Заметим, что число бент-функций от $2k$ переменных на минимальном расстоянии от заданной бент-функции можно оценить сверху числом 2^{k^2+2k} (это оценка сверху числа всевозможных аффинных подпространств размерности k), а число бент-функций на минимальном расстоянии от квадратичной бент-функции асимптотически равно $C \cdot 2^{k(k+3)/2}$. Таким образом, число бент-функций на минимальном расстоянии от квадратичной бент-функции больше, чем корень из этой тривиальной верхней оценки.

ЛИТЕРАТУРА

1. *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. No. 20. P. 300–305.
2. *Коломеец Н. А., Павлов А. В.* Свойства бент-функций, находящихся на минимальном расстоянии друг от друга // Прикладная дискретная математика. 2009. № 4. С. 5–21.

УДК 519.7

О СТАТИСТИЧЕСКОЙ НЕЗАВИСИМОСТИ СУПЕРПОЗИЦИИ БУЛЕВЫХ ФУНКЦИЙ[1]

О. Л. Колчева, И. А. Панкратова

Интерес к статистической независимости булевой функции от подмножества аргументов возникает в связи с построением статистических аналогов функции [1], которые, в свою очередь, используются в линейном криптоанализе [2, 3].

Будем говорить, что булева функция f *статистически не зависит от подмножества* U *своих аргументов*, если для любой её подфункции f', полученной фиксированием значений всех переменных в U, имеет место $\Pr[f' = 1] = \Pr[f = 1]$; или, что то же самое, $\mathrm{w}(f') = \mathrm{w}(f)/2^{|U|}$, где $\mathrm{w}(f)$ — вес функции f. В частности, для статистического аналога $\varphi(x, y, k) = 0$ функции шифрования $F(x, k)$, где x, k, y — переменные со значениями в множествах открытых текстов, ключей и шифртекстов соответственно, условие статистической независимости функции $\varphi_F(x, k) = \varphi(x, F(x, k), k)$ от переменных в x является необходимым для того, чтобы вероятность выполнения уравнения $\varphi_F = 0$ сохранялась при подстановке в это уравнение любого значения x при равновероятном выборе k [1].

Требование статистической независимости функции от *конкретного* подмножества аргументов более слабое, чем условие корреляционной иммунности [4]: функция является корреляционно-иммунной порядка m, если и только если она статистически не зависит от *любого* m-элементного подмножества своих аргументов.

В [1] сформулирован тест статистической независимости: функция $f(x, y)$, где x, y — переменные со значениями в $(\mathbb{Z}_2)^n$ и $(\mathbb{Z}_2)^m$ соответственно, статистически не зависит от булевых переменных в x, если и только если $\hat{f}(u, 0^m) = 0$ для любого ненулевого вектора $u \in (\mathbb{Z}_2)^n$. Здесь $\hat{f}$ — преобразование Уолша — Адамара функции f; 0^m — m-компонентный нулевой вектор.

Сформулируем некоторые простейшие свойства статистической независимости.

1) Если функция имеет s линейных переменных, то она статистически не зависит от любого $(s-1)$-элементного подмножества своих аргументов.
2) Если функция статистически не зависит от U, то она статистически не зависит от любого подмножества U.

[1]Работа выполнена в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт № П1010).

3) Если функция f статистически не зависит от подмножества U своих аргументов, то $2^{|U|}|\mathrm{w}(f)$.
4) Пусть f_1, f_2, …, f_{2^m} — компоненты разложения функции f по некоторым m переменным, и все они статистически не зависят от подмножества U. Тогда и f статистически не зависит от U.

Основным результатом является следующее

Утверждение 1. Пусть x, y, z — переменные со значениями в $(\mathbb{Z}_2)^n$, $(\mathbb{Z}_2)^m$ и $(\mathbb{Z}_2)^l$ соответственно и функция $f(x,y)$ статистически не зависит от переменных в x. Тогда и функция $h(x,y,z) = g\left(f(x,y),z\right)$, где g — любая функция от $l+1$ переменных, статистически не зависит от переменных в x.

Доказательство. Воспользуемся тестом статистической независимости. Пусть u — любой ненулевой вектор из $\mathbb{Z}_2^n$; тогда по условию $\hat{f}(u,0^m)=0$. Вычислим коэффициент Уолша — Адамара функции h:

$$\hat{h}(u,0^m,0^l) = \sum_{x,y,z} (-1)^{g(f(x,y),z)\oplus(u,x)} = \sum_z \underbrace{\left(\sum_{\substack{x,y,\\ f(x,y)=0}} (-1)^{g(0,z)\oplus(u,x)} + \sum_{\substack{x,y,\\ f(x,y)=1}} (-1)^{g(1,z)\oplus(u,x)} \right)}_{A}.$$

Для каждого $z \in \mathbb{Z}_2^l$ имеет место один из следующих двух случаев:

1) $g(0,z) = g(1,z) = c \in \{0,1\}$, тогда $A = (-1)^c \sum\limits_{x,y} (-1)^{(u,x)} = 0$;

2) $g(0,z) = \overline{g(1,z)} = c \in \{0,1\}$, тогда $A = (-1)^c \left(\sum\limits_{\substack{x,y,\\ f(x,y)=0}} (-1)^{(u,x)} - \sum\limits_{\substack{x,y,\\ f(x,y)=1}} (-1)^{(u,x)} \right) =$
$= (-1)^c \sum\limits_{x,y} (-1)^{f(x,y)\oplus(u,x)} = (-1)^c \hat{f}(u,0^m) = 0.$

Таким образом, $\hat{h}(u,0^m,0^l)=0$, и утверждение доказано. ■

К сожалению, это утверждение не допускает обобщения на случай нескольких функций f; так, если функции $f_1(x,y)$, $f_2(x,y)$, …, $f_s(x,y)$ статистически не зависят от переменных в x, то функция $g(f_1(x,y), f_2(x,y), \ldots, f_s(x,y), z)$ не обязательно обладает этим свойством.

ЛИТЕРАТУРА

1. *Агибалов Г. П., Панкратова И. А.* Элементы теории статистических аналогов дискретных функций с применением в криптоанализе итеративных блочных шифров // Прикладная дискретная математика. 2010. № 3(9). С. 51–68.
2. *Matsui M.* Linear Cryptanalysis Method for DES Cipher // LNCS. 1993. V. 765. P. 386–397.
3. *Matsui M.* The First Experimental Cryptanalysis of the Data Encryption Standard // LNCS. 1994. V. 839. P. 1–11.
4. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004.