ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 26 МАТЕМАТИКИ Выпуск 2
2019

А. В. Анашкин (Москва, Лаб. ТВП)**.** Об оценках некоторых численных характеристик композиции биективных отображений

В ряде работ [1–5] излагаются способы оценивания характеристик преобразования H векторного пространства V_n, реализуемого композицией биективных отображений. Суть этих способов обычно сводится к следующему. Получают оценку или точное значение требуемой характеристики для одного или произведения небольшого числа отображений (как правило, 1–2), а затем интерполируют результат на всё преобразование. Интерполяция состоит в перемножении значений характеристики для каждого отображения (или произведения нескольких отображений), а если отображения однотипные, то, соответственно, в возведении в степень. Полученное «малое» значение характеристики представляется в качестве «доказательства» «хороших свойств» результирующего преобразования.

Каких-либо обоснований близости точного значения рассматриваемой характеристики и получаемой «оценки» авторами работ не приводится.

Между тем, преобразование H является взаимно-однозначным и, значит, найдется натуральное t такое, что $H^t = E$ — тождественное отображение, для которого множество значения упоминаемых характеристик состоит всего из двух элементов — 0 или 1.

Задача нахождения минимального значения величины t, порядка подстановки H в группе S_{V_n}, для преобразований из некоторых заданных классов, представляет самостоятельный интерес. Известно, что t делит порядок группы $|S_{V_n}| = (2^n)!$, но последняя величина достаточно большая. В то же время даже для сложно устроенных преобразований их порядок может иметь и минимальное нетривиальное значение, равное 2 [6].

СПИСОК ЛИТЕРАТУРЫ

1. *Кирюхин В. А.* Верхние оценки на вероятность дифференциалов в двухраундовых LSX-шифрах. — Обозрение прикл. и промышл. матем., 2018, т. 25, в. 4, с. 370–371.
2. *Matsui M.* Linear cryptanalysis method for DES cipher. — Advances in Cryptology, proc. of Eurocrypt '93, LNCS v. 765, Berlin: Springer, 1999, p. 386–397.
3. *Ohta K.*, *Morari S.*, *Aoki K.* Improving the search algorithm for the best linear expression. — Advances in Cryptology, proc. of Crypto '95, LNCS v. 963, Berlin: Springer-Verlag, 1995, p. 157–170.
4. *Wang M. Q.*, *Wang X. Y.*, *Hu C. H.* New linear cryptanalytic results of reduced-round of CAST-128 and CAST-256. — Selected Areas in Cryptology, SAC 2008, LNCS v. 5381, Berlin: Springer, 2009, p. 429–441.
5. *Daemen J.*, *Rijmen V.* The design of Rijndael. Berlin: Springer-Verlag, 2002.
6. *Biham E.*, *Dunkelman O.*, *Keller N.* Improved Slide Attacks. — Fast Software Encryption, 14th International Workshop, FSE 2007, LNCS v. 4593, Berlin: Springer, 2007, p. 153–166.