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-ФУНКЦИЙ[1]

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 $n \leqslant 6$.

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 $d \leqslant n/2$, n чётно, может быть представлена в виде суммы не более чем $2\binom{2b}{b}$ бент-функций от n переменных, где b — наименьшее число, $b \geqslant d$, 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].

[1]Исследование 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).

Впервые в криптографии латинский квадрат был применён в шифре И. Тритемия [3]. Значение латинских квадратов для криптографии иллюстрирует теорема Шеннона, в соответствии с которой единственными совершенными шифрами являются шифры гаммирования, наложение гаммы в которых определяется латинским квадратом [4]. Попытка обобщить подход Шеннона и ввести понятие «сильно совершенный шифр» предпринята в [5].

Краткий обзор результатов по применению латинских квадратов для построения схем аутентификации, шифрования и однонаправленных функций содержится в [6].

В ряду примеров применения латинских квадратов для построения поточных шифров необходимо выделить предложенный в 2005 г. шифр Edon80 [7], который дошёл до третьего тура конкурса ESTREAM. Разработчики шифра из 576 существующих латинских квадратов 4-го порядка тщательно выбрали 4, на основе которых в криптосхеме строится конвейер из 80 латинских квадратов, он используется для выработки гаммы.

При разработке блочного шифра IDEA [8] авторы использовали три квазигруппы, соответствующие операциям сложения по модулю 2, сложения по модулю 2^{16} и умножения по модулю $2^{16}+1$. При этом высокие криптографические свойства шифра они обосновали существованием единственной изотопии между двумя из используемых квазигрупп.

Латинские квадраты являются привлекательным средством для построения схем разделения секрета. Секретом является латинский квадрат, а все участники схемы получают его частично заполненным (он называется частичным). Задача распознавания того, может ли частичный квадрат быть однозначно дополнен до латинского, NP-полна. Наряду с большим количеством латинских квадратов это обстоятельство и определяет стойкость схемы [9]. Предложенная схема может быть усовершенствована [10]. В свою очередь, на основе таких схем разделения секрета можно строить и криптографические хеш-функции [11]. Другой пример построения криптографической хеш-функции на основе случайного латинского квадрата приведён в [12].

Разработанное в 2008 г. для участия в конкурсе SHA-3 на новый американский стандарт хеш-функции семейство Edon-R [13] не прошло во второй тур, но интересно тем, что в основе конструкции лежит построение и использование некоммутативной неассоциативной нелинейной квазигруппы.

В [14] предложен протокол с нулевым разглашением. Каждый участник имеет открытый ключ, которым являются два эквивалентных латинских квадрата. Секретным ключом является изотопия между ними.

В заключение отметим, что о растущем внимании к теме свидетельствует появление обзоров [6, 15].

ЛИТЕРАТУРА

1. *McKay B. D. and Wanless I. M.* On the number of Latin Squares // Ann. Combin. 2005. No. 9. P. 335–344.
2. *Laywine C. F. and Mullen G. L.* Discrete mathematics using Latin squares. New York: Wiley, 1998.
3. *Trithemius J.* Polygraphiae. 1518.
4. *Shannon C.* Codes, bent functions and permutations suitable for DES-like cryptosystems // Designs, Codes and Cryptography. 1998. No. 15(2). P. 125–156.
5. *Massey J. L., Maurer U., and Wang M.* Non-Expanding, Key-Minimal, Robustly-Perfect, Linear and Bilinear Ciphers // Adv. Cryptology — EUROCRYPT'87. Berlin, Heidelberg: Springer Verlag, 1988. P. 237–247.

6. *Глухов М. М.* О применениях квазигрупп в криптографии // Прикладная дискретная математика. 2008. № 2(2). С. 28–32.
7. *Gligoroski D., Markovski S., Kocarev L., and Gusev M.* Edon80 // `http://www.ecrypt.eu.org/stream/edon80p3.html`
8. *Lai X. and Massey J.* A Proposal for a New Block Encryption Standard // Adv. Cryptology — EUROCRYPT'90. New York: Springer Verlag, 1991. P. 55–70.
9. *Cooper J., Donovan D., and Seberry J.* Secret Sharing Schemes Arising From Latin Squares // Bulletin of the ICA. 1994. V. 12. P. 33–43.
10. *Chum C. S. and Zhang X.* The Latin squares and the secret sharing schemes // Groups Complex. Cryptol. 2010. V. 2. P. 175–202.
11. *Chum C. S.* Hash functions, Latin squares and secret sharing schemes. New York: ProQuest, 2010.
12. *Pal S. K., Bhardwaj D., Kumar R., and Bhatia V.* A New Cryptographic Hash Function based on Latin Squares and Non-linear Transformations // Adv. Comput. Conf. IACC, 2009. P. 862–867.
13. *Gligoroski D., Ødegård R. S., Mihova M., et al.* Cryptographic Hash Function Edon-R // Proc. IWSCN, 2009. P. 1–9.
14. *Dènes J. and Dènes T.* Non-associative algebraic system in cryptology. Protection against "meet in the middle" attack // Quasigroups and Related Systems. 2001. No. 8. P. 7–14.
15. *Shcherbacov V. A.* Quasigroups in cryptology // Comput. Sci. J. Moldova. 2009. V. 17. No. 2(50). P. 193–228.

УДК 519.7

СВОЙСТВО КРАТНЫХ ПРОИЗВОДНЫХ БЕНТ-ФУНКЦИЙ КАСАМИ[1]

А. А. Фролова

Одно из криптографических свойств булевой функции — это высокая нелинейность. Булевы функции, обладающие экстремальной нелинейностью, при чётном числе переменных называются *бент-функциями*. Описание класса всех бент-функций от произвольного числа переменных остается открытой проблемой, однако известны некоторые конструкции бент-функций [1]. Одна из них — алгебраическая конструкция Касами. Булева функция от n переменных рассматривается как функция над конечным полем $\mathrm{GF}(2^n)$. Любая булева функция f от n переменных может быть представлена с помощью функции *следа* $\mathrm{tr}(\beta) : \mathrm{GF}(2^n) \to \mathrm{GF}(2)$ следующим образом (см. подробнее [2]):

$$f(\beta) = \mathrm{tr}(\sum_{j=0}^{2^n-1} a_j \beta^j), \text{ где } a_j \in \mathrm{GF}(2^n), \text{ а } \mathrm{tr}(\beta) = \sum_{i=0}^{n-1} \beta^{2^i} \text{ для любого } \beta \in \mathrm{GF}(2^n).$$

Определение 1. Булева функция от n переменных (n чётное) вида $f(\beta) = \mathrm{tr}(\lambda\beta^k)$ называется *булевой функцией Касами*, если выполнено условие

1) $k = 2^{2d} - 2^d + 1$, где $(n, d) = 1,\ 0 < d < n$.

Если к тому же выполнено условие

2) λ не принадлежит множеству $\{\gamma^3 : \gamma \in \mathrm{GF}(2^n)\}$,

то f является бент-функцией и называется *бент-функцией Касами*.

[1]Исследование выполнено при поддержке гранта РФФИ, проект № 11-01-00997.