ки звучит так: существует ли алгоритм, определяющий по произвольным точкам $x_0, x_1 \in X$ принадлежность $x_1 \in f^*(x_0)$. Ограничимся рассмотрением только рациональных точек X по следующим соображениям. Кусочно-аффинное отображение $f(x) = 2x \pmod 1$ является хаотическим для почти всех $x \in X$. Но ни одно число этого множества почти всех из X не представимо на компьютере, если под числом не понимать алгоритм, его порождающий. Если же под числом понимать произвольный порождающий его алгоритм, проблема достижимости для $f(x)$ оказывается тривиально алгоритмически неразрешимой в общем случае, несмотря на то, что отображение очень простое. Стоит при этом заметить, что некоторые сопряжённые $f(x)$ отображения показывают хаотическое поведение на множестве рациональных точек.

Теорема 1. Если f строго эргодическое, т. е. имеет единственную инвариантную меру, или, другими словами, плотности распределения орбит всех точек совпадают, то проблема достижимости алгоритмически разрешима.

Следствие 1. Если пространство инвариантных мер конечномерно, то проблема достижимости алгоритмически разрешима.

ЛИТЕРАТУРА

1. *Savchenko A. Ya., Kovalev A. M., Kozlovskii V. A., and Scherbak V. F.* Inverse dynamical systems in secure communication and its discrete analogs for information transfer // Proc. NDES 2003, May 18–22, Scuol/Schuls, Switzerland. P. 112–116.
2. *Asarin E., Mysore V., Pnueli A., and Schneider G.* Low dimensional hybrid systems — decidable, undecidable, don't know // Inform. Comput. 2012. V. 211. P. 138–159.
3. *Kurganskyy O., Potapov I., and Sancho-Caparrini F.* Reachability problems in low-dimensional iterative maps // Int. J. Found. Comput. Sci. 2008. No. 19(4). P. 935–951.

УДК 519.7

О СТАТИСТИЧЕСКОЙ НЕЗАВИСИМОСТИ ПРОИЗВОЛЬНОЙ СУПЕРПОЗИЦИИ БУЛЕВЫХ ФУНКЦИЙ

О. Л. Мироненко

Доказаны достаточные условия статистической независимости суперпозиции произвольного числа булевых функций от подмножества своих аргументов.

Ключевые слова: *суперпозиция булевых функций, статистическая независимость от подмножества аргументов.*

Определение 1. Для любой булевой функции $f(x)$, где x — переменные со значениями в $\mathbb{Z}_2^n$, и для любого подмножества U её аргументов будем говорить, что $f(x)$ статистически не зависит от переменных множества U, если для любой её подфункции $f'(x')$, полученной фиксированием значений всех переменный в U, имеет место равенство $\Pr[f'(x') = 0] = \Pr[f(x) = 0]$.

В [1] доказано, что если булева функция $f_1(x)$ статистически не зависит от некоторого подмножества своих аргументов, то это свойство сохраняется для произвольной суперпозиции $g(f_1(x), y)$. Для суперпозиции $g(f_1(x), f_2(x), y)$ в [2] доказано более сложное достаточное условие сохранения статистической независимости: этим свойством, помимо f_1 и f_2, должна обладать и их сумма $f_1 \oplus f_2$. В данной работе условие из [2] обобщается на случай произвольного числа внутренних функций суперпозиции.

Утверждение 1. Пусть x, y, z — переменные со значениями в $\mathbb{Z}_2^n$, $\mathbb{Z}_2^m$ и $\mathbb{Z}_2^k$ соответственно и для всех $1 \leqslant s \leqslant l$ и $1 \leqslant i_1 < i_2 < \ldots < i_s \leqslant l$ функции $f_{i_1}(x, y) \oplus \ldots \oplus \oplus f_{i_s}(x, y)$ статистически не зависят от переменных в x. Тогда для любой функции g от $l + k$ переменных суперпозиция $g(f_1(x, y), \ldots, f_l(x, y), z)$ статистически не зависит от переменных в x.

Замечание 1. В ряде случаев (для конкретных функций g и ограничений на функции $f_1, \ldots, f_l$) можно сократить количество достаточных условий утверждения; этот вопрос составляет предмет дальнейших исследований.

ЛИТЕРАТУРА

1. *Колчева О. Л., Панкратова И. А.* О статистической независимости суперпозиции булевых функций // Прикладная дискретная математика. Приложение. 2011. № 4. С. 11–12.
2. *Колчева О. Л., Панкратова И. А.* О статистической независимости суперпозиции булевых функций. II // Прикладная дискретная математика. Приложение. 2012. № 5. С. 14–15.

УДК 519.7

ВЕРХНЯЯ ОЦЕНКА АЛГЕБРАИЧЕСКОЙ ИММУННОСТИ НЕКОТОРЫХ БЕНТ-ФУНКЦИЙ ДИЛЛОНА

С. Ю. Филюзин

Получена верхняя оценка алгебраической иммунности некоторых бент-функций Диллона. Приводится степень бент-функций максимальной алгебраической иммунности, предложенных З. Ту и Й. Денгом.

Ключевые слова: *булева функция, нелинейность, бент-функция, алгебраическая иммунность.*

Путём детального анализа успешных способов взлома блочных и поточных шифров были определены свойства булевой функции, которыми она должна обладать для использования её в криптографических приложениях. На данный момент остаётся открытым вопрос о том, как совмещаются различные криптографические свойства у одной булевой функции. Данная работа посвящена изучению алгебраической иммунности при максимальной нелинейности булевой функции.

Булева функция от n переменных представима единственным образом в виде *алгебраической нормальной формы* (АНФ): $f(x_1, \ldots, x_n) = (\bigoplus_{k=1}^{n} \bigoplus_{i_1,\ldots,i_k} a_{i_1,\ldots,i_k} x_{i_1} \cdot \ldots \cdot x_{i_k}) \bigoplus a_0$, где $a_0, a_i \in \mathbb{Z}_2$. *Степенью* $\deg(f)$ булевой функции f называется число переменных в самом длинном слагаемом её АНФ. *Алгебраической иммунностью* $\mathrm{AI}(f)$ булевой функции f называется минимальное целое число $d \geqslant 1$, такое, что существует булева функция g степени d, для которой выполняется равенство $fg = 0$ или $(f \oplus 1)g = 0$. *Нелинейностью* $\mathrm{nl}(f)$ булевой функции f от n переменных называется расстояние Хэмминга от данной функции до множества аффинных функций от n переменных. *Бент-функция* — булева функция от n переменных (n чётно), обладающая максимальной нелинейностью равной $2^{n-1} - 2^{(n/2)-1}$.

На сегодняшний день полная классификация бент-функций не произведена, но предложены способы построения таких функций. Функцию вида $g : \mathrm{GF}(2^k) \to \mathrm{GF}(2)$ будем рассматривать как булеву, зафиксировав некоторый базис в поле $\mathrm{GF}(2^k)$. В работе [1] Диллон приводит следующий способ построения бент-функций. Пусть