КІБЕРНЕТИКА

А.Н. АЛЕКСЕЙЧУК, С.Н. КОНЮШОК

УДК 519.7

# ОБ ЭФФЕКТИВНОСТИ МЕТОДА ВЕРОЯТНОСТНО НЕЙТРАЛЬНЫХ БИТОВ В СТАТИСТИЧЕСКОМ КРИПТОАНАЛИЗЕ СИНХРОННЫХ ПОТОЧНЫХ ШИФРОВ

**Аннотация.** Получены достижимые верхние границы для относительного расстояния между булевой функцией $f$ и ближайшей к ней функцией, не зависящей от переменных с номерами из заданного множества, а также между функцией $f$ и ее подфункцией, получаемой путем фиксации указанных переменных нулями. Выражения полученных границ зависят от метрических характеристик производных функции $f$, что позволяет применять эти границы для оценки и обоснования эффективности метода вероятностно нейтральных битов.

**Ключевые слова:** синхронный поточный шифр, статистический криптоанализ, метод вероятностно нейтральных битов, приближения булевых функций.

Метод вероятностно нейтральных битов [1, 2] предложен для построения статистических атак на синхронные поточные шифры и заключается в приближении булевых функций, связанных с алгоритмами шифрования, определенными функциями от меньшего числа переменных. Отметим, что аналогичные (а также более общие) приближения изучались в [3–9] и ряде других публикаций.

В [1, 2] предложено использовать в качестве приближений булевой функции $f = f(x_1, \ldots, x_n)$ ее подфункции, получаемые путем фиксации константами переменных $x_i$, для которых число единиц в векторе значений производной $D_i f = f(x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n) \oplus f(x_1, \ldots, x_{i-1}, x_i \oplus 1, x_{i+1}, \ldots, x_n)$ не превосходит заданного (небольшого) порога. На конкретных примерах показано, что эти приближения приводят к более эффективным по сравнению с полным перебором ключей атакам на редуцированные версии ряда синхронных поточных шифров, однако не исследована эффективность предложенного метода построения приближений в общем случае.

В настоящей статье получены достижимые верхние границы для относительного расстояния между булевой функцией $f$ и ближайшей к ней функцией, не зависящей от переменных с номерами из заданного множества, а также между функцией $f$ и ее приближениями, получаемыми методом вероятностно нейтральных битов [1, 2]. Выражения полученных границ позволяют установить числовые параметры производных функции $f$, от которых зависят указанные относительные расстояния, а также сформулировать условия, при которых метод вероятностно нейтральных битов приводит к приемлемым с практической точки зрения приближениям заданной функции.

Введем следующие обозначения:

$V_n$ — пространство двоичных векторов длины $n$;

$B_n = \{f \mid f: V_n \to \{0,1\}\}$ — множество булевых функций от $n$ переменных;

$\# M$ — мощность множества $M$;

$d(f,g) = 2^{-n} \# \{x \in V_n : f(x) \neq g(x)\}$ — относительное расстояние между функциями $f, g \in B_n$;

$wt(f) = 2^{-n} \# \{x \in V_n : f(x) = 1\}$ — относительный вес функции $f \in B_n$;

$d(f,U) = \min\limits_{g \in U} d(f,g)$ — относительное расстояние от функции $f \in B_n$ до множества $U \subseteq B_n$;

$\langle M \rangle$ — подпространство векторного пространства $V_n$, порожденное множеством $M \subseteq V_n$;

$H^{\perp}$ — подпространство, дуальное к векторному пространству $H \subseteq V_n$;

$\overline{a, b} = \{i \in \mathbf{Z} : a \leq i \leq b\}$, $a, b \in \mathbf{Z}$;

$\operatorname{supp}(x) = \{i \in \overline{1, n} : x_i = 1\}$ — носитель вектора $x = (x_1, \ldots, x_n) \in V_n$.

Производная функции $f \in B_n$ по направлению $\alpha \in V_n$ определяется по формуле $D_\alpha f(x) = f(x \oplus \alpha) \oplus f(x)$, $x \in V_n$. При этом число $wt(D_\alpha f)$ называется влиянием (influence) вектора $\alpha$ на функцию $f$.

Обозначим $e_1, \ldots, e_n$ стандартный базис пространства $V_n$ ($e_i$ — двоичный вектор длины $n$, все координаты которого, за исключением $i$-й, равны нулю, $i \in \overline{1, n}$). Запишем $D_i f$ вместо $D_{e_i} f$ и назовем число $wt(D_i f)$ влиянием $i$-й переменной на функцию $f \in B_n$. Согласно определению $f$ не зависит от $i$-й переменной, если $wt(D_i f) = 0$, $i \in \overline{1, n}$.

Для любого $k$-мерного подпространства $H$ векторного пространства $V_n$ обозначим $B_{n,k}(H)$ множество всех функций $g \in B_n$, допускающих представление в виде $g(x) = \varphi(xA)$, $x \in V_n$, где $\varphi \in B_k$, $A$ — $n \times k$-матрица, столбцы которой образуют базис подпространства $H$. Отметим, что если $H = \langle e_i : i \in \overline{1, n} \setminus J \rangle$, где $J \subset \overline{1, n}$, $\# J = n - k$, $k \in \overline{1, n-1}$, то множество $B_{n,k}(H)$ состоит из всех функций $g \in B_n$, не зависящих от переменных с номерами из множества $J$.

Следующая теорема устанавливает верхнюю границу относительного расстояния между булевой функцией $f$ и множеством $B_{n,k}(H)$.

**Теорема 1.** Пусть $f \in B_n$, $H$ — $k$-мерное подпространство векторного пространства $V_n$ и $\alpha_1, \ldots, \alpha_{n-k}$ — произвольный базис подпространства $H^{\perp}$, $k \in \overline{1, n-1}$. Тогда

$$d(f, B_{n,k}(H)) \leq \frac{1}{2} \sum_{i=1}^{n-k} wt(D_{\alpha_i} f). \tag{1}$$

**Доказательство.** Воспользуемся неравенством

$$d(f, B_{n,k}(H)) \leq 2^{-(n-k)} \sum_{\alpha \in H^{\perp}} wt(D_\alpha f),$$

вытекающим из формул (4), (9) и (13) в [9].

Заметим, что каждый вектор $\alpha \in H^{\perp}$ может быть однозначно записан в виде $\alpha = \alpha_{j_1} \oplus \cdots \oplus \alpha_{j_l}$, где $1 \leq j_1 < \ldots < j_l \leq n-k$, $l \in \overline{1, n-k}$. При этом

$$D_\alpha f(x) = \bigoplus_{i=1}^{l} (f(x \oplus \alpha_{j_1} \oplus \cdots \oplus \alpha_{j_i}) \oplus f(x \oplus \alpha_{j_1} \oplus \cdots \oplus \alpha_{j_{i-1}})).$$

Следовательно,

$$wt(D_\alpha f) \le \sum_{i=1}^{l} wt\,(f(x \oplus \alpha_{j_1} \oplus \cdots \oplus \alpha_{j_i}) \oplus f(x \oplus \alpha_{j_1} \oplus \cdots \oplus \alpha_{j_{i-1}})) =$$

$$= \sum_{i=1}^{l} wt\,(f(x \oplus \alpha_{j_i}) \oplus f(x)) = \sum_{i=1}^{l} wt\,(D_{\alpha_{j_i}} f)\,.$$

Таким образом, для любого $z = (z_1, \ldots, z_{n-k}) \in V_{n-k}$ справедливо неравенство $wt(D_{z_1\alpha_1 \oplus \cdots \oplus z_{n-k}\alpha_{n-k}} f) \le \sum_{i \in \mathrm{supp}(z)} wt(D_{\alpha_i} f)$. Отсюда находим

$$d(f, B_{n,k}(H)) \le 2^{-(n-k)} \sum_{\alpha \in H^\perp} wt(D_\alpha f) =$$

$$= 2^{-(n-k)} \sum_{(z_1, \ldots, z_{n-k}) \in V_{n-k}} wt(D_{z_1\alpha_1 \oplus \cdots \oplus z_{n-k}\alpha_{n-k}} f) \le$$

$$\le 2^{-(n-k)} \sum_{z \in V_{n-k}} \sum_{i \in \mathrm{supp}(z)} wt(D_{\alpha_i} f) = 2^{-(n-k)} \sum_{i=1}^{n-k} wt(D_{\alpha_i} f) \sum_{\substack{z \in V_{n-k}: \\ i \in \mathrm{supp}(z)}} 1 = \frac{1}{2} \sum_{i=1}^{n-k} wt(D_{\alpha_i} f)\,.$$

Теорема доказана.

Применяя теорему 1 к подпространству $H = \langle e_i : i \in \overline{1, n} \setminus J \rangle$, где $J \subset \overline{1, n}$, $J \ne \varnothing$, получаем следующий результат.

**Следствие.** Относительное расстояние между функцией $f \in B_n$ и ближайшей к ней функцией $g^*$, не зависящей от переменных с номерами из множества $J \subset \overline{1, n}$, $J \ne \varnothing$, не превосходит полусуммы влияний указанных переменных на функцию $f$:

$$d(f, g^*) \le \frac{1}{2} \sum_{i \in J} wt(D_i f)\,.$$

Отметим, что неравенство (1) представляет достижимую верхнюю границу параметра $d(f, B_{n,k}(H))$.

**Пример 1.** Пусть $f(x) = f(y, z) = z_1 g_1(y) \oplus \cdots \oplus z_{n-k} g_{n-k}(y)$, где $y = (y_1, \ldots, y_k) \in V_k$, $z = (z_1, \ldots, z_{n-k}) \in V_{n-k}$, $g_i \in B_k$, $wt(g_i) = w$, $0 < w(n-k) < 1$ и $g_i g_j = 0$ при $i \ne j$, $i, j \in \overline{1, n-k}$. Положим $H = \langle e_i : i \in \overline{1, k} \rangle$. Тогда $H^\perp = \langle e_i : i \in \overline{k+1, n} \rangle$ и выражение в правой части неравенства (1) имеет вид

$$\frac{1}{2} \sum_{i=k+1}^{n} wt(D_i f) = \frac{1}{2} \sum_{i=1}^{n-k} wt(g_i) = \frac{w(n-k)}{2}\,.$$

Далее, множество $B_{n,k}(H)$ состоит из всех функций $g \in B_n$ таких, что $g(y, z) = g(y, 0)$ для любых $y \in V_k$, $z \in V_{n-k}$, а сужение функции $f$ на каждое из множеств $\{(y, z) : z \in V_{n-k}\}$ является линейной функцией от $z$. При этом в силу условия $wt(g_i) = w$, $g_i g_j = 0$ при $i \ne j$, $i, j \in \overline{1, n-k}$, существует ровно $2^k w(n-k)$ векторов $y \in V_k$, для которых указанная линейная функция не равна тождественно нулю. Отсюда следует, что относительное расстояние между функцией $f$ и множеством $B_{n,k}(H)$ равно $2^{-n}(2^{n-k-1} \cdot 2^k w(n-k)) = \dfrac{w(n-k)}{2}$.

Получим теперь верхнюю границу относительного расстояния $d_k(f)$ между функцией $f \in B_n$ и ее приближением вида $f(y, 0)$, $y \in V_k$. Напомним, что именно такие приближения рассматриваются в [1, 2]; при этом фиксация последних $n-k$ переменных функции $f$ нулями (а не произвольными константами) не является принципиальным ограничением.

Введем ряд дополнительных обозначений. Для любого $z \in V_{n-k}$ обозначим $f(\cdot, z)$ подфункцию функции $f$, полученную путем фиксации ее последних $n-k$ переменных вектором $z$. Обозначим $e'_1, \ldots, e'_{n-k}$ стандартный базис векторного пространства $V_{n-k}$; для любого $A \subseteq \overline{1, n-k}$ положим $e'_A = \bigoplus_{i \in A} e'_i$. Наконец, обозначим $D_i f(\cdot, z)$ функцию на множестве $V_k$, принимающую в точке $y \in V_k$ значение $D_i f(y, z) = f(y, z \oplus e'_i) \oplus f(y, z)$, $i \in \overline{1, n-k}$. Отметим, что в силу определения параметра $d_k(f)$ справедливо равенство

$$d_k(f) = d(f, f(\cdot, 0)) = 2^{-(n-k)} \sum_{z \in V_{n-k}} d(f(\cdot, z), f(\cdot, 0)). \qquad (2)$$

**Лемма.** Пусть $z \in V_{n-k}$ — вектор с носителем $\operatorname{supp}(z) = A$ мощности $l \in \overline{1, n-k}$. Тогда

$$d(f(\cdot, z), f(\cdot, 0)) \le \sum_{i \in A} \sum_{j=1}^{l} \frac{(j-1)!(l-j)!}{l!} \sum_{\substack{B \subseteq A \setminus \{i\}: \\ \# B = j-1}} wt(D_i f(\cdot, e'_B)). \qquad (3)$$

**Доказательство.** Для простоты обозначений будем считать $A = \{1, 2, \ldots, l\}$; тогда для любой перестановки $(i_1, \ldots, i_l)$ элементов множества $A$ имеют место следующие соотношения:

$$d(f(\cdot, z), f(\cdot, 0)) = wt(f(\cdot, z) \oplus f(\cdot, 0)) = wt(f(\cdot, \bigoplus_{j=1}^{l} e'_{i_j}) \oplus f(\cdot, 0)) =$$

$$= wt\left( \bigoplus_{j=1}^{l} (f(\cdot, e'_{i_1} \oplus \cdots \oplus e'_{i_j}) \oplus f(\cdot, e'_{i_1} \oplus \cdots \oplus e'_{i_{j-1}})) \right) =$$

$$= wt\left( \bigoplus_{j=1}^{l} D_{i_j} f(\cdot, e'_{i_1} \oplus \cdots \oplus e'_{i_{j-1}}) \right) \le \sum_{j=1}^{l} wt(D_{i_j} f(\cdot, e'_{i_1} \oplus \cdots \oplus e'_{i_{j-1}})).$$

Суммируя указанные неравенства по всем перестановкам $(i_1, \ldots, i_l)$ элементов множества $A$, получаем

$$l! \cdot d(f(\cdot, z), f(\cdot, 0)) \le \sum_{j=1}^{l} \sum_{(i_1, \ldots, i_l)} wt(D_{i_j} f(\cdot, e'_{i_1} \oplus \cdots \oplus e'_{i_{j-1}})) =$$

$$\sum_{j=1}^{l} \sum_{i \in A} \sum_{\substack{B \subseteq A \setminus \{i\}: \\ \# B = j-1}} wt(D_i f(\cdot, e'_B)) \cdot \# \{(i_1, \ldots, i_l): i_j = i, \{i_1, \ldots, i_{j-1}\} = B\}.$$

Поскольку для любых $j \in \overline{1, l}$, $i \in A$ и $B \subseteq A \setminus \{i\}$, где $\# B = j-1$, существует ровно $(j-1)!(l-j)!$ перестановок $(i_1, \ldots, i_l)$ элементов множества $A$ таких, что $i_j = i$, $\{i_1, \ldots, i_{j-1}\} = B$, то из полученного неравенства следует формула (3).

Лемма доказана.

**Теорема 2.** Для любых $f \in B_n$, $k \in \overline{1, n-1}$ справедливы следующие неравенства:

$$d_k(f) \le \sum_{i=1}^{n-k} \frac{1}{n-k} \sum_{j=0}^{n-k-1} \left( 2^{-(n-k)} \sum_{l=j+1}^{n-k} \binom{n-k}{l} \right) w_{n-k,\,j}(D_i f) \le$$

$$\le \frac{1}{2} \sum_{i=1}^{n-k} \max_{0 \le j \le n-k-1} \{ w_{n-k,\,j}(D_i f) \}, \tag{4}$$

где

$$w_{n-k,\,j}(D_i f) = \binom{n-k-1}{j}^{-1} \sum_{\substack{B \subseteq \overline{1, n-k} \setminus \{i\}: \\ \# B = j}} wt(D_i f(\cdot, e'_B))$$

является относительным весом сужения функции $D_i f : V_n \to \{0, 1\}$ на множество

$$\{(y, z) : y \in V_k,\, z = (z_1, \ldots, z_{n-k}) \in V_{n-k},\, z_i = 0,\, \# \operatorname{supp}(z) = j\},\quad j \in \overline{0, n-k-1}.$$

**Доказательство.** На основании (2), (3) получаем, что

$$d_k(f) \le 2^{-(n-k)} \sum_{l=1}^{n-k} \sum_{\substack{A \subseteq \overline{1, n-k}: \\ \# A = l}} \sum_{i \in A} \sum_{j=1}^{l} \frac{(j-1)!(l-j)!}{l!} \sum_{\substack{B \subseteq A \setminus \{i\}: \\ \# B = j-1}} wt(D_i f(\cdot, e'_B)) =$$

$$= 2^{-(n-k)} \sum_{i=1}^{n-k} \sum_{l=1}^{n-k} \sum_{j=1}^{l} \frac{(j-1)!(l-j)!}{l!} \sum_{\substack{B \subseteq \overline{1, n-k} \setminus \{i\}: \\ \# B = j-1}} wt(D_i f(\cdot, e'_B)) \times$$

$$\times \# \{A \subseteq \overline{1, n-k} : A \supseteq B \cup \{i\},\ \# A = l\}.$$

Поскольку для любых $B \subseteq \overline{1, n-k}$, $i \in \overline{1, n-k}$ таких, что $i \notin B$, $\# B = j-1$ существует ровно $\binom{n-k-j}{l-j}$ множеств $A \subseteq \overline{1, n-k}$, удовлетворяющих условию $A \supseteq B \cup \{i\}, \# A = l$, то

$$d_k(f) \le 2^{-(n-k)} \sum_{i=1}^{n-k} \sum_{l=1}^{n-k} \sum_{j=1}^{l} \sum_{\substack{B \subseteq \overline{1, n-k} \setminus \{i\}: \\ \# B = j-1}} wt(D_i f(\cdot, e'_B)) \times$$

$$\times \frac{(j-1)!(l-j)!}{l!} \frac{(n-k-j)!}{(l-j)!(n-k-l)!} =$$

$$= 2^{-(n-k)} \sum_{i=1}^{n-k} \sum_{l=1}^{n-k} \sum_{j=1}^{l} \sum_{\substack{B \subseteq \overline{1, n-k} \setminus \{i\}: \\ \# B = j-1}} wt(D_i f(\cdot, e'_B)) \binom{n-k-1}{j-1}^{-1} \frac{1}{n-k} \binom{n-k}{l} =$$

$$= 2^{-(n-k)} \sum_{i=1}^{n-k} \frac{1}{n-k} \sum_{l=1}^{n-k} \binom{n-k}{l} \sum_{j=0}^{l-1} \binom{n-k-1}{j}^{-1} \sum_{\substack{B \subseteq \overline{1, n-k} \setminus \{i\}: \\ \# B = j}} wt(D_i f(\cdot, e'_B)) =$$

$$=\sum_{i=1}^{n-k}\frac{1}{n-k}\sum_{j=0}^{n-k-1}\left(2^{-(n-k)}\sum_{l=j+1}^{n-k}\binom{n-k}{l}\right)\left(\binom{n-k-1}{j}^{-1}\sum_{\substack{B\subseteq\overline{1,\,n-k}\setminus\{i\}:\\ \#B=j}} wt(D_i f(\cdot,\, e'_B))\right)=$$

$$=\sum_{i=1}^{n-k}\frac{1}{n-k}\sum_{j=0}^{n-k-1}\left(2^{-(n-k)}\sum_{l=j+1}^{n-k}\binom{n-k}{l}\right)w_{n-k,\,j}(D_i f)\,.$$

Наконец, остается заметить, что последнее выражение не превосходит

$$\sum_{i=1}^{n-k}\left(\frac{1}{n-k}\sum_{j=0}^{n-k-1}2^{-(n-k)}\sum_{l=j+1}^{n-k}\binom{n-k}{l}\right)\max_{0\le j\le n-k-1}\{w_{n-k,\,j}(D_i f)\}=$$

$$=\sum_{i=1}^{n-k}\left(\frac{1}{n-k}\sum_{l=1}^{n-k}2^{-(n-k)}\binom{n-k}{l}l\right)\max_{0\le j\le n-k-1}\{w_{n-k,\,j}(D_i f)\}=$$

$$=\frac{1}{2}\sum_{i=1}^{n-k}\max_{0\le j\le n-k-1}\{w_{n-k,\,j}(D_i f)\}\,.$$

Теорема доказана.

Отметим, что неравенство (4) представляет достижимую верхнюю границу параметра $d_k(f)$.

**Пример 2.** Рассмотрим функцию $f$ из примера 1. Поскольку ее производная $D_i f(y,z)=f(y,z\oplus e'_i)\oplus f(y,z)=g_i(y)$, $y\in V_k$, $z\in V_{n-k}$, не зависит от $z$, то $w_{n-k,\,j}(D_i f)=wt(g_i)=w$ для любых $i\in\overline{1,\,n-k}$, $j\in\overline{0,\,n-k-1}$. При этом согласно равенству (2)

$$d_k(f)=2^{-(n-k)}\sum_{z\in V_{n-k}} wt(z_1 g_1(\cdot)\oplus\cdots\oplus z_{n-k}g_{n-k}(\cdot))=$$

$$=2^{-(n-k)}\sum_{l=1}^{n-k}\sum_{1\le i_1<\ldots<i_l\le n-k} wt(g_{i_1}\oplus\cdots\oplus g_{i_l})=2^{-(n-k)}\sum_{l=1}^{n-k}\binom{n-k}{l}wl=\frac{(n-k)w}{2}\,.$$

Таким образом, неравенство (4) обращается в равенство.

Сравним значения параметров в правых частях неравенств (4) и (1) (при $H=\langle e_i : i\in\overline{1,\,k}\rangle$). Согласно следствию из теоремы 1 относительное расстояние между функцией $f\in B_n$ и ближайшей к ней функцией, не зависящей от последних $n-k$ переменных, ограничено сверху значением $\frac{1}{2}\sum_{i=k+1}^{n} wt(D_i f)$, в то время как расстояние от $f$ до одной из указанных функций (а именно $f(y,0)$, $y\in V_k$) ограничено сверху значением $\frac{1}{2}\sum_{i=1}^{n-k}\max_{0\le j\le n-k-1}\{w_{n-k,\,j}(D_i f)\}$, которое не меньше первого.

Действительно, поскольку для любого $i\in\overline{k+1,\,n}$

$$wt(D_i f)=2^{-(n-k-1)}\sum_{j=0}^{n-k-1}\sum_{\substack{B\subseteq\overline{1,\,n-k}\setminus\{i\}:\\ \#B=j}} wt(D_i f(\cdot,\, e'_B))=$$

$$= 2^{-(n-k-1)} \sum_{j=0}^{n-k-1} \left( \binom{n-k-1}{j}^{-1} \sum_{\substack{B \subseteq \overline{1,\, n-k} \setminus \{i\}: \\ \# B = j}} wt(D_i f(\cdot,\, e'_B)) \right) \binom{n-k-1}{j} \le$$

$$\le 2^{-(n-k-1)} \max_{0 \le j \le n-k-1} \{ w_{n-k,\, j}(D_i f) \} \sum_{j=0}^{n-k-1} \binom{n-k-1}{j} = \max_{0 \le j \le n-k-1} \{ w_{n-k,\, j}(D_i f) \},$$

то

$$\frac{1}{2} \sum_{i=k+1}^{n} wt(D_i f) \le \frac{1}{2} \sum_{i=1}^{n-k} \max_{0 \le j \le n-k-1} \{ w_{n-k,\, j}(D_i f) \},$$

что и требовалось доказать.

Как показывает следующий пример, приближения, получаемые методом вероятностно нейтральных битов, могут быть далеки от наилучших.

**Пример 3.** Рассмотрим функцию: $f(y, z) = 0$, если $z = 0$; $f(y, z) = 1$ — в противном случае, $y \in V_k$, $z \in V_{n-k}$. Нетрудно видеть, что влияние на функцию $f$ каждой из последних $n-k$ переменных равно $2^{k-n+1}$. При этом относительное расстояние между функциями $f$ и $f(y, 0)$, $y \in V_k$, равно $wt(f) = 1 - 2^{k-n}$, в то время как относительное расстояние между функцией $f$ и ближайшей к ней функцией, не зависящей от последних $n-k$ переменных, равно $1 - wt(f) = 2^{k-n}$.

В целом полученные результаты показывают, что при построении приближений функции $f \in B_n$ методом вероятностно нейтральных битов следует ориентироваться не столько на влияния отдельных неизвестных (параметры $wt(D_i f)$, $i \in \overline{k+1,\, n}$), сколько на значения параметров $\max\limits_{0 \le j \le n-k-1} \{ w_{n-k,\, j}(D_i f) \}$, определенных в теореме 2. Эти значения могут совпадать с $wt(D_i f)$ (см. примеры 1, 2), но могут быть и заметно больше последних (см. пример 3).

По-видимому, лучшие приближения функции $f$ можно получить, присваивая ее $n-k$ переменным с малыми влияниями случайные (а не заранее фиксированные, например, нулевые) значения. Указанную идею можно обобщить, рассматривая в качестве приближений функции $f$ ее сужения на случайно выбранные смежные классы по некоторому $k$-мерному подпространству векторного пространства $V_n$, однако развитие этого подхода требует отдельного исследования.

СПИСОК ЛИТЕРАТУРЫ


1. Aumasson J.-Ph. New features of latin dances: Analysis of Salsa, ChaCha, and Rumba / J.-Ph. Aumasson, S. Fischer, S. Khazaei, W. Meier, C. Rechberger // Fast Softvare Encryption — FSE 2008, Proceedings. — Berlin: Springer-Verlag, 2008. — P. 470–488.
2. Fischer S. Chosen IV statistical analysis for key recovery attacks on stream ciphers / S. Fischer, S. Khazaei, W. Meier // AFRICACRYPT 2008, Proceedings. — Berlin: Springer-Verlag, 2008. — P. 236–245.
3. Dawson E., Wu C.K. Construction of correlation immune Boolean functions // Information and Communication Security, Proceedings. — Berlin: Springer-Verlag, 1997. — P. 170–180.
4. Friedgut E. Boolean functions with low average sensitivity depend of few coordinates // Combinatorica. — 1998. — **18**, N 1. — P. 27–35.
5. Canteaut A., Trabbia M. Improved fast correlation attacks using parity-check equations of weight 4 and 5 // Advances in Cryptology — EUROCRYPT'00, Proceedings. — Berlin: Springer-Verlag, 2000. — P. 573–588.

6. Canteaut A. On the correlations between a combining function and function of fewer variables // The 2002 IEEE Information Theory Workshop, Proceedings. — Berlin: Springer-Verlag, 2002. — P. 78–81.
7. Gopalan P., O'Donnel R., Servedio A., Shpilka A., Wimmer K. Testing Fourier dimensionality and sparsity // SIAM J. on Computing. — 2011. — **40**, N 4. — P. 1075–1100.
8. Алексеев Е.К. О некоторых мерах нелинейности булевых функций // Прикладная дискретная математика. — 2011. — **12**, № 2. — С. 5–16.
9. Алексейчук А.Н., Конюшок С.Н. Алгебраически вырожденные приближения булевых функций // Кибернетика и системный анализ. — 2014. — **50**, № 6. — С. 3–14.

*Надійшла до редакції 03.12.2015*

**А.М. Олексійчук, С.М. Конюшок**

**ПРО ЕФЕКТИВНІСТЬ МЕТОДУ ЙМОВІРНІСНО НЕЙТРАЛЬНИХ БІТІВ У СТАТИСТИЧНОМУ КРИПТОАНАЛІЗІ СИНХРОННИХ ПОТОКОВИХ ШИФРІВ**

**Анотація.** Отримано досяжні верхні межі відносної відстані між булевою функцією $f$ та найближчою до неї функцією, що не залежить від змінних з номерами із заданої множини, а також між функцією $f$ та її підфункцією, яка отримується шляхом фіксації зазначених змінних нулями. Вирази отриманих меж залежать від метричних характеристик похідних функції $f$, що дозволяє застосовувати ці межі для оцінювання та обгрунтування ефективності методу ймовірнісно нейтральних бітів.

**Ключові слова:** синхронний потоковий шифр, статистичний криптоаналіз, метод ймовірнісно нейтральних бітів, наближення булевих функцій.

**A.N. Alekseychuk, S.N. Konyushok**

**EFFECTIVENESS OF PROBABILISTIC NEUTRAL BITS METHOD IN STATISTICAL CRYPTANALYSIS OF SYNCHRONOUS STREAM CIPHERS**

**Abstract.** In this paper, we obtain two achievable upper bounds. The first bound estimates the relative distance between a Boolean function $f$ and the nearest to it function that is independent of the variables in a given set. The second bound estimates the relative distance between the function $f$ and its sub-functions, obtained by stating the above-mentioned variables at zeros. The expressions of the derived bounds depend on some metric characteristics of derivatives of the function $f$. This fact allows us to use these bounds to evaluate and prove the effectiveness of probabilistic neutral bits method.

**Keywords:** synchronous stream cipher, statistical cryptanalysis, method of probabilistic neutral bits, approximations of Boolean functions.

**Алексейчук Антон Николаевич,**
доктор техн. наук, доцент, профессор Института специальной связи и защиты информации НТУУ «КПИ», Киев, e-mail: alex-dtn@ukr.net.

**Конюшок Сергей Николаевич,**
кандидат техн. наук, доцент, заместитель начальника Института специальной связи и защиты информации НТУУ «КПИ», Киев, e-mail: 3tooth@mail.ru.