308X/10/2

ХАРАКТЕРИЗАЦИЯ ЛИНЕЙНЫХ ПРЕОБРАЗОВАНИЙ, ЗАДАЮЩИХСЯ МАТРИЦАМИ АДАМАРА НАД КОНЕЧНЫМ ПОЛЕМ И ЦИРКУЛЯНТНЫМИ МАТРИЦАМИ

А. В. Волгин, Г. В. Крючков

Приведены общие и криптографические свойства циркулянтных матриц и линейных преобразований, задаваемых матрицами Адамара над конечным полем. Описаны инвариантные подпространства матриц Адамара над конечным полем. Построен класс подпространств, гарантированно являющихся инвариантными для циркулянтных матриц.

Ключевые слова: *инвариантные подпространства, матрицы Адамара над конечным полем, циркулянтные матрицы.*

В большинстве современных блочных XSL-шифрсистем преобразования линейного слоя, обеспечивающие хорошее рассеивание, являются приводимыми. Например, матрицы Адамара над конечным полем (KHAZAD [1], ANUBIS [2]), циркулянтные матрицы (AES [3], WHIRLPOOL [4]), подстановочные матрицы (SP-сети) гарантированно имеют инвариантные подпространства.

Наличие инвариантных подпространств приводит к импримитивности группы $C(g)$ [5], порождённой слоем наложения ключа V_n^+ и приводимой матрицей $g \in \mathrm{GL}_n(2)$. Системы импримитивности этой группы сохраняются линейным слоем и слоем наложения ключа, поэтому рассеивание блоков импримитивности в алгоритме шифрования может обеспечить только слой s-боксов. Подобные слабости успешно использованы в работах [6, 7] по исследованию шифрсистем KHAZAD и PRINT.

Обозначим через $P = GF(2^n)$ конечное поле, $n \in \mathbb{N}$.

Определение 1 [8, 9]. Пусть $m \in \mathbb{N}_0$. Матрица $H = (h_{i,j}) \in P_{2^m,2^m}$ называется *матрицей Адамара над конечным полем* (*FFH-матрицей*), если для некоторого вектора $(a_0, \ldots, a_{2^m-1}) \in P^{2^m}$ выполняется соотношение $h_{i,j} = a_{i \oplus j}$. При этом матрицу H будем обозначать $H = \mathrm{had}(a_0, \ldots, a_{2^m-1})$.

В работе получены следующие простейшие свойства FFH-матриц.

Утверждение 1. Пусть $H = \mathrm{had}(a_0, \ldots, a_{2^m-1}) \in P_{2^m,2^m}$, $r = \sum\limits_{i=0}^{2^m-1} a_i \in P$. Тогда

1) H — симметрическая матрица;
2) $H^2 = r^2 E$;
3) класс FFH-матриц замкнут относительно операций сложения и умножения матриц, умножения матрицы на константу, тензорного произведения матриц;
4) H подобна верхнетреугольной матрице и её характеристический многочлен имеет вид $\chi_H(x) = (x + r)^{2^m}$;
5) если $H_1, H_2 \in P_{2^m,2^m}$ — FFH-матрицы, то $H_1 H_2 = H_2 H_1$.

Далее опишем инвариантные подпространства матриц Адамара.

Теорема 1. Пусть $m \in \mathbb{N}$ и $H = \mathrm{had}(a_0, \ldots, a_{2^m-1}) \in P_{2^m,2^m}$. Пусть также $H = \begin{pmatrix} U & V \\ V & U \end{pmatrix}$ и матрица $V \in P_{2^{m-1},2^{m-1}}$ невырождена. Тогда каноническая форма матрицы $Ex + H \in P[x]_{2^m,2^m}$ имеет вид

$$K(Ex + H) = \mathrm{diag}(1, \ldots, 1, (x + r)^2, \ldots, (x + r)^2), \text{ где } r = \sum_{i=0}^{2^m-1} a_i.$$

Определение 2 [10]. Пусть $m \in \mathbb{N}$. Матрица $C = (c_{i,j})_{m,m}$ называется *циркулянтом* (*циркулянтной матрицей*), если для некоторого вектора $(c_0, c_1, \ldots, c_{m-1}) \in P^m$ выполняется $c_{i,j} = c_{j-i}$ для любых $i, j \in (\mathbb{Z}_m, +)$. Далее матрицу C будем обозначать $\mathrm{circ}(c_0, c_1, \ldots, c_{m-1})$.

Всюду далее рассматриваются циркулянты размера $2^m \times 2^m$.

Опишем класс инвариантных подпространств для циркулянтных матриц.

Утверждение 2. Пусть $m \in \mathbb{N}$, $C = \mathrm{circ}(c_0, c_1, \ldots, c_{2^m-1}) \in P_{2^m,2^m}$. Тогда характеристический многочлен матрицы C имеет вид $\chi_C(x) = (x + r)^{2^m}$, где $r = \sum\limits_{i=0}^{2^m-1} c_i$. Матрица C подобна верхнетреугольной матрице, и матрица C_m, осуществляющая подобие, имеет вид

$$C_m = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{\otimes m} \in P_{2^m,2^m}.$$

Таким образом, матрица C_m задаёт систему вложенных инвариантных подпространств преобразования, задающегося матрицей C. Данные подпространства имеют вид

$$\langle C_1^{\downarrow} \rangle,\ \langle C_1^{\downarrow}, C_2^{\downarrow} \rangle,\ \ldots,\ \langle C_1^{\downarrow}, C_2^{\downarrow}, \ldots, C_{2^m}^{\downarrow} \rangle,$$

где $C_i^{\downarrow}$ — вектор-столбцы матрицы C_m для $i \in \{1, \ldots, 2^m\}$.

ЛИТЕРАТУРА

1. *Barreto P. S. L. M. and Rijmen V.* The KHAZAD Legacy-Level Block Cipher. Submission to the NESSIE Project. 2000. `https://www.researchgate.net/publication/228924670_The_Khazad_legacy-level_block_cipher`
2. *Biryukov A.* Analysis of involutional ciphers: Khazad and Anubis // Intern. Workshop Fast Software Encryption. Berlin, Heidelberg: Springer, 2003. P. 45–53.
3. *Daemon J. and Rijmen V.* The Rijndael block cipher: AES proposal // First AES Candidate Conf. (AES1). Ventura, California, August 20–22, 1998. P. 343–348.
4. *Barreto P. S. L. M. and Rijmen V.* The Whirlpool hashing function // First open NESSIE Workshop, Leuven, Belgium. 2000. V. 13. P. 14.
5. *Погорелов Б. А., Пудовкина М. А.* Комбинаторная характеризация XL-слоев // Математические вопросы криптографии. 2013. Т. 4. №. 3. С. 99–129.
6. *Burov D. A. and Pogorelov B. A.* An attack on 6 rounds of Khazad // Математические вопросы криптографии. 2016. Т. 7. № 2. С. 35–46.
7. *Leander G. et al.* A cryptanalysis of PRINTcipher: the invariant subspace attack // Ann. Cryptology Conf. Berlin, Heidelberg: Springer, 2011. P. 206–221.
8. *Gupta K. C. and Ray I. G.* On constructions of involutory MDS matrices // Intern. Conf. Cryptology in Africa. Berlin, Heidelberg: Springer, 2013. P. 43–60.
9. *Sakall M. T., Akleylek S., Aslan B., et al.* On the construction of 20×20 and 24×24 binary matrices with good implementation properties for lightweight block ciphers and hash functions // Mathematical Problems in Engineering. 2014. V. 2014. 12 p.
10. *Gray M.* Toeplitz and circulant matrices: a review // Foundations and Trends in Communications and Information Theory. 2006. V. 2. No. 3. P. 155–239.