Н. В. Никонов (Москва, ТВП). **О существовании запретов у равновероятных пороговых функций k-значной логики.**

Представленный доклад посвящен изучению классов функций k-значной логики $\Phi_n^k = \{f^k(x_1, x_2, \ldots, x_n) | x_1, x_n$ — существенные, $k \geqslant 3\}$ с запретами — комбинациями знаков $\gamma_1, \gamma_2, \ldots, \gamma_N$ на выходе фильтрующего генератора ([1]), при которых система уравнений вида $f^k(x_{1+i}, x_{2+i}, \ldots, x_{n+i}) = \gamma_{1+i}$, $i = 0, 1, \ldots, N-1$, несовместна (см. [2]). В работах [2–4] указываются классы булевых равновероятных функций с запретами. В докладе результат работы [4] обобщается на случай k-значной логики.

Напомним ([5]), что функция $\pi^k(x_1, x_2, \ldots, x_n) \in \Phi_n^k$ называется *пороговой*, если существует такая линейная форма $L(x_1, x_2, \ldots, x_n) = a_1x_1 + a_2x_2 + \cdots + a_nx_n$, $a_i \in \mathbf{R}$, что для любого $\alpha \in \{0, 1, \ldots, k-1\}$ верно

$$\pi^k(x_1, x_2, \ldots, x_n) = \alpha \Leftrightarrow b_\alpha \leqslant L(x_1, x_2, \ldots, x_n) < b_{\alpha+1}, \quad b_0, b_1, \ldots, b_k \in \mathbf{R}.$$

Введем обозначение для весов подфункций, полученных из исходной функции фиксацией одной существенной переменной x_i: $|\{(x_1, x_2, \ldots, x_n) \,|\, \pi^k(x_1, x_2, \ldots, x_n) = \gamma,\ x_i = \varepsilon_j\}| = \omega_\gamma\binom{\varepsilon_j}{i}$, $\gamma, \varepsilon_j \in \{0, 1, \ldots, k-1\}$.

Из работы [5] известно, что любая пороговая функция k-значной логики является полностью монотонной, в частности, 1-монотонной, что позволяет доказать следующую вспомогательную лемму.

Лемма. *Если у равновероятной пороговой функции $\pi^k(x_1, x_2, \ldots, x_n) \in \Phi_n^k$ для любого знака $\gamma \in \{0, 1, \ldots, k-1\}$ при всевозможных фиксациях одной переменной $x_i \in \{0, 1, \ldots, k-1\}$ верно $\omega_\gamma\binom{0}{i} = \omega_\gamma\binom{1}{i} = \cdots = \omega_\gamma\binom{k-1}{i}$, то функция $\pi^k(\mathbf{x})$ от переменной x_i существенно не зависит.*

Следствие. *Для переменных x_1, x_n равновероятной пороговой функции $\pi^k(x_1, x_2, \ldots, x_n) \in \Phi_n^k$ найдутся такие значения γ' и γ, соответственно, что*

$$\omega_{\gamma'}\binom{0}{1} \geqslant \omega_{\gamma'}\binom{1}{1} \geqslant \cdots \geqslant \omega_{\gamma'}\binom{k-1}{1}, \quad \omega_\gamma\binom{0}{1} \geqslant \omega_\gamma\binom{1}{1} \geqslant \cdots \geqslant \omega_\gamma\binom{k-1}{1}, \qquad (1)$$

причем в каждой цепочке неравенств хотя бы одно строгое.

Обратимся к основному результату работы.

Теорема. *Любая равновероятная пороговая функция $\pi^k(x_1, x_2, \ldots, x_n)$ имеет запрет.*

Логика доказательства повторяет рассуждения работы [4]. Рассмотрим вероятность появления n-грамм вида $\overbrace{\gamma \quad \gamma'}^{n}$ при равномерном входе, где знаки $\gamma, \gamma' \in \{0, 1, \ldots, k-1\}$ удовлетворяют (1):

$$\begin{aligned}
P\left\{\overbrace{\gamma \quad \gamma'}^{n}\right\} &= \frac{1}{k}\Big[\mathbf{P}\left\{\pi^k = \gamma \,|\, x_n = 0\right\}\mathbf{P}\left\{\pi^k = \gamma' \,|\, x_1' = x_n = 0\right\} \\
&\quad + \mathbf{P}\left\{\pi^k = \gamma \,|\, x_n = 1\right\}\mathbf{P}\left\{\pi^k = \gamma' \,|\, x_1' = x_n = 1\right\} + \cdots \\
&\quad + \mathbf{P}\left\{\pi^k = \gamma \,|\, x_n = k-1\right\}\mathbf{P}\left\{\pi^k = \gamma' \,|\, x_1' = x_n = k-1\right\}\Big] \\
&= \frac{1}{k}\left[\left(\frac{1}{k} + \delta_n^0\right)\left(\frac{1}{k} + \delta_1^0\right) + \left(\frac{1}{k} + \delta_n^1\right)\left(\frac{1}{k} + \delta_1^1\right) + \cdots\right. \\
&\quad \left. + \left(\frac{1}{k} + \delta_n^{k-1}\right)\left(\frac{1}{k} + \delta_1^{k-1}\right)\right] = \frac{1}{k}\left[\frac{1}{k} + \sum_{i=0}^{k-1}\delta_1^i\delta_n^i\right],
\end{aligned}$$

причем в силу условий (1) не все δ_1^i, δ_n^i, $i = 0, 1, \ldots, k-1$, равны 0; $\delta_1^0 \geqslant \delta_1^1 \geqslant \cdots \delta_1^{k-1}$, $\delta_n^0 \geqslant \delta_n^1 \geqslant \cdots \delta_n^{k-1}$, и в этих цепочках есть хотя бы одно строгое. Теперь для обнаружения у функции $\pi^k(\mathbf{x})$ некоторой неравномерно распределенной n-граммы вида

$\gamma, \gamma_2, \ldots, \gamma_{n-1}, \gamma'$ (что будет, согласно [2], гарантировать существование запрета у функции $\pi^k(\mathbf{x})$), достаточно заметить, что $\sum_{i=0}^{k-1} \delta_1^i \delta_n^i > 0$.

Работа выполнена при поддержке гранта Президента РФ (НШ-8.2010.10).

СПИСОК ЛИТЕРАТУРЫ

1. Словарь криптографических терминов./ Под ред. Б. А. Погорелова, В. Н. Сачкова. М.: МЦНМО, 2006, 94 с.
2. *Сумароков С. Н.* Запреты двоичных функций и обратимость для одного класса кодирующих устройств. — Обозрение прикл. и промышл. матем., 1994, т. 1, в. 1, с. 33–55.
3. *Рожков М. И.* Некоторые алгоритмические вопросы идентификации конечных автоматов по распределению выходных m-грамм. Ч. II. — Обозрение прикл. и промышл. матем., 2008, т. 15, в. 5, с. 785–806.
4. *Никонов Н. В.* О существовании запрета у пороговой функции. — Обозрение прикл. и промышл. матем., 2009, т. 16, в. 1, с. 162–164.
5. *Никонов В. Г.*, *Никонов Н. В.* Особенности пороговых представлений k-значных функций. — Труды по дискретн. матем., 2008, т. 11, в. 1.