УДК 681.326.7:519.718.7

Л.П.Мах

ДОСТОВЕРНОСТЬ КЛАССОВ СИГНАТУРНЫХ АНАЛИЗАТОРОВ, ПОРОЖДАЕМЫХ ПРОИЗВЕДЕНИЯМИ МИНИМАЛЬНЫХ ПОЛИНОМОВ

Предлагаются точные границы достоверности сигнатурных анализаторов, порождаемых полиномами, которые являются образующими полиномами примитивных БЧХ-кодов, исправляющих две ошибки; найдены классы сигнатурных анализаторов, имеющие такие же характеристики, как и сигнатурные анализаторы, порождаемые полиномами - образующими примитивных БЧХ-кодов, исправляющих две ошибки.

Одним из подходов повышения достоверности сигнатурного анализа является способ, основанный на применении нескольких сигнатурных анализаторов, реализованных с помощью примитивных и непримитивных полиномов, имеющих одинаковую степень [5].

В качестве меры оценки достоверности сигнатурного анализа будем рассматривать распределение вероятностей необнаружения ошибки в зависимости от веса k последовательностей данных, которое определяется следующим образом:

$$P_n(k) = A_n(k) / C_n^k,$$

где $A_n(k)$ - количество необнаруживаемых определенным методом сжатия ошибочных последовательностей длины n, содержащих ошибки веса k, к общему числу последовательностей C_n^k (число сочетаний из n по k). Такой подход к оценке достоверности использовался для сигнатурных анализаторов, порождаемых примитивными полиномами, в [5].

В работе приведены результаты анализа достоверности классов сигнатурных анализаторов, порождаемых полиномами, образующими примитивные БЧХ-коды, которые исправляют две ошибки [1,3,4], исследован класс сигнатурных анализаторов, имеющий такие же характеристики, как и некоторые сигнатурные анализаторы, порождаемые полиномами, образующими примитивные БЧХ-коды, которые исправляют две ошибки.

Для сигнатурного анализатора, порождаемого полиномами нечетной степени, произведение которых является образующим примитивного БЧХ-кода, исправляющего две ошибки, найдены точные формулы числа двоичных последовательностей длины $n=2^m-1$ веса k, инициирующих нулевую

сигнатуру, получено распределение величин $P_n(k)$ и найдена точная верхняя граница достоверности $\max P_n(k)$ указанного выше сигнатурного анализатора. Распределение вероятностей необнаружения ошибки в зависимости от веса k последовательностей данных может быть рассчитано на основе следующего рекуррентного соотношения:

$$(n-k+4)(n-k+3)(n-k+2)P_n(k) = n-1-$$
$$-(n-k+4)\{2(k-2)(n-k+3)+(k-4)(n-k+4)\}P_n(k-2)-$$
$$-(k-3)\{2(k-4)(n-k+5)+(k-3)(n-k+3)\}P_n(k-4)-$$
$$-(k-3)(k-4)(k-5)P_n(k-6),$$

с начальными условиями $P_n(0)=1$, $P_n(2)=0$, $P_n(4)=0$, если k четное, и $P_n(k)=P_n(k+1)$, если k нечетное ($0 \le k \le n$). Анализ этого соотношения дает возможность оценить предельные границы достоверности.

Теорема 1. Максимальное значение вероятности необнаружения ошибочной последовательности длины $n = 2^m - 1$ сигнатурным анализатором, порождаемым полиномом степени 2m (m нечетно, $m \ge 5$) – образующим примитивного кода БЧХ, исправляющего две ошибки, определяется выражением:

$$\max_k P_n(k) = \frac{n-7}{(n-2)(n-3)(n-4)}, \qquad (1)$$

и достигается при k=5, 6, n-6, n-5 [6].

Также найдена и нижняя граница достоверности для соответствующего сигнатурного анализатора.

Рассмотрим класс сигнатурных анализаторов, обладающий такими же характеристиками, как и сигнатурный анализатор, порождаемый полиномом степени 2m (m нечетно) – образующим примитивного БЧХ-кода, исправляющего две ошибки [6].

Утверждение 1. Пусть M_1 – примитивный полином нечетной степени m=2t+1 над полем GF(2), а элемент b поля $GF(2^m)$ – некоторый его корень [2]. Образуем множество минимальных многочленов M_s элементов b^s, где $s=2^i+1$, $1 \le i \le t$, а числа m и i взаимно просты. Построим множество сигнатурных анализаторов G_s, порождаемых произведениями примитивного полинома M_1 и некоторого минимального многочлена M_s. Тогда предельная оценка P_s вероятности необнаружения ошибочной последовательности сигнатурным анализатором G_s не зависит от s и определяется соотношением (1) [6].

Пример 1. Пусть m=9, t=4, $M_1=x^9+x^5+1$ – примитивный полином. Тогда i может принимать значения 1, 2, 4 и множество минимальных многочленов M_s состоит из многочленов $M_3=x^9+x^6+x^5+x^3+1$, $M_5=x^9+x^5+x^4+x+1$, $M_{17}=x^9+x^8+x^6+x^5+x^3+x^2+1$. Тогда сигнатурные анализаторы G_3, G_5, G_{17}, порождаемые полиномами M_1M_3, M_1M_5, M_1M_{17} соответственно, имеют одну и туже предельную оценку вероятности необнаружения ошибочной

последовательности. Заметим, что сигнатурный анализатор G_3, порождается полиномом M_1M_3, который является образующим примитивного БЧХ-кода, исправляющего две ошибки. Поэтому для него, очевидно, выполняется соотношение (1).

В работе исследуется достоверность сигнатурного анализатора, порождаемого полиномом степени 2m (m - четно) – образующим примитивного БЧХ-кода, исправляющего две ошибки. В этом случае порождающий полином является произведением примитивного и, в общем случае, непримитивного полиномов, степени которых равны некоторому четному числу m.

Теорема 2. Максимальное значение вероятности необнаружения ошибочной последовательности длины $n = 2^m - 1$ сигнатурным анализатором, порождаемым полиномом степени 2m (m четно, m≥4) – образующим примитивного кода БЧХ, исправляющего две ошибки, определяется выражением:

$$\max_k P_n(k) = \frac{n-3}{(n-1)(n-2)(n-4)}, \qquad (2)$$

и достигается при k=5, 6, n-6, n-5 [6].

Для данного сигнатурного анализатора также определена нижняя граница достоверности, найдены точные формулы числа двоичных последовательностей длины $n = 2^m - 1$ веса k, инициирующих нулевую сигнатуру для фиксированного сигнатурного анализатора, порождаемого полиномом степени 2m (m четно) – образующим примитивного БЧХ-кода, исправляющего две ошибки, а также распределение величин $P_n(k)$ [6].

Рассмотрим класс сигнатурных анализаторов, обладающий такими же характеристиками, как и сигнатурный анализатор, порождаемый полиномом степени 2m (m четно) – образующим примитивного БЧХ-кода, исправляющего две ошибки.

Утверждение 2. Пусть M_1 – примитивный полином четной степени m над полем GF(2), а элемент b поля $GF(2^m)$ – некоторый его корень [2]. Образуем множество минимальных многочленов M_s элементов b^s, где $s=2^i+1$, $1 \le i<m/2$, а числа m и i - взаимно просты. Построим множество сигнатурных анализаторов G_s, порождаемых произведениями примитивного полинома M_1 и некоторого минимального многочлена M_s. Тогда предельная оценка P_s вероятности необнаружения ошибочной последовательности сигнатурным анализатором G_s не зависит от s и определяется соотношением (2) [6].

Пример 2. Пусть m=14, $M_1=x^{14}+x^{12}+x^{11}+x+1$ – примитивный полином, и числа i и m взаимно просты. Тогда i, учитывая утверждение 2, может принимать значения 1, 3, 5 и множество минимальных многочленов M_s состоит из многочленов $M_3=x^{14}+x^{13}+x^{11}+x^9+x^5+x+1$, $M_9=x^{14}+x^{11}+x^9+x^8+x^4+x^3+x^2+x+1$ и $M_{33}=x^{14}+x^{13}+x^{12}+x^{11}+x^9+x^5+x^2+x+1$. Тогда сигнатурные анализаторы G_3, G_9, G_{33}, порождаемые полиномами M_1M_3, M_1M_9, M_1M_{33} соответственно, имеют одну и ту же предельную оценку вероятности необна-

ружения ошибочной последовательности. Заметим, что сигнатурный анализатор G_3 порождается полиномом M_1M_3, который является образующим примитивного БЧХ-кода, исправляющего две ошибки. Поэтому для него, очевидно, выполняется соотношение (2).

Следует отметить, что при любом m (четном или нечетном) в качестве минимального многочлена M_1 можно взять в точности $\varphi(2^m-1)/m$ различных примитивных полиномов степени m, где φ - функция Эйлера (в [4] приведены полные таблицы примитивных полиномов). Тогда количество сигнатурных анализаторов, обладающих одной и той же оценкой достоверности, определяется соотношением: $\varphi(2^m-1)\varphi(m)/(2m)$. Действительно, количество чисел i, взаимно простых с m, и удовлетворяющих соотношению $1 \le i < m/2$ (утверждение 1, 2), не зависит от четности m и равно $\varphi(m)/2$.

В табл. 1, 2 приведены все порождающие многочлены $M_1 \times M_s$ (для m=5, 6) сигнатурных анализаторов, имеющих одинаковые границы достоверности, определяемые соотношениями (1) и (2) соответственно. Так, например, при m=5, $M_1=x^5+x^2+1$ (101001, десятичное представление – 37), $M_5=x^5+x^4+x^2+x+1$ (111011, 55). Тогда $M_1 \times M_s=M_1 \times M_5=x^{10}+x^9+x^5+x+1$ (11010000011, 1547), что соответствует второй строке табл. 1. Алгоритм нахождения всех полиномов, описанных в утверждениях 1, 2, программно реализован для $4 \le m \le 32$, что дает возможность построения сигнатурных анализаторов достаточно большой разрядности (до 64 разрядов).

Таблица 1

Порождающие многочлены степени 2m сигнатурных анализаторов с одинаковыми границами достоверности (m=5)

	M_1		l	M_s		$M_1 \times M_s$	
1	101001	37	3	101111	61	10010110111	1897
2	101001	37	5	111011	55	11010000011	1547
3	101111	61	3	111011	55	11000011001	1219
4	101111	61	5	100101	41	10101110011	1653
5	111011	55	3	100101	41	11110110111	1903
6	111011	55	5	111101	47	10111011111	2013
7	111101	47	3	110111	59	10011000011	1561
8	111101	47	5	101001	37	11001110101	1395
9	110111	59	3	101001	37	11101101111	1975
10	110111	59	5	101111	61	11111011101	1503
11	100101	41	3	111101	47	11101101001	1207
'12	100101	41	5	110111	59	11000001011	1667

Заметим, что использование произведения минимальных многочленов, которое является образующим кода, исправляющего две ошибки, для построения сигнатурного анализатора, в общем случае, не приводит к ана-

логичным результатам. Оценка их достоверности не совпадает с (1) или (2) в зависимости от четности m.

Таблица 2

Порождающие многочлены степени 2m сигнатурных анализаторов с одинаковыми границами достоверности (m=6)

	M_1		s	M_s		$M_1 \times M_s$	
1	1100001	67	3	1110101	87	1001110010101	5433
2	1110011	103	3	1010111	117	1101010101001	4779
3	1011011	109	3	1110101	87	1100100100111	7315
4	1101101	91	3	1010111	117	1110010010011	6439
5	1100111	115	3	1110101	87	1001010101011	6825
6	1000011	97	3	1010111	117	1010100111001	5013

В заключение на основе полученных выше результатов и программного моделирования произведем сравнение достоверности класса сигнатурных анализаторов G_s (m нечетно) с классом сигнатурных анализаторов, порождаемых произведением примитивного и возвратного к нему полиномов нечетных степеней – образующих код Мелласа. Сравнительный анализ показывает, что верхняя граница вероятности необнаружения ошибок для первого класса не превышает соответствующую границу для второго. Так, например, пусть m=5, t=2, i=2, s=5 и $M_1 = x^5+x^2+1$ – примитивный полином, определяемый утверждением 1. Тогда сигнатурный анализатор G_s порождается произведением полиномов M_1 и $M_s=x^5+x^4+x^2+x+1$. Сравним достоверность данного сигнатурного анализатора и сигнатурного анализатора H_M, порождаемого произведением примитивного M_1 и возвратного к нему $M_1=x^5+x^3+1$ полиномов. Между $G_s(k)$ и $H_M(k)$ - количеством последовательностей веса k длины n=31, дающих нулевую сигнатуру для анализаторов G_s и H_M соответственно, выполняется следующее соотношение:

$$G_s(k) = H_M(k) + (-1)^{[k/2]} C_{2m}^{[k/2]-3} n,$$

если $5 \le k \le n-5$, и $G_s(k)=H_M(k)$ для остальных весов ([k/2] - целая часть числа k/2). В табл. 3 приведены результаты программного моделирования для сигнатурных анализаторов G_s и H_M. Анализ последнего соотношения показывает, что достоверность сигнатурного анализатора G_s выше, чем у анализатора H_M, т. е.

$$\max_k \; G_s(k)/C_n^k \le \max_k \; H_M(k)/C_n^k.$$

Таблица 3

Количество последовательностей, инициирующих нулевую сигнатуру

k	$G_s(k)$	$H_M(k)$
0	1	1
1	0	0
2	0	0
3	0	0
4	0	0
5	186	217
6	806	837
7	2635	2325
8	7905	7595
9	18910	20305
10	41602	42997
11	85560	81840
12	142600	138880
13	195300	201810
14	251100	257610
15	301971	294159

Литература

1. Берлекэмп Э. Алгебраическая теория кодирования: Пер. с англ. - М.: Мир, 1971. – 477 с.

2. Лидл Р., Нидеррайтер Г. Конечные поля. Т. 1, 2: Пер. с англ. - М.: Мир, 1988. – 824 с.

3. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки: Пер с англ. - М.: Связь, 1979. – 744 с.

4. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки: Пер. с англ. - М.: Мир, 1976. – 594 с.

5. Ярмолик В. Н. Контроль и диагностика цифровых узлов ЭВМ. - Минск: Наука и техника, 1988. – 240 с.

6. Махнист Л. П. Оценивание достоверности сигнатурного анализа для контроля цифровых схем: Дисс... канд. техн. наук. - Минск: БГУИР, 1999. – 127 с.

Брестский политехнический институт