ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 23 МАТЕМАТИКИ Выпуск 5
2016

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

В работе [1] исследуются свойства, так называемого отношения расширенной аффинной эквивалентности (EA-эквивалентность). При фиксированном натуральном числе n две подстановки g и h из множества S_{V_n} всех подстановок на множестве V_n двоичных векторов длины называются EA-эквивалентными, если найдутся два аффинных отображения $A, B \in AGL(n, 2)$ и одно линейное, не обязательно обратимое отображение $L : V_n \to V_n$ такие, что $g = AhB + L$. Отметим, что отношение аффинной эквивалентности получается из EA-эквивалентности при $L = 0$. Если дополнительно выполняется $A, B \in GL(n, 2)$, то отношение называется отношением линейной эквивалентности.

В работе [2] предложен алгоритм проверки аффинной (и линейной) эквивалентности двух подстановок. Авторы работы упоминают и об общем числе классов аффинной эквивалентности подстановок $S_{V_4} - 302$.

Представители классов аффинной эквивалентности можно получить случайным поиском. Поскольку классы EA-эквивалентности являются объединением классов аффинной эквивалентности, то для выделения представителей EA-эквивалентности достаточно проверить, являются ли попарно эквивалентными представители аффинной эквивалентности. Или, другими словами, для данного представителя g класса аффинной эквивалентности, перебирая все линейные отображения $L : V_n \to V_n$, требуется проверить, является ли отображение $g + L$ подстановкой, и в какой класс аффинной эквивалентности эта подстановка попадает.

Проведя необходимые вычисления, получаем

Утверждение. *Число классов подстановок из* S_{V_4} *по отношению EA-эквивалентности составляет* 194.

СПИСОК ЛИТЕРАТУРЫ

1. *Carlet C.*, *Charpin 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.*, *De Canniere C.*, *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.

© Редакция журнала «ОПиПМ», 2016 г.