ПОДХОД К КРИПТОАНАЛИЗУ БЛОЧНОГО СИММЕТРИЧНОГО ШИФРА «ЛАБИРИНТ»

Казимиров А.В., Олейников Р.В., Небывайлов А.Б.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, каф. Безопасности информационных технологий,
тел. (057) 702-14-25,
E-mail: vrona@yandex.ru

This work is devoted to the analysis of the symmetric block cipher “Labyrinth” proposed as a candidate to a national standard of Ukraine. We applied first stage of algebraic attack on S-box, which is used in the encryption algorithm. The main point of the attack is to represent S-box as a system of equation. Researched S-box is weak to algebraic attack, that is a vulnerable part of cipher “Labyrinth”.

В настоящее время на Украине проводится открытый конкурс блочных симметричных шифров (БСШ) с целью определения алгоритма-прототипа национального стандарта шифрования. Одним из основных требований к перспективному шифру является высокий уровень стойкости к различным видам криптоаналитических атак, одновременно с обеспечением необходимой производительности. Среди участников открытого конкурса представлен и шифр «Лабиринт», разработанный в ЗАО «Криптомаш». Криптоанализ этого алгоритма необходим для реальной оценки стойкости шифра и его дальнейших перспектив в конкурсе.

В основе рассматриваемого алгоритма шифрования лежит цепь Фейстеля. В остальных конструктивных особенностях структура «Лабиринта» схожа со структурой шифра, принятого в качестве американского стандарта Advanced Encryption Standard (AES, FIPS PUB 197). Учитывая, что по результатам публикаций в открытой печати этот алгоритм является наиболее исследованным с точки зрения криптографических свойств и стойкости, целесообразно применить ряд предложенных для AES атак и для алгоритма «Лабиринт».

Одним из наиболее перспективных методов криптоанализа симметричных систем в настоящее время является алгебраическая атака. Этот метод позволяет описать всё шифрующее преобразование в виде одной системы уравнений, причём из-за особенностей построения S-блока AES (который одновременно является единственным нелинейным преобразованием во всём алгоритме) степень такой системы равна 2.

Было предложено использовать алгебраическую атаку на шифр. Основным нелинейным преобразованием в алгоритме является S-блок, поэтому в первую очередь был выполнен анализ именно этого компонента.

Пусть $X = \{x_7,x_6,x_5,x_4,x_3,x_2,x_1,x_0\}$ – байт, подающийся на вход S-блока, а $Y = \{y_7,y_6,y_5,y_4,y_3,y_2,y_1,y_0\}$ - байт на выходе S-блока.

В большинстве случаев при анализе свойств S-блока рассматривается функциональная зависимость выходных значений битов от входных следующего вида: $y_l = f_l(x_7, x_6, \ldots, x_0)$, $l = 0,1,\ldots 7$. Для большинства современных шифров, включая «Лабиринт», степень такого уравнения равна 7. Тем не менее, используя более общий вариант описания S-блока системой уравнений, где используются все входные и выходные переменные, можно получить более низкую степень. Более того, в большинстве случаев, такая система оказывается переопределённой.

Один из алгоритмов поиска системы переопределённых уравнений предполагает построение матрицы, описывающей все возможные значения термов для всех вариантов входных переменных. Для k битов на входе матрицы её размерность составляет $\left(2^k\right)\times\left(C_{2k}^2+2k+1\right)$. Соответственно, первый индекс элемента матрицы определяет вариант входа S-блока, второй – номер терма, включая все входные и выходные

переменные, все комбинации второй степени и константу 1: { 1, x_7, ... , x_0, y_7, ... , y_0, x_7x_6, x_7x_5, ... , x_1x_0, x_7y_7, x_7y_6, ... , x_0y_0, y_7y_6, y_7y_5,…, y_1y_0 }.

Соответственно, для S-блока шифра «Лабиринт» размерность матрицы имеет вид $\left(2^8\right)\times\left(C_{16}^2+16+1\right)$, т.е. 256×137. Фрагмент построенной матрицы приведен в таблице 1.

Таблица 1 – фрагмент матрицы значений термов степени не выше 2 для описания S-блока шифра «Лабиринт»

№	1	x_7	…	x_0	y_7	…	y_0	x_7x_6	...	x_1x_0,	x_7y_7	…	x_0y_0,	y_7y_6,	…	y_1y_0
0	1	0	…	0	0	…	1	0	…	0	0	…	0	0	…	1
1	1	0	…	1	1	…	0	0	…	0	0	…	0	1	…	0
2	1	0	…	0	1	…	0	0	…	0	0	…	0	1	…	0
…	…	…	…	…	…	…	…		…	…	…	…	…	…	…	…
255	1	1	…	1	0	…	1	1	…	1	0	…	1	0	…	1

Полученная матрица используется для построения переопределённой системы уравнений. На основе вычисленных значений формируется 137 уравнений, каждое из которых содержит 256 значений. Использование метода Гаусса позволяет выполнить приведение полученной системы, уже на основании которой вычисляется переопределённая система уравнений.

Для описания S-блока алгоритма шифрования «Лабиринт» была получена переопределённая система из 39 уравнений, несколько из которых приведены ниже.

$$\begin{cases}
1+x_7+x_4+x_2+y_7+y_6+y_3+y_2+y_0+x_7x_6+x_7x_5+x_7x_3+x_7x_0+x_6x_1+x_6x_0+x_5x_4+x_4x_3+\\
+x_4x_1+x_4x_0+x_3x_0+x_1x_0+x_7y_6+x_7y_3+x_7y_2+x_7y_0+x_6y_7+x_6y_5+x_6y_4+x_6y_3+x_6y_2+\\
+x_5y_6+x_5y_5+x_5y_4+x_5y_0+x_4y_7+x_4y_2+x_4y_0+y_7y_6+y_7y_4+y_6y_5+y_6y_3+y_6y_1+y_6y_0+\\
+y_5y_2+y_5y_1+y_2y_0=0\\
x_7+x_4+x_1+y_6+y_4+y_1+x_7x_5+x_7x_4+x_7x_2+x_6x_5+x_6x_4+x_6x_1+x_6x_0+x_5x_1+x_4x_3+\\
+x_4x_2+x_4x_0+x_3x_0+x_2x_1+x_2x_0+x_7y_5+x_7y_2+x_7y_0+x_6y_7+x_6y_5+x_6y_4+x_6y_3+x_6y_1+\\
+x_5y_3+x_5y_2+x_5y_1+x_5y_0+x_4y_7+x_4y_6+x_4y_5+y_7y_3+y_7y_1+y_6y_4+y_6y_3+y_6y_2+y_6y_0+\\
+y_5y_2+y_5y_1+y_4y_3+y_2y_1=0\\
\qquad\vdots\qquad\qquad\qquad\vdots\qquad\qquad\qquad\vdots\\
1+x_7+x_3+x_1+x_0+y_6+y_3+y_1+y_0+x_7x_6+x_7x_3+x_6x_0+x_5x_4+x_4x_3+x_4x_2+x_4x_1+x_4x_0+\\
+x_2x_1+x_2x_0+x_1x_0+x_7y_3+x_6y_5+x_6y_4+x_6y_2+x_6y_1+x_6y_0+x_5y_7+x_5y_3+x_5y_0+x_4y_6+\\
x_4y_5+x_4y_4+x_4y_3+x_3y_7=0
\end{cases}$$

Необходимо отметить, что уравнения справедливы для всех входных наборов, и при этом максимальная степень системы равна 2. Полученный результат свидетельствует об уязвимости S-блока алгоритма шифрования «Лабиринт» с точки зрения алгебраической атаки и потенциальной уязвимости всего шифра в целом.

В ходе дальнейших исследований планируется расширить построенную систему на цикловую функцию шифра «Лабиринт», 16 циклов шифрования и начальное и конечное преобразование.