Н. В. Никонов (Москва, ТВП). **О построении классов k-значных функций с обобщенными полузапретами при помощи пороговых методов.**

В докладе рассматривается фильтрующий генератор [1], [2] в случае, когда информация с регистра сдвига поступает на функцию $f^k(\vec{x})$ с ячеек, расположенных на некоторых расстояниях $l_1, \ldots, l_{n-1}$. Данная постановка приводит к появлению понятия *обобщенного запрета* функции

$$\gamma_{j_1} \overbrace{\qquad}^{\Phi_1(\vec{l})} \gamma_{j_2} \overbrace{\qquad}^{\Phi_2(\vec{l})} \gamma_{j_3} \ldots \gamma_{j_{S-1}} \overbrace{\qquad}^{\Phi_{S-1}(\vec{l})} \gamma_{j_S}, \tag{1}$$

в котором знаки $\gamma_{j_i} \in \{0, \ldots, k-1\}$, $i = 1, \ldots, S$, располагаются на расстояниях, являющихся функциями $\Phi_t(\vec{l}) = \Phi_t(l_1, \ldots, l_{n-1})$, $t = 1, \ldots, S-1$, принимающими натуральные значения. При этом системы

$$F^k_{\vec{l}}(x_{1+\psi_{i-1}(\vec{l})}, \ldots, x_{m+\psi_{i-1}(\vec{l})}) = \gamma_{j_i}, \qquad i = 1, \ldots, S, \tag{2}$$

где $F^k_{\vec{l}}(x_1, \ldots, x_m) = f^k(x_1, x_{1+l_1}, x_{1+l_1+l_2}, \ldots, x_m)$, $m = 1 + \sum_{r=1}^{n-1} l_r$, $\psi_t(\vec{l}) = \sum_{u=1}^{t} \Psi_u(\vec{l})$, $t = 1, \ldots, S-1$, $\psi_0(\vec{l}) = 0$, при любой фиксации $\vec{l}$ являются несовместными (см. [3]). Пусть все системы вида (2) являются совместными и существует хотя бы одно такое неизвестное x_s, $s = 1, \ldots, T(\vec{l})$, в каждой из систем вида (2) с $T(\vec{l})$ неизвестными, что $x_s \in \Omega_s(\vec{l}) \subset \{0, \ldots, k-1\}$. Комбинация (1) называется *обобщенным полузапретом I рода*, если $|\Omega_s(\vec{l})| = 1$, и *II рода*, если $|\Omega_s(\vec{l})| < k$ с эффективностью

$$e_0 = \min_{\vec{l} \in \mathbf{N}^{n-1}} \frac{1}{S} \left\{ T(\vec{l}) - \log_k \prod_{s=1}^{T(\vec{l})} |\Omega_s(\vec{l})| \right\}.$$

В связи со сложностью задачи поиска обобщенного запрета и полузапрета в общем виде у произвольной функции, представляет интерес изучение конкретных классов функций k-значной логики с известными обобщенными запретами и полузапретами. В работе [3] предлагается *метод растяжения* для построения таких классов, исходя из булевого случая, заключающийся в погружении исходной булевой системы вида (2) в некоторую систему линейных неравенств

$$a^{(j)}_1 x_1 + \cdots + a^{(j)}_{m+\psi_{S-1}(\vec{l})} x_{m+\psi_{S-1}(\vec{l})} \geqslant \varepsilon^{(j)}, \qquad j = 1, \ldots, M, \tag{3}$$

с параметрами $\varepsilon^{(j)} \in [0, 1]$ ([4]). Для системы (3) факт ее несовместности, заключающейся в существовании противоречивого неравенства-следствия, означает наличие у булевой функции $f(\vec{x})$ обобщенного запрета, который при методе растяжения переходит в k-значный обобщенный запрет с теми же функциями $\Phi_t(\vec{l})$ для класса k-значных функций, включая равновероятные ([5]).

Получение нетривиальных оценок отдельных неизвестных системы (3) свидетельствует о наличии обобщенного полузапрета у функции $f(\vec{x})$. В случае, если полученные оценки противоречивы, доказывается существование у функции обобщенного запрета ([5]). Однако в этом случае при переходе в k-значную область обобщенный запрет может трансформироваться как в обобщенный запрет, так и полузапрет I или II рода. Поясним это замечание, рассмотрев частный случай таких доказательств, при котором формируется совокупность двух условий

$$ax_s \geqslant \sum_{j=1}^{m} c^{(j)} \varepsilon^{(j)} - A, \quad -bx_s \geqslant \sum_{j=1}^{m} d^{(j)} \varepsilon^{(j)} - B, \tag{4}$$

где $a, b, A, B, c^{(j)}, d^{(j)} \in \mathbf{N}$, $j = 1, \ldots, M$. Совокупность (4) дает противоречивые оценки неизвестной x_s системы (3), исходя из ее булевой принадлежности при выполнении некоторых ограничений, налагаемых на $\varepsilon^{(j)}$, переходящих при методе растяжения в условия, при которых

$$x_s \in \Omega = \left\{ \left\lceil \frac{1}{a} \sum_{j=1}^{M} c^{(j)} \delta^{(j)} - \frac{A}{a}(k-1) \right\rceil, \ldots, \left\lfloor \frac{B}{b}(k-1) - \frac{1}{b} \sum_{j=1}^{m} d^{(j)} \delta^{(j)} \right\rfloor \right\} \subset \{0, \ldots, k-1\},$$

$\delta^{(j)} \in \{0, \ldots, k-1\}$. Неизвестное $x_s \neq 0, k-1$, что говорит о наличии у класса функций k-значной логики обобщенного полузапрета II рода. При определенном выборе параметров $\delta^{(j)}$, $|\Omega| = 1$ либо $|\Omega| = 0$, что будет свидетельствовать о том, что комбинация вида (1) станет обобщенным полузапретом I рода, либо останется обобщенным запретом. При изучении построенного класса функций k-значной логики представляет интерес рассмотрение зависимости мощности класса, определяемой параметрами $\delta^{(j)}$, и эффективностей найденных у него обобщенных полузапретов.

Работа выполнена при поддержке гранта Президента РФ (НШ–4.2008.10).

СПИСОК ЛИТЕРАТУРЫ

1. *Golic J. D.* On the Security of Nonlinear Filter Generators. — In: Fast Software Encryption, FSE'96 / D. Gollmann (Ed.). Berlin, Heidelberg: Springer–Verlag, 1996. LNCS.1039.
2. *Сумароков С. Н.* Запреты двоичных функций и обратимость для одного класса кодирующих устройств. —Обозрение прикл. и промышл. матем., 1994, т. 1, в. 1.
3. *Никонов Н. В.* Метод растяжения в построении классов равновероятных k-значных функций с запретом. — Обозрение прикл. и промышл. матем., 2006, т. 13, в. 6.
4. *Балакин Г. В.*, *Никонов В. Г.* Методы сведения булевых уравнений к системам пороговых соотношений. — Обозрение прикл. и промышл. матем., 1994, т. 1, в. 3.
5. *Никонов Н. В.* О пороговых методах доказательства наличия запретов булевых и k-значных функций. — Обозрение прикл. и промышл. матем., 2006, т. 13, в. 5.