ИССЛЕДОВАНИЕ КОРРЕЛЯЦИОННОЙ ИММУННОСТИ БУЛЕВЫХ ФУНКЦИЙ СЛЕДА

М. Н. Кондратюк

Аннотация: Булевы функции широко используются в криптографии для различных целей, например, для комбинирования значений нескольких генераторов псевдослучайных последовательностей или для конструирования *S*-блоков. В работе рассматриваются булевы функции следа и проверяются свойства корреляционной иммунности данных конструкций.

Пусть F_{2^n} – поле из 2^n элементов, расширение поля $F_2 = \{0,1\}$. Через V_n обозначим *n*-мерное векторное пространство над полем F_2, через $w(a)$ – вес Хэмминга вектора a (число ненулевых координат), а через $< a,b >$ – скалярное произведение векторов $a,b \in V_n$.

Говорят [1], что булева функция $f : V_n \to F_2$ удовлетворяет *критерию корреляционной иммунности* порядка *k* (обозначают CI(*k*)), если для случайного вектора x с равномерным распределением на V_n выполняется:

$$P\{f(x) =< a,x >\} = \frac{1}{2}$$

при любом $a \in V_n$, $1 \le w(a) \le k$.

Функция f может быть задана таблицей истинности, т. е. своими значениями $s_0, s_1, ..., s_{2^n-1}$ на лексикографически упорядоченных векторах V_n.

В данной работе рассматривается корреляционная иммунность первого порядка для булевой функции следа. Таблица истинности такой булевой функции имеет вид:

$$s_t = \begin{cases} 0, t = 0, \\ Tr(\alpha^t), t = 1,2...2^n - 1, \end{cases} \quad (1)$$

где α – примитивный элемент поля F_{2^n}, $Tr : F_{2^n} \to F_2$, $Tr(\alpha) = \alpha + \alpha^2 + +\alpha^{2^2} + ... + \alpha^{2^{n-1}}$ – функция следа [2].

Заметим, что таблица истинности (1) представляет собой линейную рекуррентную последовательность (л.р.п.) максимального периода, в начало которой добавлен нулевой элемент. Таким образом, таблица истинности булевой функции удовлетворяют всем известным свойствам л.р.п. максимального периода (длина периода, сбалансированность и др.).

Теорема 1. Булева функция следа (1) удовлетворяет критерию CI(1) тогда и только тогда, когда

$$\sum_{t=0}^{2^{n-1}-1} s_t = \sum_{t=2^{n-1}}^{2^n-1} s_t = 2^{n-2}. \qquad (2)$$

Доказательство. Преобразование Уолша-Адамара функции следа $f(x)$ задается по правилу

$$\hat{f}(\lambda) = \sum_{t=0}^{2^n-1} (-1)^{f(x)} (-1)^{<\lambda,x>}, \quad \lambda \in V_n.$$

При этом $f(x)$ удовлетворяет CI(1) тогда и только тогда, когда $\hat{f}(\lambda) = 0$ для всех $\lambda \in V_n$ с весом $w(\lambda) = 1$.

Поскольку $\forall \gamma \in F_{2^n}$ выполняются равенства $Tr(\gamma) = Tr(\gamma^2)$ и $\gamma^{2^n} = \gamma$, то $s_t = s_{2t \bmod (2^n-1)}$, $t = 1,...,2^n - 2$. Отсюда следует, что $\hat{f}(\lambda) = \hat{f}(\rho(\lambda))$, где $\rho -$ преобразование циклического сдвига координат векторов из V_n. Поэтому условие $\hat{f}(\lambda) = 0$ достаточно проверить только для одного вектора $\lambda \in V_n$, $w(\lambda) = 1$.

Выберем $\lambda = (1,0,0,...,0,0)$. Тогда

$$\hat{f}(\lambda) = \sum_{t=0}^{2^{n-1}-1} (-1)^{s_t} - \sum_{t=2^{n-1}}^{2^n-1} (-1)^{s_t}.$$

Поэтому $\hat{f}(\lambda) = 0$ тогда и только тогда, когда

$$\sum_{t=0}^{2^{n-1}-1} (-1)^{s_t} = \sum_{t=2^{n-1}}^{2^n-1} (-1)^{s_t} \Leftrightarrow \sum_{t=0}^{2^{n-1}-1} s_t = \sum_{t=2^{n-1}}^{2^n-1} s_t.$$

Остается отметить, что на периоде $s_1,...,s_{2^n-1}$ л.р.п. максимального периода встречается ровно 2^{n-1} единичных элементов, откуда и следует второе равенство в (2). Теорема доказана.

Сформулируем еще одно необходимое условие корреляционной иммунности. Предварительно обозначим $\alpha_i = \alpha^{2^i}$, $i = 0,1,2...$

Теорема 2. Для того, чтобы булева функция следа (1) удовлетворяла критерию CI(1) необходимо выполнение равенств:

$$Tr\left(\left(\alpha_{n-1+k} + \alpha_k\right)\left(\alpha_k + 1\right)^{-1}\right) = 0, \quad k=0,...,n-1. \qquad (3)$$

В частности, должны существовать элементы $\beta_0,...,\beta_{n-1} \in F_{2^n}$ такие, что

$$\left(\alpha_{n-1+k} + \alpha_k\right)\left(\alpha_k + 1\right)^{-1} = \beta_k(\beta_k + 1), \quad k=0,...,n-1. \qquad (4)$$

Доказательство. Не нарушая общности, докажем (3) и (4) только для *k=0*. Выберем $\lambda = (1,0,0,...,0,0)$. Для выполнения (2), т. е. равенства $\sum_{t=0}^{2^{n-1}-1} s_t = 2^{n-2}$ необходимо, чтобы $\sum_{t=1}^{2^{n-1}-1} Tr(\alpha^t) = 0$.

Преобразуя выражение в левой части равенства, получим

$$\sum_{t=1}^{2^{n-1}-1} Tr(\alpha^t) = Tr\left(\sum_{t=1}^{2^{n-1}-1} \alpha^t\right) = Tr\left(\frac{\alpha\cdot\alpha+\alpha}{\alpha+1}\right) =$$

$$= Tr\left(\left(\alpha^{2^{n-1}}+\alpha\right)(\alpha+1)^{-1}\right). \qquad (5)$$

Известно [2], что $\forall \gamma \in F_{2^n}$ $Tr(\gamma) = 0$ тогда и только тогда, когда $\exists \beta \in F_{2^n}$ такой, что $\gamma = \beta^2 - \beta$. Т. е. условие (5) эквивалентно условию

$$\left(\alpha_{n-1}+\alpha_0\right)\left(\alpha_0+1\right)^{-1} = \beta^2+\beta = \beta(\beta+1).$$

Следовательно, формула (3) равносильна формуле (4). Теорема доказана.

В ходе практических экспериментов проверялись свойства CI(*k*) для функций, таблица истинности которых задавалась примитивным элементом поля $F_{2^n} \cong F_2[x]/p(x)$, где $p(x)$ – неприводимый многочлен степени *n*, $3 \le n \le 8$. Примитивный элемент α задавался мономом *x* факторкольца $F_2[x]/p(x)$. В результате были найдены 6 функций, удовлетворяющих CI(1). Данные функции определяются следующим выбором многочленов $p(x)$:

$$p(x) = x^3 + x^2 + 1,$$

$$p(x) = x^5 + x^2 + 1, \quad p(x) = x^5 + x^4 + x^3 + x + 1,$$

$$p(x) = x^7 + x^6 + x^5 + x^4 + x^2 + x + 1,$$

$$p(x) = x^8 + x^7 + x^2 + x + 1, \quad p(x) = x^8 + x^7 + x^6 + x + 1.$$

При этом функция, определяемая первым указанным многочленом, удовлетворяет также критерию CI(2). Критерии более высокого порядка в проведенных экспериментах не наблюдались.

Литература

1. *Siegenthaler T.* Correlation-immunity of nonlinear combining functions for cryptographic applications // IEEE Transactions on Information Theory. 1984. Vol. 30. P. 776–780.
2. *Лидл Р., Нидеррайтер Г.* Конечные поля: в 2 т. М.: Мир, 1988.