РОССИЙСКАЯ ФЕДЕРАЦИЯ

МЕЖДУНАРОДНАЯ НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ «СВЯЗЬ-ПРОМ 2009»,

в рамках

VI МЕЖДУНАРОДНОГО ФОРУМА

«СВЯЗЬ-ПРОМЭКСПО 2009»,

посвященного 150-летию со дня рождения изобретателя радио

А.С. Попова

Сборник научных трудов

17-19 марта 2009 г.

ЕКАТЕРИНБУРГ

УДК 621.37 (060.55)

Научные труды международной научно-практической конференции «СВЯЗЬ-ПРОМ 2009» в рамках 6го Международного форума «СВЯЗЬ-ПРОМЭКСПО 2009», посвященного 150 – летию со дня рождения изобретателя радио А.С. Попова. - Екатеринбург: УрТИСИ ГОУ ВПО «СибГУТИ», 2009. – 572 с.

Сборник посвящен актуальным проблемам отрасли связи.

УЧРЕДИТЕЛИ И ОРГАНИЗАТОРЫ КОНФЕРЕНЦИИ

Правительство Свердловской области
Администрация города Екатеринбурга
ООО «СОЮЗПРОМЭКСПО»
Уральский технический институт связи и информатики ГОУ ВПО «СибГУТИ»
ГОУ ВПО «Сибирский государственный университет телекоммуникаций и информатики»
ГОУ ВПО «Уральский государственный технический университет – УПИ имени первого Президента России Б.Н. Ельцина»
ГОУ ВПО «Уральский государственный университет путей сообщения»

ОРГКОМИТЕТ КОНФЕРЕНЦИИ

Председатель:
Ректор ГОУ ВПО «УГТУ-УПИ имени Первого президента России Б.Н. Ельцина», д.х.н., профессор **Матерн А.И.**
Заместители председателя:
начальник отдела связи и информационных технологий Министерства энергетики и жилищно-коммунального хозяйства Свердловской области **Семаков В.И.**
директор УрТИСИ ГОУ ВПО «СибГУТИ» - проректор ГОУ ВПО «СибГУТИ», к.т.н., профессор **Субботин Е.А.**
руководитель Радиотехнического института (радиотехнического факультета) ГОУ ВПО «УГТУ-УПИ имени первого Президента России Б.Н. Ельцина», д.т.н., профессор **Доросинский Л.Г.**
директор Центра стратегического развития ГОУ ВПО «УрГУПС» д.т.н., профессор **Нестеров В.Л.**
Секретарь:
Зав. кафедрой экономики связи УрТИСИ ГОУ ВПО «СибГУТИ», к.э.н. **Евдакова Л.Н.**

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

д.т.н., профессор Л.Г. Доросинский, к.т.н., доцент К.А. Паршин, д.т.н., профессор В.Г. Лисиенко, д.т.н., профессор С.В. Поршнев, д.т.н., профессор Д.Г. Неволин, д.т.н., профессор В.Э. Иванов, к.т.н., профессор Е.А. Субботин, к.т.н., доцент Н.В. Будылдина, д.т.н., профессор Б.А. Панченко, к.т.н., профессор А.А. Калмыков, к.э.н. Л.Н. Евдакова, к.п.н. М.А. Капшутарь

Ответственный за выпуск: директор УрТИСИ ГОУ ВПО «СибГУТИ» - проректор ГОУ ВПО «СибГУТИ», к.т.н., профессор Е.А. Субботин

Доклады представлены в авторской редакции.

УДК 512

ВЕКТОР СЛЕДА

К.Л. Глуско, Т.С. Носачёва, С.С. Титов

След имеет очень большое значение в кодировании, передаче информации и информационной технике, а также прикладной математике, компьютерной алгебре. В данной работе рассмотрен один из более простых способ нахождения следа – вычисление вектора следа. Сформулированы и доказаны теоремы для нахождения вектора следа определенных видов многочленов четной и нечетной степени.

VECTOR OF THE TRACE

K. L. Glusko, T.S. Nosachyova, S.S. Titov

The trace has very much great value in coding, an information transfer and the information technics, and also the applied mathematics, computer algebra. In the given work one of more simple a way of a finding of a trace – calculation of a vector of a trace is considered. Theorems for a finding of a vector of a trace of certain kinds of multinomials of even and odd degree are formulated and proved.

Одним из способов нахождения следа, упрощающего эту процедуру, является вычисление так называемого вектор следа для данного многочлена. Значение функции следа для элемента α поля GF (2^n) равно сумме (по модулю 2) элементов вектора, получаемого как поразрядное произведение (конъюнкция) элементов вектора α и вектора следа. Элементы t_i, $i = 0, \ldots, n-1$ вектор следа $(t_i, \ldots, t_{n-1})$ образуются суммированием по модулю два элементов таблицы, расположенных по диагонали (слева направо и сверху вниз) в соседних векторах $\alpha_i, \alpha_{i+1}, \ldots, \alpha_{i+n-1}$.

Теорема 1. Вектор следа при нечетном n будет иметь вид 1000...0, если и только если все показатели степеней членов неприводимого многочлена нечетные, за исключением нулевой.

Так как n – нечетное число (табл.1), то количество строк с нулевой по (n–1)-ю будет нечетным, в клетках по диагонали таблицы будут стоять единички и их сумма (по модулю два) будет равна единице. При расчете следующих цифр вектора следа количество единичек по диагоналям будет четным, так как единички начнут появляться с нечетных степеней x и они «пробегут» до конца таблицы четное число ячеек – последующие цифры вектора следа будут нулями.

Теорема 2. Вектор следа при четном n будет иметь вид 000…01, если и только если все показатели степеней членов неприводимого многочлена четные, за исключением первой.

Так как n – четное число (табл.2), то количество строк с нулевой по $(n-1)$-ю будет четным, в клетках по диагонали таблицы будут стоять единички и их сумма (по модулю два) будет равна нулю. При расчете следующих цифр вектора следа количество единичек будет четным, так как единички будут начинаться только в n-й строке в k-й позиции, а количество столбцов от k до $(n-1)$ – четное число, соответственно сумма (по модулю два) битов в каждой такой диагонали будет равна нулю. При расчете последней цифры мы начинаем с $(n-1)$-й строки, где заведомо будет стоять ноль, и заканчиваем на строке (2n–2) (количество строк с n-й но $(2n-2)$-ю нечетное) – сумма будет равна единице.

Таблица 1 - Таблица для произвольного многочлена $x^n + x^{n-1} + x^f + x^m + x^k + \ldots 1$

	0	1	2	3	4		k			m			f			n-1	Tr	
степень	1	1	0	1	0		1			1						1		
0	1	0	0	0	0											0	1	нечетное число строк
1	0	1	0	0	0											0	0	
2	0	0	1	0	0											0	0	
3	0	0	0	1	0											0	0	
4	0	0	0	0	1											0	0	
n-1	0											0						
n	1	1	0	0	0		1			1			1			0	1	четное число строк
n+1		1	1	0	0		0	1		0	1		0	1				
2n-2										1		1			1	1		

Таблица 2 - Таблица для произвольного многочлена $x^n + x^{n-1} + x^f + x^m + x^k + \ldots + x + 1$

	0	1	2	3	4	5		k			m			f			n–1	Tr	
степень	1	1	1	0	1	0		1			1						1		
0	1	0	0	0	0	0											0	0	четное число строк
1	0	1	0	0	0	0											0	0	
2	0	0	1	0	0	0											0	0	
3	0	0	0	1	0	0											0	0	
4	0	0	0	0	1	0											0	0	
5	0	0	0	0	0	1													
n–1	0												0						
n	1	1	1	0	1	0		1			1			1			1	1	нечетное число строк
n+1		1	1	1	0	1		0	1		0	1		0	1				
2n–2											1		1						

УДК 512

ГИПОТЕЗЫ О ЗАПРЕТАХ БУЛЕВЫХ ФУНКЦИЙ

А.Ю. Рожнёв

В статье рассмотрен возникающий при усложнении псевдослучайных последовательностей важный параметр булевой функции – запрет. Исследованы различные функции на данный параметр, а также предложен ряд гипотез по определению наличия или отсутствия запрета по виду функции.

HYPOTHESES ABOUT INTERDICTIONS OF BULIAN FUNCTIONS

A.J. Rozhnyov

In article the important parametre bulian functions – an interdiction is considered arising at complication of pseudo-casual sequences. Various functions on the given parametre are investigated, and also a number of hypotheses by definition of presence or absence of an interdiction by the form is offered function.

В криптоанализе запрет является одной из важных характеристик булевой функции [1]. Если функция, по которой работает автомат, имеет запрет, то некоторые комбинации битов в канале связи не могут появиться, что даёт дополнительную информацию криптоаналитику поточного шифра. Это значит, что комбинации битов в канале связи неравноправны, неравновероятны, и злоумышленник-криптоаналитик этим может воспользоваться, к тому же сокращается количество вариантов перебора ключей-комбинаций. Поэтому, в [1] поставлена задача нахождения эффективного критерия отсутствия или наличия запрета булевой функции.

Пусть $f(x^1, x^2, ..., x^n) \in F_n$, т.е. f - булева функция n переменных, причем x^1 и x^n - её существенные переменные, а среди остальных переменных могут быть и фиктивные переменные. Пусть некоторое устройство (конечный автомат) перерабатывает произвольную входную двоичную последовательность в выходную двоичную последовательность по следующему закону:

$$\begin{Bmatrix} f(x^s, x^{s+1}, ..., \mathrm{x}^{\mathrm{s+n-1}}) = y^s \\ s = 1,2,...,l, \end{Bmatrix} \quad , \tag{1}$$

где $f \in F_n, l$ - натуральное число. Таким образом, это устройство перерабатывает последовательность $x = (x^1, x^2, ..., x^{l+n-1}) \in V_{l+n-1}$ в последовательность $y = (y^1, y^2, ..., y^l) \in V_l$ для любого натурального числа l . Такое устройство называется кодирующим устройством с конечной памятью и без обратной связи.

Относительно системы уравнений (1) с фиксированной булевой функцией возможны два случая: либо для любого натурального числа l система уравнений (1) совместна при любых значениях правых частей, либо существует такое число l^* и такой набор $\widetilde{y} = (\widetilde{y}^{(1)}, \widetilde{y}^{(2)}, ..., \widetilde{y}^{(l^*)})^T \in V_{l^*}$, что система

$$\begin{Bmatrix} f(x^{(s)}, x^{(s+1)}, ..., x^{(s+n-1)}) = \widetilde{y}^{(s)}, \\ s = 1,2,...,l^* \end{Bmatrix} \tag{2}$$

несовместна, т.е. выходная последовательность $\widetilde{y} \in V_{l*}$ не может быть получена с помощью данного кодирующего устройства ни при каких входных последовательностях $x = (x^{(1)}, x^{(2)}, ..., x^{(l*+n-1)})^T$. Здесь и далее будем представлять функции в виде полинома Жегалкина.

Определение ([1]). *Булева функция $f \in F_n$ называется функцией без запрета, если для любого натурального числа l и для любого набора $y = (y^{(1)}, y^{(2)}, ..., y^{(l)}) \in V_l$ система уравнений (1) совместна. В противном случае функция f называется функцией запрета, а набор $\widetilde{y} = (\widetilde{y}^{(1)}, \widetilde{y}^{(2)}, ..., \widetilde{y}^{(l*)}) \in V_{l*}$ для которого система уравнений (1) не совместна, называется запретом булевой функции f длины l^*.*

Определение ([1]). *Если $deg(f,x^{(i)})=1$, то функция f зависит от переменной $x^{(i)}$ линейно. Если $deg(f,x^{(i)})>1$, то функция f зависит от переменной $x^{(i)}$ нелинейно.*

Согласно задаче 9.54, с. 419 [1] функция $f(x^{(1)}, x^{(2)}, ..., x^{(n)}) \in F_n$, линейная по первой или/и по последней переменной, является функцией без запрета.

Определение ([1]). *Булева функция $f \in F_n$ называется сильно равновероятной, если для любого натурального числа l и для любого набора $y = (y^{(1)}, y^{(2)}, ..., y^{(l)}) \in V_l$ система уравнений (1) имеет ровно 2^{n-1} решений.*

Теорема([1]). *Булева функция $f \in F_n$ не имеет запрета тогда и только тогда, когда она сильно равновероятна.*

Следствие([1]). *Если функция $f \in F_n$ не уравновешена, то эта функция имеет запрет.*

Рассмотрим функции двух переменных. Из 16 функций 6 уравновешенных. Но в расчёт берутся только функции двух переменных, в итоге остается две функции: $f(x_1, x_2) = x_1 + x_2$, $f(x_1, x_2) = (x_1 + x_2) + 1$. Но так как эти функции линейные по крайним переменным, это значит, что у них нет запрета.

Исследуем функции трех переменных. Функция трех переменных имеет вид:

$$f(x_1, x_2) = a + bx_1 + cx_2 + dx_3 + ex_1x_2 + fx_2x_3 + gx_1x_3 + hx_1x_2x_3. \tag{3}$$

Коэффициент a мы не учитываем, поэтому остается 2^7 функций. Также мы не рассматриваем функции, содержащие член $x_1x_2x_3$, т.к. они не будут уравновешенными, а нас, согласно следствию [1], интересуют только уравновешенные функции, поскольку если функция $f \in F_n$ не уравновешена, то эта функция имеет запрет. Путём полного перебора всех булевых функций трёх переменных, записанных в виде многочлена Жегалкина, получено:

Утверждение 1. *Нелинейные по крайним переменным уравновешенные булевы функции трёх переменных имеют запрет.*

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

$$f(x_1, x_2, x_3, x_4) = 1 + x_1 + x_3 + x_1x_2 + x_2x_4 + x_1x_2x_4 \tag{4}$$

не имеет запрета. Согласно определению 9.55, с.419 [1], мы проверили функцию на сильную равновероятность, и оказалось, что она не сильно равновероятна. Получилось, что система (1) при *l=2* имеет разное количество решений при всех возможных значения y_1 и y_2, следовательно, по теореме 9.56, с.420 [1] данная функция имеет запрет, а из теоремы 9.59, с.423 [1] вытекает, что имеется запрет длины $l \leq 242$. Но 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 убрать несущественный член 1, а также добавить существенную переменную x_2, при этом функция станет иметь вид

$$f(x_1,x_2,x_3,x_4)=x_1+x_2+x_3+x_1x_2+x_2x_4+x_1x_2x_4, \tag{5}$$

тогда она станет равновероятной при проверке на запрет длины 10, поэтому можно предположить, что она не имеет запрета.

Перед нами была поставлена задача доказать что функция (5) не имеет запрета.

Определение. *Функция f называется l-сильно уравновешенной, если система уравнений (1) имеет 2^{n-1} решений для любого набора $y_1,y_2,\dots,y_l$.*

Решение данной задачи состояло в проверке на запрет длины 10, а также нахождения различных закономерностей, возникающих при этой проверке. В итоге получены следующая гипотеза:

Гипотеза 1. *Сильная уравновешенность при l=2 (и при l=1) влечёт за собой отсутствие запрета (т.е. сильную уравновешенность для любого l), если это выполняется для n=3 и для n=4.*

Также были проверены следующие максимально-нелинейные функции степени 3 от 6 переменных (Бент-функции):

$$f(x_1,x_2,x_3,x_4,x_5,x_6)=x_1x_2x_3+x_1x_4+x_2x_5+x_3x_6, \tag{6}$$

$$f(x_1,x_2,x_3,x_4)=x_1x_2x_3+x_2x_4x_5+x_1x_2+x_1x_4+x_2x_6+x_3x_5+x_4x_5 \tag{7}$$

При проверке на уравновешенность оказалось, что данные функции неуравновешенные, а, следовательно, они имеют запрет (по теореме из [1]). Проведенный эксперимент позволяет выдвинуть предположение о том, что чем больше функция нелинейна, тем больше вероятность того, что имеется запрет.

Следующей задачей была проверка всех функций 4-х переменных на наличие или отсутствие запрета. Так как основным критерием, влияющим на наличие или отсутствие запрета является уравновешенность, то стояла задача проверки всех функции 4-х переменных именно на это свойство. По итогам такой проверке было получено: из 16 384 функций 9949 являются неуравновешенными, соответственно 6435 – уравновешенные, при проверке на сильную уравновешенность с *l=2* оказалось, что уравновешенными являются 2073 функции из 16384, с *l=4* - 307 уравновешенных функций.

По итогам работы с запретами можно отметить, что был произведен перебор всех функций двух и трех переменных на запрет длины 5, перебор функций 4-х переменных на запрет длины 4, составлен алгоритм для автоматического перебора функций.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

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 К.Л., Рожнёв А.Ю., Титов С.С.* О запретах булевой функции majority. Сборник научных трудов «Молодежь – будущее атомной промышленности России». Снежинск: СГФТА, 2007. 82-86 с.

Глуско К.Л., Носачёва Т.С., Рожнёв А.Ю. О следах и запретах булевых функций. Научные труды Междунар. научно-практич. конф. «СВЯЗЬ-ПРОМ 2008». - Екатеринбург: ЗАО «Компания Реал-Медиа», 2008. - 4

УДК 681.3

ИССЛЕДОВАНИЕ УРАВНОВЕШЕННЫХ БУЛЕВЫХ ФУНКЦИЙ НАД ПОЛЕМ GF(2^4)

О.А. Таскин, Д.С. Тарасов

В работе объектом исследования являются булевы функции [1], которые широко применяются в логике, электротехнике, при кодировании информации, во многих разделах информатики. В результате была написана программа, которая позволила найти все уравновешенные булевы функции от четырех переменных.

RESEARCH COUNTERBALANCED BULIAN FUNCTIONS OVER FIELD GF(2^4)

O.A. Taskin, D.S. Tarasov

In work as object of research are bulian functions [1] which are widely applied in the logician, the electrical engineer, at information coding, in many sections of computer science. The purpose – to investigate them on steadiness on the first bit. The program which has allowed to find all counterbalanced булевы functions from four variables has been as a result written.

В работе была поставлена следующая задача: найти все уравновешенные булевы функции в поле многочленов GF(2^4).

Был взят неприводимый над полем GF(2) многочлен $x^4 + x^3 + x^2 + x + 1$, порядок которого – 5. Если α – корень данного многочлена, то справедливо тождество $\alpha^4 = \alpha^3 + \alpha^2 + \alpha + 1$.

Если $x^{15}=0$, то $x=0$. Если $x^{15}=1$, то $x\neq0$. Любой элемент x можно представить через степени корня α: $x=(x_0,x_1,x_2,x_3)=x_0\alpha^0+ x_1\alpha^1+ x_2\alpha^2+ x_3\alpha^3$.

Для проверки булевой функции на уравновешенность необходимо построить ее таблицу истинности. В данном случае она строилась по младшему биту. В таблицах 1 и 2 показаны примеры заполнения таких таблиц для двух функций, причем первая оказалась неуравновешенной, а вторая – уравновешенной.

Таблица 1 - Таблица истинности булевой функции $F(x)= x^5+x^3+x$

x	$x_0x_1x_2x_3$	f(x)	F(x)
0	0 0 0 0	0	0=(0,0,0,0)
1	1 0 0 0	1	1=(1,0,0,0)
α	0 1 0 0	1	$1+\alpha+\alpha^3$=(1,1,0,1)
$1+\alpha$	1 1 0 0	1	1=(1,0,0,0)
α^2	0 0 1 0	1	$1+\alpha+\alpha^2$=(1,1,1,0)
$1+\alpha^2$	1 0 1 0	1	1=(1,0,0,0)
$\alpha+\alpha^2$	0 1 1 0	1	$1+\alpha+\alpha^2+\alpha^3$=(1,1,1,1)
$1+\alpha+\alpha^2$	1 1 1 0	0	α=(0,1,0,0)
α^3	0 0 0 1	0	$\alpha+\alpha^2$=(0,1,1,0)

$1+\alpha^3$	1 0 0 1	1	1=(1,0,0,0)
$\alpha+\alpha^3$	0 1 0 1	0	α^2=(0,0,1,0)
$1+\alpha+\alpha^3$	1 1 0 1	1	$1+\alpha+\alpha^2$=(1,1,1,0)
$\alpha^2+\alpha^3$	0 0 1 1	0	0=(0,0,0,0)
$1+\alpha^2+\alpha^3$	1 0 1 1	0	0=(0,0,0,0)
$\alpha+\alpha^2+\alpha^3$	0 1 1 1	1	1=(1,0,0,0)
$1+\alpha+\alpha^2+\alpha^3$	1 1 1 1	0	$\alpha+\alpha^3$=(0,1,0,1)

Таблица 2 - Таблица истинности булевой функции $F(x)= x^6+x^5+x$

x	$x_0x_1x_2x_3$	f(x)	F(x)
0	0 0 0 0	0	0=(0,0,0,0)
1	1 0 0 0	1	1=(1,0,0,0)
α	0 1 0 0	1	1=(1,0,0,0)
$1+\alpha$	1 1 0 0	0	$\alpha+\alpha^2$=(0,1,1,0)
α^2	0 0 1 0	1	1=(1,0,0,0)
$1+\alpha^2$	1 0 1 0	1	$1+\alpha+\alpha^3$=(1,1,0,1)
$\alpha+\alpha^2$	0 1 1 0	0	α^2=(0,0,1,0)
$1+\alpha+\alpha^2$	1 1 1 0	0	α^3=(0,0,0,1)
α^3	0 0 0 1	1	1=(1,0,0,0)
$1+\alpha^3$	1 0 0 1	0	$\alpha+\alpha^3$=(0,1,0,1)
$\alpha+\alpha^3$	0 1 0 1	0	α=(0,1,0,0)
$1+\alpha+\alpha^3$	1 1 0 1	1	$1+\alpha^2+\alpha^3$=(1,0,1,1)
$\alpha^2+\alpha^3$	0 0 1 1	0	0=(0,0,0,0)
$1+\alpha^2+\alpha^3$	1 0 1 1	0	0=(0,0,0,0)
$\alpha+\alpha^2+\alpha^3$	0 1 1 1	1	$1+\alpha+\alpha^2$=(1,1,1,0)
$1+\alpha+\alpha^2+\alpha^3$	1 1 1 1	1	1=(1,0,0,0)

Для увеличения скорости выполнения расчетов и повышения их точности на Delphi 7 [2] была написана программа, выполняющая аналогичные расчеты автоматически.

В результате использования данной программы при исследовании булевых функций было найдено 6435 уравновешенных функций. С учетом нулевого (инвертирующего) бита общее число уравновешенных функций составляет 12870.

Развитый метод предполагается использовать для исследования криптографических свойств булевых функций.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. Логачев О.А. Криптографические свойства дискретных функций /О.А. Логачев, А.А. Сальников,В.В.Ященко // Материалы / Конференция «Московский Университет и развитие криптографии в России» М: Изд-во МГУ, 2002.

2. Иллюстрированный самоучитель по Delphi для начинающих. [Электрон. ресурс] / Режим доступа : www.booksforall.ru/view_975.html.

МЕЖДУНАРОДНАЯ НАУЧНО-ПРАКТИЧЕСКАЯ

КОНФЕРЕНЦИЯ «СВЯЗЬ-ПРОМ 2009»,

в рамках

VI МЕЖДУНАРОДНОГО ФОРУМА

«СВЯЗЬ-ПРОМЭКСПО 2009»,

посвященного 150-летию со дня рождения изобретателя радио

А.С. Попова

Подписано в печать 15.04.09,
формат бумаги 62x84/16, отпечатано на ризографе,
шрифт № 10
печ. л. 33,13, тираж 200, заказ 480
Типография УрТИСИ ГОУ ВПО «СибГУТИ»
620109, Екатеринбург, ул. Репина, 15