# Раздел III. Методы и средства криптографии и стеганографии

УДК 003.26.09

**Л.К. Бабенко, Е.А. Маро**

## АЛГЕБРАИЧЕСКИЙ КРИПТОАНАЛИЗ УПРОЩЕННОГО АЛГОРИТМА ШИФРОВАНИЯ RIJNDAEL*

*В работе проведено исследование методов алгебраического криптоанализа. Получены системы уравнений для различных размеров таблиц нелинейных преобразований замены упрощенного алгоритма шифрования Rijndael, а также выполнено решение одной из систем методом XL. В ходе работы программно реализован алгоритм генерации и решения системы уравнений для преобразований замены. Проведен анализ полученных нелинейных систем и выполнена оценка трудоемкости метода XL алгебраического криптоанализа для трех блоков замены.*

*Алгебраический криптоанализ; XL метод; нелинейные преобразования замены; линеаризация нелинейных систем; метод исключения Гаусса; криптографический ключ.*

**L.K. Babenko, E.A. Maro**

## ALGEBRAIC CRYPTANALYSIS OF SIMPLIFIED RIJNDAEL ALGORITHM

*The research of algebraic cryptanalysis method was carried out in this work. Systems of the equations for tables of various sizes of nonlinear transformations of substitution for simplified model of Rijndael algorithm are received, also we solve a one of this systems by a XL method. During this work we produced a program, which has realised a generation and solving of system of equations describing nonlinear transformations of substitution. We analysed a nonlinear systems of equations and calculated a value of complexity of XL method for three blocks of substitution.*

*Algebraic cryptanalysis; XL method; nonlinear transformations of substitution; linearization nonlinear systems; Gauss elimination method; a cryptographic key.*

Криптоанализ долгое время основывался на статистических подходах. Таким статистическим методам криптоанализа как линейный и дифференциальный для осуществления атаки требуется большое количество открытых текстов и шифротекстов. Кроме того, современные алгоритмы шифрования разрабатывались с учетом обеспечения стойкости к подобного рода атакам. Актуальность алгебраиче-

* Работа поддержана грантом РФФИ № 09-07-00245-а.

ских методов криптоанализа базируется на возможности взлома с их помощью алгоритмов шифрования при наличии у криптоаналитика всего одной пары открытый текст/шифротекст. Также важно отметить, что данные методы применимы к стойким современным шифрам, таким как алгоритмы шифрования Rijndael, Serpent.

В данной работе проведена разработка и исследование XL метода алгебраического криптоанализа. Исследование проводилось с помощью разработанного программного приложения, позволяющего генерировать системы уравнений для нелинейных преобразований, а именно для S-блоков замены. Сущность данного метода заключается в получении уравнений, описывающих нелинейные преобразования замены S-блоков, с последующим решением найденных систем уравнений и получением ключа шифрования. Данный метод криптоанализа относится к атакам с известным открытым текстом, поэтому в ходе работы использовалась одна пара открытый текст/шифротекст. В результате осуществления атаки криптоаналитик вычисляет секретный ключ.

Алгебраические методы криптоанализа состоят из следующих этапов:

- составление нелинейной системы уравнений, описывающей преобразования в S-блоках;
- решение нелинейной системы.

Рассмотрим подробнее первый этап алгебраического криптоанализа. Для шифров, подобных Rijndael, при составлении уравнений используется таблица замены S-блоков. Ограничимся рассмотрением одночленов, состоящих из произведения двух переменных. Тогда уравнения, описывающие работу S-блоков, имеют вид [1]:

$$\sum \alpha_{ij} x_i x_j + \sum \beta_{ij} y_i y_j + \sum \gamma_{ij} x_i y_j + \sum \delta_i x_i + \sum \varepsilon_i y_i + \eta = 0,$$

где $x_i x_j$ - комбинация входных битов S-блока;

$y_i y_j$ - комбинация выходных битов S-блока;

$x_i y_j$ – комбинация входных и выходных битов;

$x_i$ и $y_i$ – соответственно входные и выходные биты S-блока;

$\eta$ – коэффициент, принимающий значения 0 или 1.

При получении уравнений нужно рассмотреть все возможные комбинации данных одночленов. В случае, когда число бит на входе S-блоков равно s, получаем, что число одночленов, встречающихся в системе, вычисляется по формуле $t=\frac{2s}{2}+2s+1$ и включает в себя входные и выходные значения S-блока (2s), все их возможные произведения $\binom{2s}{2}$ и коэффициент $\eta$. Число всех возможных комбинаций одночленов составляет $2^t$. Для проверки всех полученных комбинаций на соответствие заданному S-блоку требуется составить таблицу истинности на основании замен, выполняемых в исследуемом S-блоке. В общем виде таблица истинности для S-блока содержит $2^s$ строк и t столбцов и имеет вид, представленный в табл. 1. Входные и соответствующие им выходные значения S-блока определяются таблицей замены, значения сочетаний определяются путем вычисления произведения соответствующих элементов.

Таблица 1

**Общий вид таблицы истинности для S-блока**

| | Входные значения S-блока | | | Выходные значения S-блока | | | Все сочетания входных и выходных значений S-блока | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Все возможные входные значения S-блока (от 0 до $2^s$) | $x_s$ | … | $x_1$ | $y_s$ | … | $y_1$ | $x_sx_{s-1}$ | … | $x_2x_1$ | $y_sy_{s-1}$ | … | $y_2y_1$ | $x_sy_s$ | … | $x_1y_1$ | η |
| | 0 | … | 0 | 1 | … | 1 | | | | | | | | | | 1 |
| | … | | | | | | | | | | | | | | | |
| | 1 | … | 1 | 0 | … | 1 | | | | | | | | | | 1 |

Для проверки комбинаций на соответствие таблице истинности следует осуществить построковую подстановку значений одночленов из таблицы и выполнить операцию сложения по модулю 2. Таким образом, для каждой комбинации выполняется подстановка и сложение для всех возможных входных значений S-блока ($2^s$ раз). Результаты суммирования сравниваются с нулем. Если для всех строк таблицы истинности равенство оказывается верным, то уравнение, заданное данной комбинацией одночленов, удовлетворяет таблице замены исследуемого S-блока, и его следует отобрать для составления искомой системы. Далее необходимо провести анализ уравнений и выбрать для формирования системы уравнения, содержащие минимальное число нелинейных элементов. Предлагаемый в работе метод формирования системы будет раскрыт ниже на примере конкретного S-блока.

Второй этап алгебраического криптоанализа заключается в решении нелинейной системы. В криптоанализе разработаны различные подходы к решению нелинейных систем булевых уравнений. Наиболее эффективными, как показывает практика криптоанализа, являются методы, использующие линеаризацию исходной системы. В данной работе исследован XL метод алгебраического криптоанализа.

XL метод (eXtended Linearization) предложен Nicolas Courtois, Alexander Klimov, Jacques Patarin и Adi Shamir в работе [2].

Пусть имеется нелинейная система, содержащая m уравнений и 2s переменных. XL метод базируется на умножении каждого уравнения 1…m на произведения переменных степени меньшей или равной D-2. Рассмотрим вычисление параметра D алгоритма XL атаки. При умножении исходных уравнений системы на одночлены степени ≤(D-2) получаем примерно $R \approx \binom{2s}{\mathrm{D}-2} m$ новых уравнений. Общее число одночленов, встречающихся в этих уравнениях, составляет $T = \binom{2s}{D}$. Так как система будет решаться способом линеаризации, то есть путем замены всех нелинейных одночленов на новые переменные, необходимо чтобы число уравнений было больше числа одночленов $R = \binom{2s}{\mathrm{D}-2} m \geq \binom{2s}{D} = T$. Отсюда полу-

чаем, что $m \geq \binom{2s}{D} / \binom{2s}{D-2} \approx (2s)^2 / D^2$. Следовательно, $D \approx \frac{2s}{\sqrt{m}}$. При этом должно выполняться условие D>2, иначе не будет получено новых уравнений, так как степень отобранных для умножения уравнений одночленов, определяемая разностью D-2, будет равна нулю.

*Алгоритм XL метода* состоит из двух шагов:

- Multiply: умножение каждого уравнения исходной системы на произведение переменных в степени $\leq$ D-2.
- Linearize: замена каждого одночлена в степени $\leq$ D на новую переменную и применение метода исключения Гаусса.

Следуя алгоритму, после определения параметра D, нужно составить список исходных переменных и список одночленов в степени меньшей или равной D-2. Затем произвести умножение уравнений и добавить к исходной системе полученные в результате умножения новые уравнения. Для решения системы каждый нелинейный элемент (вида $x_i x_j$ или $x_i y_j$, или $y_i y_j$) в этих уравнениях заменяется новой переменной $u_g$. В результате система становится линейной относительно новых переменных, поэтому данный метод называется линеаризацией. Для возможности нахождения решения линейной системы необходимо, чтобы количество уравнений было не меньше, чем число новых неизвестных. Чаще всего для решения линейной системы используется метод исключения Гаусса. После нахождения решений линейной системы уравнений относительно новых переменных выполняется вычисление решений первоначальной нелинейной системы путем решения систем специального вида ($x_i y_j = u_g$ или $x_i x_j = u_g$, или $y_i y_j = u_g$,) для каждого полученного решения линейной системы [3].

Трудоемкость атаки определяется трудоемкостью нахождения решений системы линейных уравнений методом исключения Гаусса, пренебрегая трудоемкостью решения систем специального вида. Трудоемкость алгебраической атаки методом XL составляет ($T^3$).

Выполним алгебраический криптоанализ методом XL упрощенной модели алгоритма шифрования Rijndael, схема которого представлена на рис. 1. Размер шифруемого блока данных и размер ключа шифрования для данного алгоритма равен 12 бит. Результаты всех операций алгоритма шифрования представляются в виде состояний. Пусть имеется 12-битовое значение 100 010 011 101, тогда состояние записывают в виде $\begin{pmatrix} 100 & 011 \\ 010 & 101 \end{pmatrix}$. В алгоритме шифрования параллельно используются четыре S-блока размерами 3x3 бита.

В начале алгоритма шифрования выполняется сложение по модулю два входного текста и начального ключа. Полученное значение, обозначим его x, разбивается на части, равные размеру S-блока, и подается на вход S-блоков, в которых происходит нелинейное преобразование согласно заданной таблице замены. Замена в S-блоках имеет вид:

| x | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| y | 7 | 6 | 0 | 4 | 2 | 5 | 1 | 3 |

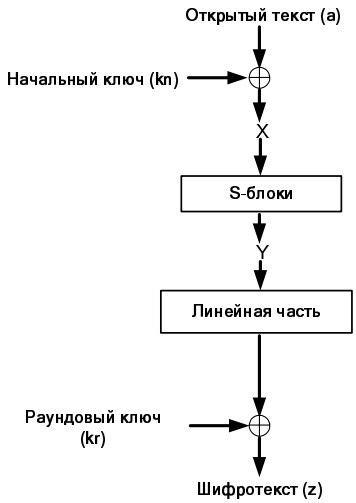


*Рис. 1. Уменьшенный алгоритм шифрования Rijndael*

Выходы S-блоков (y) конкатенируются, после чего выполняются линейные преобразования шифра: операция ShiftRow, заключающаяся в обмене значений строк состояния, и операция MixColumns, осуществляющая перемешивание столбцов состояния.

Заключительным шагом алгоритма служит сложение по модулю два значения, полученного после выполнения линейных операций, и раундового ключа. В результате происходит зашифрование открытого текста. Обозначим шифротекст через z.

Рассмотрим получение нелинейной системы уравнений. Для исследуемого примера число одночленов t равно 22, для генерации уравнений используются следующие одночлены $\{x_1, x_2, x_3, y_1, y_2, y_3, x_1x_2, x_1x_3, x_2x_3, y_1y_2, y_1y_3, y_2y_3, x_1y_1, x_1y_2, x_1y_3, x_2y_1, x_2y_2, x_2y_3, x_3y_1, x_3y_2, x_3y_3, \eta\}$.

Всего можно сгенерировать $2^{22}$=4 194 304 комбинации одночленов. Составим таблицу истинности. Для исследуемого S-блока таблица истинности задается табл. 2.

Таблица 2

**Таблица истинности для S-блока**

| $x_3$ | $x_2$ | $x_1$ | $y_3$ | $y_2$ | $y_1$ | $x_3x_2$ | $x_3x_1$ | $x_3y_3$ | $x_3y_2$ | $x_3y_1$ | $x_2x_1$ | $x_2y_3$ | $x_2y_2$ | $x_2y_1$ | $x_1y_3$ | $x_1y_2$ | $x_1y_1$ | $y_3y_2$ | $y_3y_1$ | $y_2y_1$ | $\eta$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 |
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |

После проверки соответствия 4 194 304 комбинаций таблице истинности были составлены 16 383 уравнения, верные для всех возможных входных значений S-блока. Обозначим найденные уравнения «Система 1».

Для формирования искомой нелинейной системы желательно использовать уравнения с минимальным числом квадратных одночленов. Проанализируем полученные уравнения. В ходе анализа выявлено, что из 16 383 уравнений только 10 содержат единственный квадратный элемент (элемент вида $x_iy_j$, $x_ix_j$ или $y_iy_j$). Эти уравнения составляют часть искомой системы уравнений, описывающей работу S-блока. Обозначим отобранные 10 уравнений как «Система 2»:

$$x_3 + x_1 + y_3 + y_1 + x_3y_2 = 0;$$
$$x_3 + y_2 + y_1 + x_1y_2 = 0;$$
$$x_3 + x_1 + y_3 + y_2 + y_1 + y_3y_2 = 0;$$
$$x_1 + y_3 + y_2y_1 = 0;$$
$$x_2 + x_1 + y_3 + y_2 + y_1 + x_3x_2 + 1 = 0;$$
$$x_2 + y_2 + x_3x_1 + 1 = 0;$$
$$x_3 + x_2 + x_1 + y_1 + x_2x_1 + 1 = 0;$$
$$x_2 + x_1 + y_3 + y_2 + y_1 + x_2\,y_1 + 1 = 0;$$
$$x_2 + y_2 + x_1\,y_1 + 1 = 0;$$
$$x_2 + x_1 + y_3 + y_2 + y_3y_1 + 1 = 0.$$

При анализе приведенных выше 10 уравнений видно, что они содержат не все квадратные элементы. Отсутствуют элементы $x_3y_3$, $x_3y_1$, $x_2y_3$, $x_2y_2$ и $x_1y_3$. Таким образом, в системе не используются пять квадратных одночленов.

Искомая нелинейная система уравнений должна содержать максимальное число возможных нелинейных (квадратных) одночленов для наиболее полного задания преобразований, выполняемых в S-блоке замены. Следовательно, необходимо получить уравнения, содержащие недостающие одночлены. При этом также требуется, чтобы уравнения содержали минимальное число нелинейных элементов. В работе [4] предложен следующий способ получения таких уравнений. В уравнениях «Системы 1» производится обнуление всех уже встречавшихся квадратных одночленов, путем сложения по модулю 2 уравнения, содержащего недостающий квадратный одночлен, с уравнением из «Системы 2», включающим в себя обнуляемый одночлен. В ходе сложения большинство левых частей уравнений «Системы 1» приняли нулевое значение, а оставшиеся уравнения содержат недостающие одночлены. В результате получены 15 уравнений:

$$x_2 + x_1 + y_3 + y_2 + y_1 + x_3y_3 + x_3y_1 + 1 = 0;$$
$$x_3 + x_1 + y_2 + y_1 + x_3y_3 + x_2y_3 = 0;$$
$$x_3 + x_2 + y_3 + x_3y_1 + x_2y_3 + 1 = 0;$$
$$x_2 + y_2 + x_3y_3 + x_2y_2 + 1 = 0;$$
$$x_1 + y_3 + y_1 + x_3y_1 + x_2y_2 = 0;$$
$$x_3 + x_2 + x_1 + y_1 + x_2y_3 + x_2y_2 + 1 = 0;$$
$$x_3 + y_3 + y_2 + x_3y_3 + x_3y_1 + x_2y_3 + x_2y_2 = 0;$$
$$x_2 + x_1 + y_2 + x_3y_3 + x_1y_3 + 1 = 0;$$
$$y_3 + y_1 + x_3y_1 + x_1y_3 = 0;$$
$$x_3 + x_2 + y_1 + x_2y_3 + x_1y_3 + 1 = 0;$$
$$x_3 + x_1 + y_3 + y_2 + x_3y_3 + x_3y_1 + x_2y_3 + x_1y_3 = 0;$$
$$x_1 + x_2y_2 + x_1y_3 = 0;$$
$$x_2 + y_3 + y_2 + y_1 + x_3y_3 + x_3y_1 + x_2y_2 + x_1y_3 + 1 = 0;$$

$$x_3 + y_2 + y_1 + x_3y_3 + x_2y_3 + x_2y_2 + x_1y_3 = 0;$$
$$x_3 + x_2 + x_1 + y_3 + x_3y_1 + x_2y_3 + x_2y_2 + x_1y_3 + 1 = 0.$$

Для дальнейшего анализа оставим уравнения, содержащие минимальное число нелинейных элементов. В данном случае отбросим уравнения, содержащие более двух квадратных элементов, то есть уравнения под номерами 7,11,13,14,15. Осталось 10 уравнений («Система 3»):

$$x_2 + x_1 + y_3 + y_2 + y_1 + x_3y_3 + x_3y_1 + 1 = 0;$$
$$x_3 + x_1 + y_2 + y_1 + x_3y_3 + x_2y_3 = 0;$$
$$x_3 + x_2 + y_3 + x_3y_1 + x_2y_3 + 1 = 0;$$
$$x_2 + y_2 + x_3y_3 + x_2y_2 + 1 = 0;$$
$$x_1 + y_3 + y_1 + x_3y_1 + x_2y_2 = 0;$$
$$x_3 + x_2 + x_1 + y_1 + x_2y_3 + x_2y_2 + 1 = 0;$$
$$x_2 + x_1 + y_2 + x_3y_3 + x_1y_3 + 1 = 0;$$
$$y_3 + y_1 + x_3y_1 + x_1y_3 = 0;$$
$$x_3 + x_2 + y_1 + x_2y_3 + x_1y_3 + 1 = 0;$$
$$x_1 + x_2y_2 + x_1y_3 = 0.$$

Для формирования системы, содержащей все квадратные элементы, необязательно к «Системе 2» добавлять все уравнения, содержащие недостающие элементы. Достаточно добавить 4 уравнения «Системы 3», отобранные таким образом, что один квадратный элемент встречается в каждом из них, а остальные не повторяются. Для наглядности группировки уравнений сумму всех линейных элементов обозначим $C_x$, где x – номер уравнения «Системы 3». Можно составить 5 вариантов группировки уравнений:

1 вариант:
$$x_3y_3 + x_3y_1 + C_1 = 0$$
$$x_3y_3 + x_2y_3 + C_2 = 0$$
$$x_3y_3 + x_2y_2 + C_4 = 0$$
$$x_3y_3 + x_1y_3 + C_7 = 0$$

2 вариант:
$$x_3y_1 + x_3y_3 + C_1 = 0$$
$$x_3y_1 + x_2y_3 + C_3 = 0$$
$$x_3y_1 + x_2y_2 + C_5 = 0$$
$$x_3y_1 + x_1y_3 + C_8 = 0$$

3 вариант:
$$x_2y_3 + x_3y_3 + C_2 = 0$$
$$x_2y_3 + x_3y_1 + C_3 = 0$$
$$x_2y_3 + x_2y_2 + C_6 = 0$$
$$x_2y_3 + x_1y_3 + C_9 = 0$$

4 вариант:
$$x_3y_3 + x_2y_2 + C_4 = 0$$
$$x_3y_1 + x_2y_2 + C_5 = 0$$
$$x_2y_3 + x_2y_2 + C_6 = 0$$
$$x_2y_2 + x_1y_3 + C_9 = 0$$

5 вариант:

$$x_3y_3 + x_1y_3 + C_7 = 0$$
$$x_3y_1 + x_1y_3 + C_8 = 0$$
$$x_2y_3 + x_1y_3 + C_9 = 0$$
$$x_2y_2 + x_1y_3 + C_{10} = 0$$

При составлении искомой нелинейной системы уравнений можно использовать любой из пяти вариантов группировки уравнений. В работе используется пятый вариант:

$$x_2 + x_1 + y_2 + x_3y_3 + x_1y_3 + 1 = 0;$$
$$y_3 + y_1 + x_3y_1 + x_1y_3 = 0;$$
$$x_3 + x_2 + y_1 + x_2y_3 + x_1y_3 + 1 = 0;$$
$$x_1 + x_2y_2 + x_1y_3 = 0.$$

Объединяя приведенные выше 4 уравнения и «Систему 2», в результате получим систему уравнений, описывающую работу S-блоков:

$$\begin{cases} x_3 + x_1 + y_3 + y_1 + x_3y_2 = 0; \\ x_3 + y_2 + y_1 + x_1y_2 = 0; \\ x_3 + x_1 + y_3 + y_2 + y_1 + y_3y_2 = 0; \\ x_1 + y_3 + y_2y_1 = 0; \\ x_2 + x_1 + y_3 + y_2 + y_1 + x_3x_2 + 1 = 0; \\ x_2 + y_2 + x_3x_1 + 1 = 0; \\ x_3 + x_2 + x_1 + y_1 + x_2x_1 + 1 = 0; \\ x_2 + x_1 + y_3 + y_2 + y_1 + x_2y_1 + 1 = 0; \\ x_2 + y_2 + x_1y_1 + 1 = 0; \\ x_2 + x_1 + y_3 + y_2 + y_3y_1 + 1 = 0; \\ x_2 + x_1 + y_2 + x_3y_3 + x_1y_3 + 1 = 0; \\ y_3 + y_1 + x_3y_1 + x_1y_3 = 0; \\ x_3 + x_2 + y_1 + x_2y_3 + x_1y_3 + 1 = 0; \\ x_1 + x_2y_2 + x_1y_3 = 0. \end{cases}$$

Аналогичным образом получены системы уравнений для S-блоков размерами 2x2 и 4x4:

| x | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| S(x) | 3 | 2 | 0 | 1 |

(1)

| x | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S(x) | 10 | 4 | 3 | 11 | 8 | 14 | 2 | 12 | 5 | 7 | 6 | 15 | 0 | 1 | 9 | 13 |

(2)

Для S-блока (1) размером 2x2 получена система из 7 уравнений:

$$\begin{cases} x_2 + y_2 + x_2y_2 + 1 = 0; \\ x_1 + y_2 + y_1 + x_2y_2 = 0; \\ x_2 + x_1 + y_1 + x_2y_2 + 1 = 0; \\ y_1 + x_2x_1 + y_2y_1 = 0; \\ x_2 + y_2 + x_2x_1 + x_2y_1 + 1 = 0; \\ x_2 + y_1 + x_2x_1 + x_1y_2 + 1 = 0; \\ x_1 + y_2 + y_1 + x_2x_1 + x_1y_1 = 0. \end{cases}$$

Для S-блока(2) размером 4x4 получена система из 21 уравнения:

$$\begin{cases} 1 + x_1x_2 + x_1x_3 + x_2x_3 + x_1x_4 + x_3x_4 + y_1y_2 + y_3 + y_4 = 0; \\ x_2 + x_1x_2 + x_3 + x_1x_3 + x_2x_3 + x_4 + x_1x_4 + x_2x_4 + y_2 + y_1y_3 + y_4 = 0; \\ 1 + x_1 + x_2 + x_1x_2 + x_3 + x_1x_3 + x_1x_4 + y_1y_2 + y_3 + y_4 = 0; \\ x_1 + x_2 + x_1x_2 + x_3 + x_1x_3 + x_2x_3 + x_4 + y_2 + y_3 + y_4 + y_1y_4 = 0; \\ x_1x_2 + x_2x_3 + x_4 + x_1x_4 + x_3x_4 + y_1 + y_2 + y_2y_4 = 0; \\ 1 + x_3 + x_1x_3 + x_2x_3 + x_1x_4 + x_2x_4 + y_2 + y_3 + y_3y_4 = 0; \\ x_1 + x_2 + x_1x_2 + x_3 + x_1x_3 + x_2x_3 + x_4 + x_1x_4 + x_1y_1 + y_2 + y_3 + y_4 + x_4y_4 = 0; \\ 1 + x_2x_3 + x_4 + x_1x_4 + x_2x_4 + y_1 + x_1y_2 + y_3 + y_4 = 0; \\ x_1x_2 + x_3 + x_1x_3 + x_3x_4 + y_1 + y_2 + y_3 + x_1y_3 + y_4 = 0; \\ 1 + x_1 + x_2 + x_1x_2 + x_4 + x_1x_4 + x_2x_4 + y_4 + x_1y_4 + x_4y_4 = 0; \\ 1 + x_3 + x_2x_3 + x_4 + x_1x_4 + x_3x_4 + y_1 + x_2y_1 + y_2 + y_3 + x_4y_4 = 0; \\ x_1 + x_2 + x_1x_2 + x_4 + x_1x_4 + x_3x_4 + x_2y_2 + y_3 + x_4y_4 = 0; \\ x_1 + x_2 + x_3 + x_1x_3 + x_2x_3 + x_4 + x_2x_4 + y_2 + y_3 + x_2y_3 + y_4 = 0; \\ 1 + x_1x_3 + x_2x_3 + x_4 + x_2x_4 + y_1 + y_3 + y_4 + x_2y_4 + x_4y_4 = 0; \\ 1 + x_3 + x_2x_3 + x_1x_4 + x_2x_4 + x_3y_1 + y_2 + y_3 + x_4y_4 = 0; \\ 1 + x_2 + x_1x_2 + x_2x_3 + x_2x_4 + x_3x_4 + x_3y_2 + y_3 + y_4 = 0; \\ x_2 + x_1x_3 + x_2x_3 + x_4 + x_3x_4 + y_1 + x_3y_3 + x_4y_4 = 0; \\ 1 + x_1 + x_2 + x_1x_2 + x_2x_3 + x_2x_4 + x_3x_4 + y_1 + y_2 + x_3y_4 + x_4y_4 = 0; \\ 1 + x_3 + x_2x_3 + x_4 + x_1x_4 + x_3x_4 + x_4y_1 + y_2 + y_3 = 0; \\ x_1x_2 + x_3 + x_1x_3 + x_4 + x_2x_4 + y_1 + y_2 + x_4y_2 + y_4 + x_4y_4 = 0; \\ x_2 + x_1x_2 + x_3 + x_1x_3 + x_2x_3 + x_4 + x_1x_4 + y_2 + x_4y_3 + y_4 + x_4y_4 = 0. \end{cases}$$

В табл. 3 приведены численные характеристики нелинейных системы уравнений для трех S-блоков замены.

Таблица 3

**Численные характеристики нелинейных систем уравнений, полученных для трех S-блоков**

| Размер S-блока в битах | Число уравнений в системе | Количество переменных | Количество квадратных элементов | Трудоемкость XL метода |
|---|---|---|---|---|
| 2x2 | 7 | 4 | 6 | $2^6$ |
| 3x3 | 14 | 6 | 15 | $2^{13}$ |
| 4x4 | 21 | 8 | 28 | $2^{17}$ |

Рассмотрим решение нелинейной системы для S-блока размером 3x3. Исходная система содержит 14 уравнений с 6 переменными. По формуле вычисления коэффициента D алгоритма XL имеем $D \geq \frac{2s}{\sqrt{m}} = \frac{6}{\sqrt{14}} \approx 1{,}6$, но по условию D>2, поэтому используем параметр D=3. Следовательно, систему уравнений нужно умножить на все одночлены первой степени (так как D-2=1), а именно, на переменные $\{x_3, x_2, x_1, y_3, y_2, y_1\}$. При умножении получено $R=2s \cdot m=84$ новых уравнений. В исходной системе присутствовали квадратные элементы, значит, после умножения максимальная степень одночленов будет равна трем. Всего в уравнениях используются 2s=6 переменных, следовательно, число одночленов в новой системе будет равно $t' = \binom{2s}{3} + \binom{2s}{2} + 2s = 41$. При дополнении исходной системы новыми уравнениями, получаем систему из 98 уравнений с 41 одночленом:

$$\begin{cases} x_1 + y_3 + y_2 y_1 = 0; \\ x_3 + y_2 + y_1 + x_1 y_2 = 0; \\ \dots \\ y_3 y_1 + y_1 + x_3 y_1 + x_1 y_3 y_1 = 0; \\ x_3 y_1 + x_2 y_1 + y_1 + x_2 y_3 y_1 + x_1 y_3 y_1 + y_1 = 0; \\ x_1 y_1 + x_2 y_2 y_1 + x_1 y_3 y_1 = 0. \end{cases}$$

Для возможности решения системы методом линеаризации необходимо, чтобы она содержала, по крайней мере столько же линейно-независимых уравнений, сколько одночленов в ней встречается.

Все квадратные и кубические элементы в данной системе в соответствии с алгоритмом метода XL заменяем на новые переменные. При приведении системы уравнений по алгоритму Гаусса к треугольному виду часть из 98 уравнений превратились в тождества, а именно приняли вид 0=0. Треугольная матрица для решаемой линейной системы представлена на рис. 2.

В результате выполнения обратного хода алгоритма исключения Гаусса, вычислено решение линейной системы уравнений.

После возврата к первоначальным переменным и решения специальной системы уравнений, получено, что исходная нелинейная система уравнений, описывающая выполняемые в S-блоках преобразования, имеет решение: $x_3=1$; $x_2=1$; $x_1=0$; $y_3=0$; $y_2=0$; $y_1=1$.

Таким образом, были найдены значения входов и выходов S-блоков. Далее, основываясь на схеме алгоритма шифрования, можно выполнить следующие замены:

- входное значение S-блока представить в виде суммы по модулю 2 открытого текста и начального ключа: x=a+kn;
- выходное значение S-блока записать как результат суммы по модулю 2 шифротекста и раундового ключа: y= z+$k_r$.

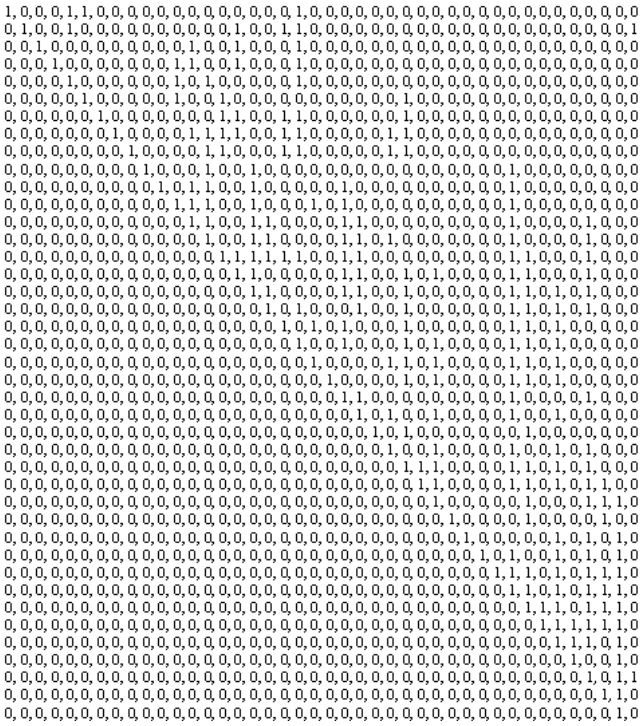

*Рис. 2. Треугольная матрица системы уравнений для S-блока размером 3x3*

Из данных замен выразим начальный и раундовый ключи через известные открытый текст, шифротекст, входы и выходы S-блоков:

$$k_n=a+x,$$

$$k_r=z+y.$$

По условию атаки криптоаналитику доступна одна пара открытый текст/шифротекст. Задан открытый текст a=010 101 001 110 и соответствующий ему шифротекст z=111 011 100 101. Тогда вычисление ключей выполняется следующим образом:

$k_{n0}=a_0+x=010+110=100$, $k_{n1}=a_1+x=101+110=011$, $k_{n2}=a_2+x=001+110=111$,
$k_{n3}=a_3+x=110+110=000$;
$k_{r0}=z_0+y=111+001=110$, $k_{r1}=z_1+y=011+001=010$, $k_{r2}=z_2+y=100+001=101$,
$k_{r3}=z_3+y=101+001=100$.

Начальный ключ $k_n$ равен 100 011 111 000, а раундовый $k_r$ 110 010 101 100.

В работе была выполнена проверка полученных значений ключа. Для этого производилось зашифрование открытого текста на вычисленных ключах и последующее сравнение полученного шифротекста со значением, заданным в начале криптоанализа. На основании проведенных расчетов, можно сделать вывод о правильности вычисления ключей.

Таким образом, для составления системы уравнений, описывающей преобразования замены в S-блоках, оказалось достаточным рассмотрение только входных ($x_i$) и выходных ($y_i$) значений блока замены и их произведений вида $x_iy_j$, $x_ix_j$ и $y_iy_j$.

В данной статье предложен алгоритм получения нелинейной системы уравнений, описывающей преобразования замены в S-блоках. Показано применение данного алгоритма для конкретных таблиц замены S-блоков размерами 2x2, 3x3 и 4x4 бита. Исследован XL метод алгебраического криптоанализа. Для трех таблиц замены вычислены трудоемкости реализации метода XL. Выполнен криптоанализ упрощенного алгоритма шифрования Rijndael, использующего четыре S-блока размером 3x3 бита. В результате получены секретные ключи шифрования, а также выполнена проверка правильности их вычисления.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Nicolas T. Courtois.* How Fast can be Algebraic Attacks on Block Ciphers./ *Nicolas T. Courtois //* Cryptology ePrint Archive, Report 2006/168, 2006.

2. *Courtois N., Klimov A., Patarin J., Shamir A.* Efficient algorithms for solving overdefined systems of multivariate polynomial equations / N. Courtois, A. Klimov, J. Patarin, A. Shamir // EUROCRYPT, 2000. – P. 392–407.

3. *Бабаш А.В., Шанкин Г.П.* Криптография. Аспекты защиты / А.В. Бабаш, Г.П. Шанкин. – М.: Издательский дом «Солон-Р», 2002. – 511 с.

4. *Маро Е.А.* Разработка и исследование алгоритмов алгебраического криптоанализа / Е.А. Маро // Материалы I Всероссийской молодежной конференции по проблемам информационной безопасности ПЕРСПЕКТИВА – 2009. – Таганрог: Изд-во ТТИ ЮФУ, 2009. – С. 259 – 265.

**Бабенко Людмила Климентьевна**
Технологический институт Федерального государственного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: blk@fib.tsure.ru.
347928, г. Таганрог, ул. Чехова, 2, корпус "И".
Тел.: 8 (8634) 312-018.
Кафедра безопасности информационных технологий; профессор.

**Babenko Lyudmila Klimentevna**
Taganrog Institute of Technology – Federal State-Owned Educational Establishment of Higher Vocational Education “Southern Federal University”.
E-mail: blk@fib.tsure.ru.
Block “I”, 2, Chehov str., Taganrog, 347928, Russia.
Phone: 8 (8634) 312-018.
The Department of Security of Information Technologies; professor.

**Маро Екатерина Александровна**
Технологический институт Федерального государственного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: maro-kat@yandex.ru.
347928, г. Таганрог, ул. Чехова, 2, корпус "И".

Тел.: +7 (961) 27-23-100.
Кафедра безопасности информационных технологий; аспирант.

**Maro Ekaterina Aleksandrovna**
Taganrog Institute of Technology – Federal State-Owned Educational Establishment of Higher Vocational Education "Southern Federal University".
E-mail: maro-kat@yandex.ru.
Block "I", 2, Chehov str., Taganrog, 347928, Russia.
Phone: +7 (961) 27-23-100.
The Department of Security of Information Technologies; post-graduate student.

УДК 681.3.067

**Д.П. Рублёв, О.Б. Макаревич, В.М. Федоров**

## МЕТОД СТЕГАНОГРАФИЧЕСКОГО ВСТРАИВАНИЯ СООБЩЕНИЙ В АУДИОДАННЫЕ НА ОСНОВЕ ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ*

*Предлагается стеганографический метод встраивания бинарных сообщений в аудиоданные, основанный на модификации вейвлет-коэффициентов, предназначенный для сокрытия двоичных данных в оцифрованных речевых сообщениях. Встраивание осуществляется модуляцией коэффициентов вейвлет-преобразования, что позволяет повысить стойкость скрытых сообщений к преобразованию формата хранения аудиоданных в форматы с потерей качества.*

*Стеганография; вейвлет-преобразование; корреляция; робастные стегосистемы.*

**D.P. Rublev, O.B. Makarevich, V.M. Fedorov**

## STEGANOGRAPHICAL METHOD FOR MESSAGES EMBEDDING TO AUDIODATA BASED ON THE WAVELET-TRANSFORM

*We propose a steganographical method of binary messages embedding to audio data based on wavelet coefficient modifying, which is intended to hide binary data in digitized speech messages. Embedding in performed via wavelet coefficients modulation which allows to achieve robustness to lossy compression schemes*

*Steganography; wavelet transform; correlation; robust stegosystems.*

В связи с широким распространением сетевых средств передачи мультимедийной информации, в частности, голосового трафика в IP телефонии и трафика видеоданных, актуальным является построение на их основе потоковых стегосистем. Применение в составе стегосистемы методов стеганографии, использующих модификацию наименее значимых бит (НЗБ) исходных мультимедиа-данных ограничивается тем, что передача практически всех потоков мультимедиа-данных ведётся с применением того или иного метода сжатия, основанного на психофизиологической модели восприятия человека, то есть варианта сжатия с потерями. В частности, если рассматривать оцифрованную речь как один из наиболее распространённых источников мультимедиа-трафика, то в зависимости от области

* Работа выполнена при поддержке гранта РФФИ № 09-07-00242-а