ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 26 МАТЕМАТИКИ Выпуск 2
2019

А. В. Анашкин (Москва, Лаб. ТВП). **О числе классов CCZ эквивалентных подстановок на V_4.**

Два биективных отображения $F, G : V_n \to V_n$ будем называть:

а) *линейно эквивалентными* (обозначение $F \overset{LE}{\sim} G$), если существуют $A, B \in GL(n,2) : G = A^{-1} \cdot F \cdot B$ [2];

б) *аффинно эквивалентными* (обозначение $F \overset{AE}{\sim} G$), если существуют $A_\alpha, B_\beta \in AGL(n,2) : G = A_\alpha^{-1} \cdot F \cdot B_\beta$ [2];

в) *обобщенно линейно эквивалентными* (обозначение $F \overset{GLE}{\sim} G$), если существует $C \in GL(2n,2) : \{(x, G(x)) | x \in V_n\} = C(\{(x, F(x)) | x \in V_n\})$ [3];

г) *обобщенно аффинно эквивалентными*, или *CCZ эквивалентными* (обозначение $F \overset{GAE}{\sim} G$), если существует $G_\gamma \in AGL(2n,2) : \{(x, G(x)) | x \in V_n\} = C_\gamma(\{(x, F(x)) | x \in V_n\})$ [1];

д) *расширенно аффинно эквивалентными* (обозначение $F \overset{EAE}{\sim} G$), если существуют $A_\alpha, B_\beta \in AGL(n,2)$ и линейное отображение $L : V_n \to V_n : G = A_\alpha^{-1} \cdot F \cdot B_\beta + L$ [1].

Нетрудно проверяется справедливость следующих импликаций: $F \overset{LE}{\sim} G \Rightarrow F \overset{GLE}{\sim} G$ и $F \overset{AE}{\sim} G \Rightarrow F \overset{EAE}{\sim} G \Rightarrow F \overset{GAE}{\sim} G$, в частности, справедлива диаграмма:

$$\begin{array}{ccc} F \overset{LE}{\sim} G & \Rightarrow & F \overset{AE}{\sim} G \\ \Downarrow & & \Downarrow \\ F \overset{GLE}{\sim} G & \Rightarrow & F \overset{GAE}{\sim} G \end{array}$$

В [2] указано, что число классов аффинной эквивалентности подстановок на V_4 равно 302. В [4] приведено число классов расширенной аффинной эквивалентности, равное 194. Это же число позже получено и в [5]. Поскольку классы CCZ эквивалентности являются объединением классов (расширенной) аффинной эквивалентности, то для выделения представителей CCZ эквивалентности достаточно проверить, являются ли попарно CCZ эквивалентными представители аффинной (или расширенной аффинной) эквивалентности. Используя известные инварианты CCZ эквивалентности и проведя необходимые вычисления, получаем следующее

Утверждение. *Число классов подстановок из S_{v_4} по отношению CCZ эквивалентности составляет* 147.

СПИСОК ЛИТЕРАТУРЫ

1. *Carlet C.*, *Chaplin P.*, *Zinoviev V.* Codes, Bent functions and permutations suitable for DES-like cryptosystems. — Designs, Codes and Cryptography, 1998, v. 15, 2, p. 125–156.

2. *Biryukov A.*, *Canniere C. De.*, *Braeken A.*, *Preneel B.* A Toolbox for Cryptanalysis: Linear and Affine Equivalence Algorithms. — Proc. of Eurocrypt 2003, LNCS v. 2656, Berlin: Springer Berlin Heidelberg, 2003, p. 33–50.
3. *Breveglieri L.*, *Cherubini A.*, *Macchetti M.* On the Generalized Linear Equivalence of Functions Over Finite Fields. — Proc. of Asiacrypt 2004, LNCS v. 3329, Berlin: Springer Berlin Heidelberg, 2004, p. 79–91.
4. *Анашкин А. В.* О числе классов EA-эквивалентных подстановок на V_4. — Обозрение прикл. и промышл. матем., 2016, т. 23, в. 5, с. 459–460.
5. *Brinkmann M.* Extended Affine and CCZ Equivalence up to Dimension 4. – https://eprint.iacr.org/2019/316 – 29.03.2019.