электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 003.26

Анализ поточных шифров при разных степенях функции выхода генератора ключевого потока

Хузина Э.И., *студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»

*Научный руководитель: Матвеев В.А., д.*т.н.
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана
v.a.matveev@bmstu.ru

Криптографические поточные шифры строятся с использованием генератора ключевого потока. Генератор ключевого потока инициализируют ключом меньшего размера, чем сам ключевой поток. Генератор ключевого потока вырабатывает псевдо случайный поток бит длины, равной длине исходного текста; создается псевдо случайная ключевая последовательность. Зашифрованное сообщение (шифротекст) формируется в результате выполнения алгоритма кодирования, заключающийся в комбинировании определенным образом исходного текста и ключевого потока, и отправляется законному получателю, который расшифровывает его по алгоритму декодирования. В данной работе в качестве алгоритма кодирования использовался покомпонентный XOR ключевого потока и исходного сообщения в поле F2, в качестве алгоритма декодирования - покомпонентный XOR ключевого потока и шифротекста так же в поле F2.

Генератор ключевого потока состоит из следующих компонентов [1]:

- внутренне состояние;

- К - конечное множество возможных внутренних состояний;

- функция обновления Y: К-> К;

- конечное множество Z, называемое алфавитом ключевого потока;

- функция выхода f : К -> Z.

Внутреннее состояние $S_0 \in К$ инициализируют ключом (или начальным состоянием), затем выполняют следующие операции:

- выходной бит $z_t \in Z$ вычисляется как $z_t = f(S_t)$;

- внутреннее состояние обновляется $S_{t+1} = Y(S_t)$.

В качестве генератора ключевого потока при создании поточного шифра использовался (l,m)-комбайнер. Пусть F – конечное поле, (l,m)-комбайнер состоит из следующих шести компонентов [1]:

- s РСЛОС с длинами $n_1,\ldots,n_S$ и матрицами обратной связи $L_1,\ldots,L_S$;

- внутреннее состояние $S \in F^m \times F^n$, где $n = n_1+\ldots+n_S$;

- матрица L, размером n×n, над полем F, определена как

$$L := \begin{pmatrix} L_1 & & 0 \\ & \ddots & \\ 0 & & L_s \end{pmatrix}$$

- матрица проекций P, размером n×l, над полем F;

- функция изменения состояния памяти $\Psi : F^m \times F^l \to F^m$;

- функция выхода $f : F^m \times F^l \to F$.

Если $m \geq 1$, тогда комбайнер называется комбайнер с памятью, если $m = 0$ – простой комбайнер.

Значения функции выхода (l,m)-комбайнера являются элементами ключевого потока. Зная, некоторое количество элементов ключевого потока, соотношения для формирования РСЛОС, функции выхода и изменения состояния памяти (l,m)-комбайнера (в поле F2), обозначив элементы S_0 через переменные, составим систему уравнений, где левая часть каждого уравнения представляет собой выражение для формирования одного из известных элементов ключевого потока плюс этого элемента. Таким образом, решив указанную систему уравнений, получим значения элементов S_0, то есть ключ, использованный для формирования ключевого потока. Система уравнений имеет следующий вид:

$$\begin{cases} f_1(x_1,\ldots,x_n) = 0, \\ f_1(x_1,\ldots,x_n) = 0, \\ \ldots \\ f_1(x_1,\ldots,x_n) = 0. \end{cases} \quad (1)$$

Теорема. Пусть дан идеал, составленный из уравнений [1] над полем F_q из системы (2):

$$I = < f_1,\ldots,f_n, x_1^q - x_1, x_2^q - x_2,\ldots, x_n^q - x_n >.$$

Для любого упорядочения редуцированный базис Гребнера имеет вид:

- $\{x_1 - \chi_1, x_2 - \chi_2, \ldots, x_n - \chi_n\}$, где $(\chi_1, \chi_2, \ldots, \chi_n)$ – решение системы уравнений (1)

- $\{1\}$, если система (1) не имеет решений.

Таким образом, по виду редуцированного базиса Гребнера системы (1), делаем вывод о значениях элементов начального состояния (l,m)-комбайнера. При декодировании, зная ключ ключевого потока и соотношения для формирования ключевого потока, генерируем ключевой поток, выполняем операцию XOR над шифротекстом и ключевым потоком и определяем исходное информационное сообщение.

Разработанное программное средство, написанное на C++, формирует систему алгебраических уравнений. Сгенерированная система уравнений загружалась в функцию bibasis(polynomials, variables, degrevlex,t) программы Reduce с целью вычисления редуцированного базиса Гребнера идеала в поле F2 [3] и получения значений элементов ключа.

Определим максимальные значения параметров l, m (l,m)-комбайнера, при которых можно найти программными способами его начальное состояние при известных значениях первых нескольких бит ключевого генератора, соотношениях для формирования LFSR, функций выхода и памяти (l,m)-комбайнера (в поле F2). Исследования проводились отдельно для разных степеней функции выхода (l,m)-комбайнера. Результаты ряда программных экспериментов приводятся в таблице 1.

Таблица 1

Результаты программных экспериментов

Степень функции выхода (l,m)-комбайнера	Параметры l,m (l,m)-комбайнера	Результат нахождения значений элементов S_0
2	l=2, m=11	1
	l=3, m=7	1
	l=4, m=3	1
	l=5, m=0	5 из 11
	l=6, m=0	5 из 13
	l=7, m=0	5 из 15
3	l=2, m=3	6 из 8
	l=3, m=0	1
	l=3, m=4	7 из 11

	l=4, m=2	7 из 11
	l=5, m=0	1 из 11
	l=6, m=0	3 из 13
4	l=2, m=5	5 из 10
	l=2, m=6	1 из 11
	l=3, m=0	1
	l=3, m=1	5 из 8
	l=4, m=0	6 из 9
	l=5, m=0	7 из 11
5	l=2, m=0	1 из 5

Значение «1» в столбце «Результат нахождения значений элементов S_0» означает, что найдены все элементы в S_0, запись «1 из 5» означает, что 1 из 5 переменных найдена верно, а для остальных известны равенства.

Полученные результаты представлены в виде графиков. На рис.1, 2, 3, 4 показаны графики, характеризующие наименьшие значения параметров l, m, при которых невозможно вычислить ни один элемент из ключа в случае степеней функции выхода (l,m)-комбайнера 2, 3, 4, 5 соответственно. Оси графиков – параметры l и m (l,m)-комбайнера, цифры рядом с точками на графиках обозначают процент точно найденных элементов ключа ключевого потока, произведенного (l,m)-комбайнером с параметрами, равными координатам точек, а для остальных элементов найдены соотношения, знак * означает, что для остальных элементов соотношения не найдены.

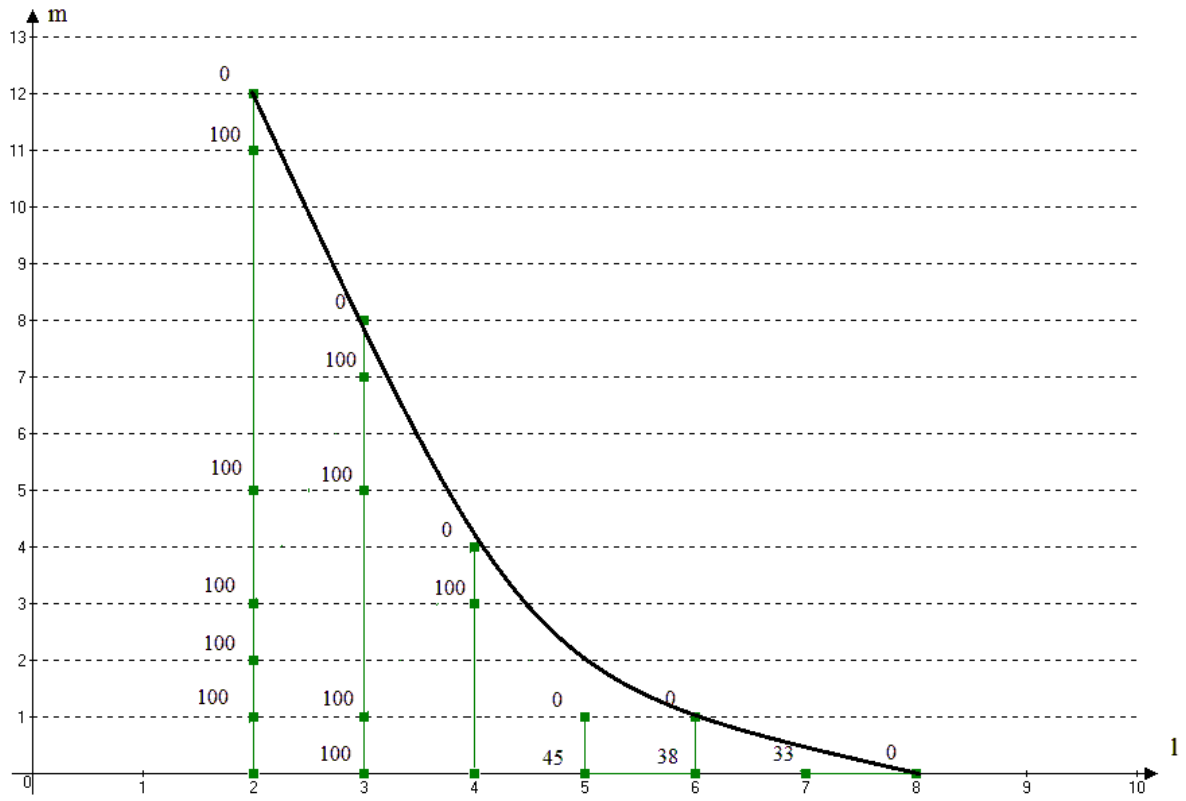

Рис. 1. Экспериментальные результаты при степени функции выхода (l,m)-комбайнера равной 2

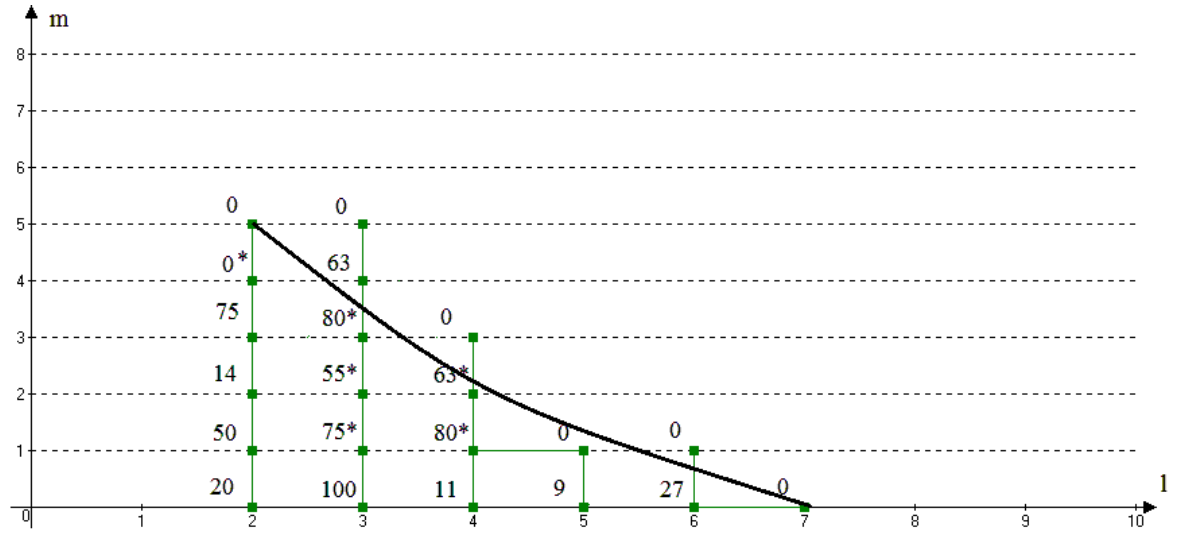

Рис. 2. Экспериментальные результаты при степени функции выхода (l,m)-комбайнера равной 3

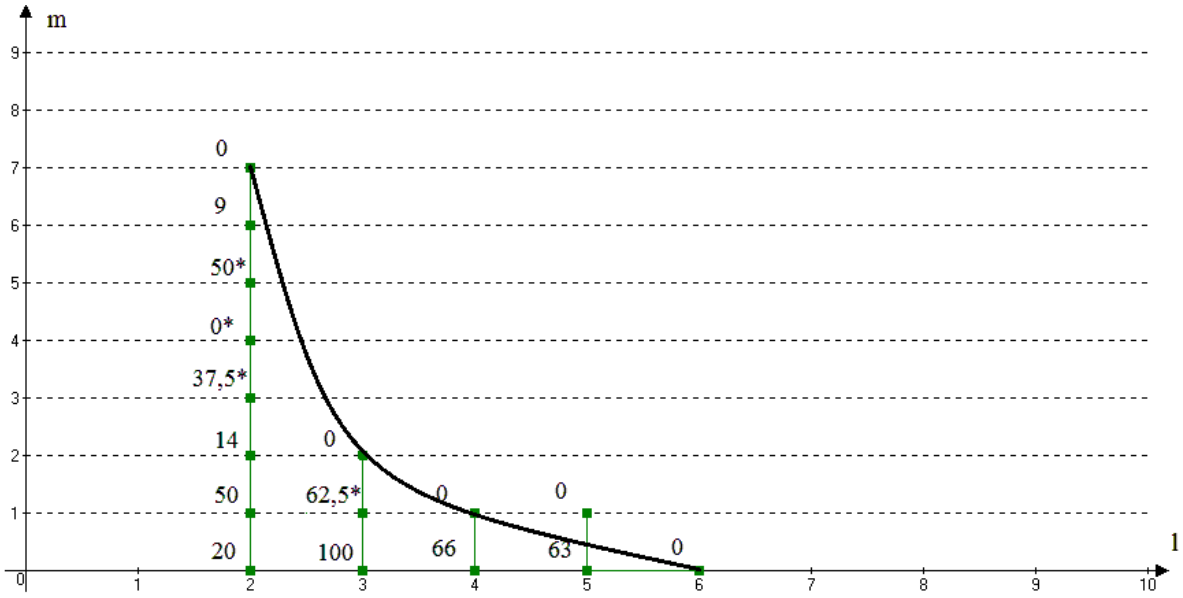

Рис. 3. Экспериментальные результаты при степени функции выхода (l,m)-комбайнера равной 4

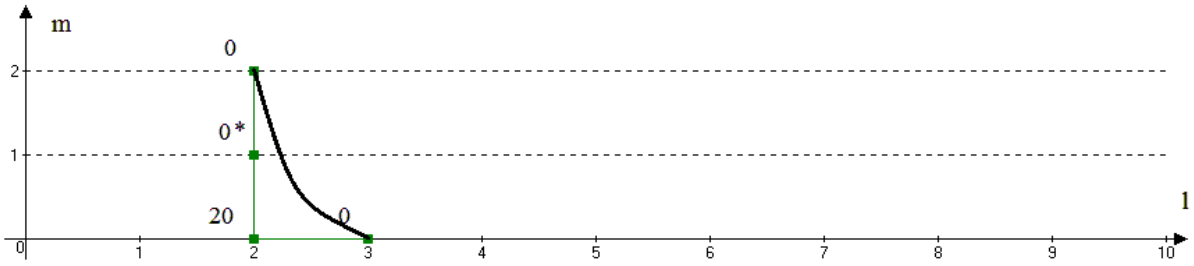

Рис. 4. Экспериментальные результаты при степени функции выхода (l,m)-комбайнера равной 5

Предположим, разработанная программа сформировала следующую систему уравнений:

Всевозможные мономы в системе (2):

$$\begin{aligned}
f_1 &= a_0 + b_0 + a_0b_0 + 1 \\
f_2 &= a_1 + b_1 + a_1b_1 + 1 \\
f_3 &= a_0 + a_1 + b_2 + a_0b_2 + a_1b_2 + 1 \\
f_4 &= a_0 + b_0 + b_2 + a_0b_0 + a_0b_2 + 1 \\
f_5 &= a_1 + b_0 + b_1 + b_2 + a_1b_0 + a_1b_1 + a_1b_2 + 1 \\
f_6 &= a_0 + a_1 + b_0 + b_1 + a_0b_0 + a_0b_1 + a_1b_0 + a_1b_1 + 1 \\
f_7 &= a_0 + b_1 + b_2 + a_0b_1 + a_0b_2 + 1 \\
f_8 &= a_1 + b_0 + a_1b_0 + 1 \\
f_9 &= a_0 + a_1 \\
f_{10} &= b_1 \\
f_{11} &= a_0b_2 + a_0 + b_2 + 1 \\
f_{12} &= a_1 + b_0 + b_2 + a_1b_0 + a_1b_2 + 1
\end{aligned} \qquad (2)$$

1, a_0, a_1, b_0, b_1, b_2, $a_0\,b_0$, $a_1\,b_0$, $a_0\,b_1$, $a_1\,b_1$, $a_0\,b_2$, $a_1\,b_2$.

Представим систему (2) в виде произведения матриц (матрицы коэффициентов и столбца мономов):

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\
1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1
\end{pmatrix}
\cdot
\begin{pmatrix}
a_1 \cdot b_2 \\ a_0 \cdot b_2 \\ a_1 \cdot b_1 \\ a_0 \cdot b_1 \\ a_1 \cdot b_0 \\ a_0 \cdot b_0 \\ b_2 \\ b_1 \\ b_0 \\ a_1 \\ a_0 \\ 1
\end{pmatrix}
=
\begin{pmatrix}
0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0
\end{pmatrix} \qquad (3)$$

Приведем левую матрицу к ступенчатому виду с помощью функции Gausselim(A) mod 2 программы [2] Maple 13, получим:

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a_1 \cdot b_2 \\ a_0 \cdot b_2 \\ a_1 \cdot b_1 \\ a_0 \cdot b_1 \\ a_1 \cdot b_0 \\ a_0 \cdot b_0 \\ b_2 \\ b_1 \\ b_0 \\ a_1 \\ a_0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad (4)$$

Умножив 4 последние строки в левой матрице в равенстве (4) на столбец мономов, легко определить, что

$a_0=1, a_1=1, b_0=1, b_1=1, b_2=1.$

Системы уравнений, получаемые из равенств (3) и (4) имеют одинаковые решения, так как приведение к ступенчатому виду включает в себя только элементарные преобразования матрицы, что не меняет множество решений системы линейных алгебраических уравнений, которую представляет эта матрица.

Из приведенного примера нахождения ключа поточного шифра видим, что в результате приведения матрицы коэффициентов к ступенчатому виду и последующем умножении ее на столбец всевозможных мономов, можно получить новую систему с большим количеством линейных уравнений, чем в исходной системе.

Список литературы

1. Armknecht F. Algebraic attacks on certain stream ciphers: Inauguraldissertation zur Erlangung des akademischen Grades eines Doktors der Naturwissenschaften / Universitat Mannheim. Mannheim. 2006.217 p.
2. Документация Maple 13. URL.http://www.maplesoft.com/support/help (дата обращения:15.05.2013г.).
3. Документация Reduce. URL.http://www.reduce-algebra.com/packages.htm (дата обращения:15.05.2013г.).