О ЗАПРЕТАХ БУЛЕВЫХ ФУНКЦИЙ

К.Л. Глуско, Т.С. Носачева, А.Ю. Рожнев, С.С. Титов

Уральский государственный университет путей сообщения, Колмогорова 66, 620034, Екатеринбург, Россия
alexon@k66.ru

В работе исследованы булевы функции на наличие или отсутствие запрета. В криптоанализе запрет является одной из важных характеристик булевой функции [1]. В результате проделанной работы были проанализированы булевы функции двух, трех и четырех переменных. Предложен критерий отсутствия запрета функции.

Среди функций двух переменных функций с запретом нет. Для функций трех переменных справедливо утверждение: нелинейные по крайним переменным уравновешенные булевы функции трех переменных имеют запрет. В качестве примера рассмотрена функция majority [3], которая имеет вид

$$f(x_1, x_2, x_3) = x_1x_2 + x_2x_3 + x_1x_3. \quad (1)$$

Интересна она тем, что применяется в стандарте связи GSM в системе шифрования A5/1 [2] в блоке нелинейного усложнения "Stop and Go" мобильных телефонов. В книге [2] приведена критика системы шифрования A5/1. Нахождение запрета у функции majority выявляет еще одну криптографическую слабость алгоритма A5/1.

Заметим также, что в [1, с. 425] в качестве задачи 9.67 предложено доказать, что функция

$$f(x_1, x_2, x_3, x_4) = 1 + x_1 + x_3 + x_1x_2 + x_2x_4 + x_1x_2x_4 \quad (2)$$

не имеет запрета. Но оказалось, что функция не сильно равновероятна. Значит, она имеет запрет. При проверке данной функции на запрет длины 6, оказалось что он существует, и имеет вид 001111. Видимо, в условие задачи вкралась опечатка.

Необходимо отметить, что если в данной функции заменить несущественный член 1, а также добавить существенную переменную x_2, то функция примет вид

$$f(x_1, x_2, x_3, x_4) = x_1 + x_2 + x_3 + x_1x_2 + x_2x_4 + x_1x_2x_4. \quad (3)$$

Данная функция сильно равновероятна, а также сильно уравновешена при $l = 2$, причем это подходит для системы уравнений любой длины. Таким образом доказано, что данная функция не имеет запрета. Теперь можно сказать, что для того, чтобы доказать сильную уравновешенность (т.е. отсутствие запрета) необходимо анализировать не всю систему уравнений, а только два последних уравнения.

Таким образом, если свойство сильной уравновешенности выполняется для первых трех уравнений системы, то оно будет выполняться для системы любой длины. Это следует из того, что для доказательства сильной уравновешенности нас интересуют только два последних уравнения.

Утверждение. *Сильная уравновешенность при $l = 2$ влечет за собой отсутствие запрета (т. е. сильную уравновешенность для любого l), если это выполняется для $n = 3$.*

Литература

1. *Логачев О.А., Сальников А.А., Ященко В.В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004. 470 с.

2. *Асосков А.В., Иванов М.А., Мирский А.А., Рузин А.В., Сланин А.В., Тютвин А.Н.* Поточные шифры. М.: КУДИЦ-ОБРАЗ, 2003. 336 с.

3. *Глуско Кр.Л., Рожнев А.Ю., Титов С.С.* О запретах булевой функции Majority // Сборник научных трудов конференции «Молодежь — будущее атомной промышленности России». Снежинск: СГФТА, 2007. С. 82–86.