

4. *Smyshlyaev S. V.* Perfectly Balanced Boolean Functions and Golić Conjecture // J. Cryptology. 2012. No. 25(3). P. 464–483.

УДК 519.7

О РАЗЛОЖЕНИИ БУЛЕВОЙ ФУНКЦИИ В СУММУ БЕНТ-ФУНКЦИЙ¹

Н. Н. Токарева

Булева функция от чётного числа переменных, максимально удалённая от класса всех аффинных функций, называется *бент-функцией*. В работах [1, 2] исследована связь между вопросом о числе бент-функций и проблемой разложения произвольной булевой функции в сумму двух бент-функций. Была представлена серия гипотез, одна из которых заключается в том, что каждую булеву функцию от n переменных степени не больше $n/2$ можно представить в виде суммы двух бент-функций от n переменных. В [2] с помощью компьютера гипотеза проверена для малых значений $n \leq 6$.

В 2011 г. Л. Ку и С. Ли [3] разобрали случай малых n аналитически. В общем случае они доказали, что в виде суммы двух бент-функций может быть представлена любая квадратичная булева функция, любая бент-функция Мак-Фарланда, любая функция частичного расщепления (*partial spread function*).

В данной работе доказан ослабленный вариант гипотезы.

Теорема 1. Любая булева функция от n переменных степени d , где $d \leq n/2$, n чётно, может быть представлена в виде суммы не более чем $2 \binom{2b}{b}$ бент-функций от n переменных, где b — наименьшее число, $b \geq d$, такое, что n делится на $2b$.

Заметим, что разложение, указанное в теореме, можно провести с помощью только бент-функций Мак-Фарланда.

ЛИТЕРАТУРА

1. *Токарева Н. Н.* Гипотезы о числе бент-функций // Прикладная дискретная математика. Приложение. 2011. № 4. С. 21–23.
2. *Tokareva N.* On the number of bent functions from iterative constructions: lower bounds and hypotheses // Adv. in Mathematics of Communications (AMC). 2011. V. 5. No. 4. P. 609–621.
3. *Qu L. and Li C.* Representing a Boolean function as the sum of two Bent functions // Discrete Applied Mathematics. 2012 (to appear).

УДК 681.03

ЛАТИНСКИЕ КВАДРАТЫ И ИХ ПРИМЕНЕНИЕ В КРИПТОГРАФИИ

М. Э. Тужилин

Подсчёт числа латинских квадратов порядка n — сложная комбинаторная задача, их точное число известно только для n от 1 до 11 [1].

Латинские квадраты находят применение в комбинаторике, алгебре (изучение латинских квадратов тесно связано с изучением квазигрупп), теории кодов, статистике и многих других областях [2].

¹Исследование выполнено при поддержке РФФИ (проекты 10-01-00424, 11-01-00997) и ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 г. (гос. контракт 02.740.11.0429).