Раздел IV. Методы и средства криптографии и стеганографии

УДК 003.26.09

Л.К. Бабенко, Е.А. Маро

АНАЛИЗ СТОЙКОСТИ БЛОЧНЫХ АЛГОРИТМОВ ШИФРОВАНИЯ К АЛГЕБРАИЧЕСКИМ АТАКАМ

Проводится исследование стойкости алгоритма ГОСТ к атаке на основе алгебраического криптоанализа. Суть алгебраического анализа заключается в представлении алгоритма шифрования в виде системы уравнений второй степени, связывающей секретный ключ шифрования с открытым и зашифрованным текстом. В качестве метода решения нелинейной системы уравнений, составленной для блоков замены, в работе рассматривается eXtended Linearization метод. В ходе исследования показано, что для 32 раундов алгоритма шифрования ГОСТ составлена система из 5376 квадратных уравнений, связывающих входы и выходы блоков замены. Общее число переменных равно 2048, в системе содержится 9472 одночлена.

ГОСТ 28147-89; ГОСТ⊕; секретный блок замены; алгебраический криптоанализ; система уравнений второй степени; eXendedLinearization метод; метод исключения Гаусса.

L.K. Babenko, E.A. Maro

ANALYSIS OF RESISTANCE BLOCK CIPHERS AGAINST ALGEBRAIC CRYPTANALYSIS

This paper is devoted to the investigation of GOST algorithm with regard to its resistance against algebraic cryptanalysis. The general idea of algebraic analysis is based on the representation of initial encryption algorithm as a system of multivariate quadratic equations, which define relations between a secret key and a cipher text. Extended linearization method is evaluated as a method for solving the nonlinear system of equations. The research has shown that 32-round GOST is described by a system of 5 376 quadratic equations, which characterize dependencies between inputs and outputs of S-blocks. The total number of variables is 2 048 and the system contains 9 472 monomials.

GOST 28147-89; GOST⊕; S-box; systems of multivariate quadratic equations; algebraic cryptanalysis; extended linearization method; Gaussian elimination.

Введение. Задача анализа надежности используемых криптографических алгоритмов является одним из актуальных направлений в информационной безопасности. Определение стойкости алгоритм шифрования ГОСТ 28147-89 имеет практическое значение и нуждается в дополнительном исследовании в связи с разработкой новых методов криптоанализа. В настоящее время активно развиваются методы алгебраических атак на алгоритмы шифрования. В работах [1, 2] проводится исследование стойкости алгоритмов Advanced Encryption Standard и Data Encryption Standard к алгебраическим атакам, однако в открытой печати до сих пор содержится недостаточное количество исследований, посвященных анализу стойкости алгоритма ГОСТ 28147-89 к данным атакам.

Российский стандарт симметричного шифрования ГОСТ 28147-89 является стойким к большинству криптографических атак, например, методу полного перебора на ключевом пространстве, дифференциальному и линейному криптоанализам [3]. В то же время существует вероятность, что алгоритм ГОСТ 28147-89 может быть уязвим к алгебраическим атакам [4]. Опираясь на методы алгебраического взлома алгоритма Advanced Encryption Standard, проведен анализ возможности применения алгебраических методов криптоанализа для взлома ГОСТ 28147-89, в частности, в данной статье рассмотрен метод Extended Linearization (XL) [5]. Для успешной реализации алгебраических атак, т.е. получения секретного ключа шифрования, достаточно будет обладать одной или небольшим количеством пар: открытый текст/шифротекст.

Алгоритм шифрования ГОСТ 28147-89. Алгоритм шифрования ГОСТ 28147-89 представляет собой 32 раунда зашифрования, построенного по принципу сети Фейстеля [6]. Длина блока открытого текста (T) и шифротекста (C) равна 64 бита (8 байт), секретный ключ шифрования (K) – случайная последовательность длиной 256 бит. Блок открытого текста разбивается на две равные части по 32 бита каждая. Над правой частью открытого текста (T_R) выполняется раундовое преобразование (F), состоящее из трех операций:

- сложение с раундовым ключом по модулю 2^{32};
- замена в восьми секретных S-блоках;
- циклический сдвиг влево на 11 позиций.

Левая часть открытого текста (T_L) складывается по модулю два с результатом раундового преобразования. После чего производится обмен местами правой и левой частей текстов. Схема алгоритма шифрования ГОСТ 28147-89 приведена на рис. 1.

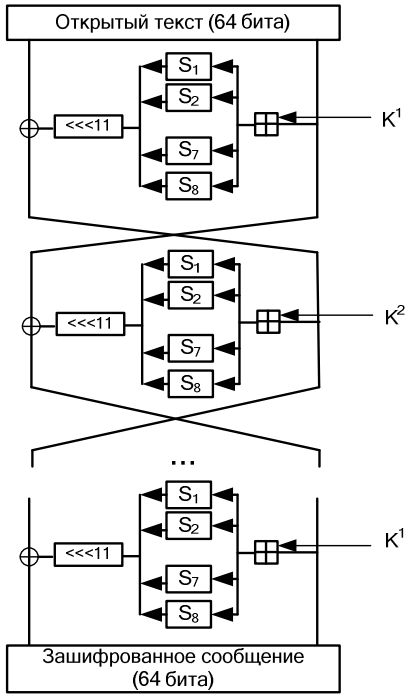

Рис. 1. Алгоритм шифрования ГОСТ 28147-89

Раундовые ключи шифрования вычисляются из исходного секретного ключа путем разбиения его на восемь 32-битных блоков: K_1, K_2,K_3, K_4, K_5, K_6, K_7, K_8. С 1 по 24 раунд ключи используются в прямом порядке: K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_8, K_1, K_2, K_3, K_4, K_5 и так далее. С 25 по 32 раунды ключи берутся в обратном порядке: K_8, K_7, K_6, K_5, K_4, K_3, K_2, K_1.

Алгоритм шифрования ГОСТ⊕. Алгоритм шифрования ГОСТ⊕ по структуре выполняемых операций полностью совпадает с ГОСТ 28147-89, отличием между алгоритмами является способ сложения раундовых ключей: по модулю два в ГОСТ⊕ и по модулю 2^{32} в ГОСТ 28147-89.

Исследуемый алгоритм ГОСТ⊕ использует 8 одинаковых блоков замен, представленных табл. 1. Один раунд шифрования ГОСТ⊕ представлен на рис. 2.

Таблица 1

Блок замены

Вход блока замены	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Выход блока замены	4	10	9	2	13	8	0	14	6	11	1	12	7	15	5	3

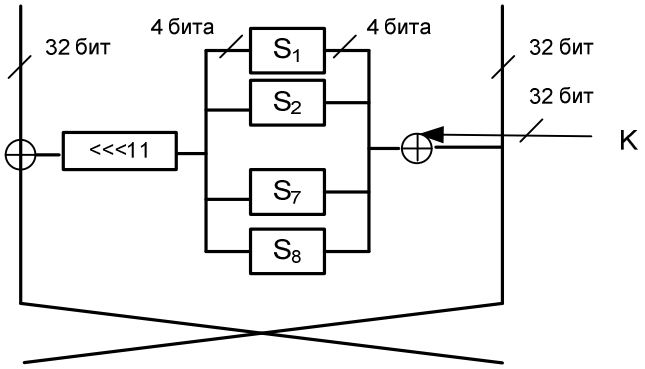

Рис. 2. Один раунд алгоритма шифрования ГОСТ ⊕

Составление системы уравнений. Клод Шеннон в работе [7] предполагал, что для взлома стойкого алгоритма шифрования будет необходимо проделать столько работы, «как для решения системы уравнений с большим числом неизвестных». В настоящее время активно развиваются алгебраические методы криптоанализа, подтверждающие предположение Шеннона. Суть данных методов заключается в представлении преобразований шифрования в виде системы уравнений, связывающей элементы секретного ключа и известные данные. При этом результирующая система содержит произведения неизвестных, вследствие чего задача нахождения решения системы сводится к необходимости решения MQ задачи. Алгебраические атаки являются атаками с известным открытым текстом, результатом успешной атаки служит секретный ключ шифрования.

В общем виде все алгебраические атаки можно разделить на два этапа:

1. Формирование системы уравнений для нелинейных преобразований алгоритмов шифрования.
2. Решение системы уравнений при заданных открытом тексте и шифротексте.

Для большинства блочных алгоритмов шифрования системы уравнений составляются для блоков замен, так как это зачастую единственное используемое в них нелинейное преобразование. Для построения системы формируются уравнения, связывающие вход и выход блоков замены (обозначим их X и Y соответственно). Для отражения нелинейности выполняемой операции искомые уравнения содержат произведения битов входа и выхода блоков. В общем виде уравнения, описывающие преобразования блоков замены, представлены формулой (1)

$$\sum \alpha_{ij} x_i x_j + \sum \beta_{ij} y_i y_j + \sum \gamma_{ij} x_i y_j + \sum \delta_i x_i + \sum \varepsilon_i y_i + \eta = 0, \qquad (1)$$

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;

η – коэффициент, принимающий значения 0 или 1.

Для блока замены размером s бит можно составить 2^t уравнений, где t – число одночленов, встречающихся в уравнениях. Параметр t вычисляется по формуле (2).

$$t = \binom{2s}{2} + 2s + 1, \qquad (2)$$

Для выбора из всего числа возможных уравнений только верных преобразованиям конкретного блока замен формируется таблица проверок уравнений. Общий вид таблицы проверок приведен в табл. 2.

Затем выполняется построчная подстановка значений из таблицы проверок в уравнения. В случае выполнения равенства для всех входов блока замены ($0\text{-}2^s$) уравнение считается соответствующим преобразованиям блока замены. Часть из полученных уравнений, верных преобразованиям замены, являются линейно зависимыми. Для выбора линейно независимых уравнений можно воспользоваться алгоритмом, описанным в работе [8], или вычислить нелинейно независимые уравнения, используя прямой ход алгоритма Гаусса.

Таблица 2

Общий вид таблицы проверки

	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	$x_s x_{s-1}$	..	$x_2 x_1$	$y_s y_{s-1}$	…	$y_2 y_1$	$x_s y_s$	…	$x_1 y_1$	η
	0	…	0	1	…	1										1
	…															
	1	…	1	0	…	1										1

При выборе линейно независимых уравнений можно воспользоваться следующей теоремой [9].

Теорема 1. Для любого блока замены размером nxm бит: $F(x_1, \ldots, x_n) \rightarrow (y_1, \ldots, y_m)$, и для любого подмножества T из t всех возможных одночленов (2^{n+m}),

если выполняется условие $t>2^n$, то существует по меньшей мере $t-2^n$ линейно независимых уравнений, содержащих одночлены из множества T и выполняющиеся с вероятностью 1.

Методы решения системы уравнений, применяемые в криптоанализе. Рассмотрим способы решения полученной системы. Применение к исходной системе метода Гаусса без дополнительных преобразований системы невозможно из-за наличия произведений неизвестных. В источниках [10, 11] для решения подобного рода систем рекомендуется способ линеаризации и его модификация для увеличения числа линейно независимых уравнений – метод eXtended Linearization.

Метод eXtended Linearization предложен Nicolas Courtois, Alexander Klimov, Jacques Patarin и Adi Shamir в работе [1].

Пусть K – некоторое поле, A – система линейно независимых уравнений $l_i=0,(1\le i\le m)$, где каждое l_i – многочлен вида $f_i(x_1, \ldots, x_n) - b_i$. Цель данного метода – получение как минимум одного решения $x = (x_1, \ldots, x_n) \in K^n$, для заданного $b = (b_1, \ldots, b_m) \in K^m$.

В XL алгоритме нужно составить все уравнения вида $(\prod_{j=1}^{k} x_{ij}) * \ell_i = 0$, где $x_{ij} \in (x_1, \ldots x_n)$. Уравнения такого типа обозначим через $x^k \ell$, в то же время данное выражение будет обозначать совокупность всех подобных уравнений. Совокупность элементов степени k обозначим как $x^k = \left\{ \prod_{j=1}^{k} x_{ij}, \quad где \quad x_{ij} \in (x_1, \ldots, x_n) \right\}$. Пусть $D \in N$, тогда I_D – линейное пространство, создаваемое всеми уравнениями вида $x^k \ell$ для $0\le k\le D-2$.

Алгоритм XL метода имеет следующий вид:

а) **Multiply:** составление всех произведений вида $(\prod_{ij}^{k} x_{ij}) * \ell_i \in I_D$, где $k\le D-2$.

б) **Linearize:** рассмотрение каждого одночлена x_i в степени $\le D$ как новой переменной и применение исключения Гаусса к уравнениям, полученным в пункте а).

в) **Solve:** повторение пункта б) до тех пор, пока в результате не будет получено, по крайней мере, одно уравнение с единственной переменной x_i.

г) **Repeat:** упростить уравнения и повторить процесс для нахождения значений других переменных.

Рассмотрим вычисление параметра алгоритма XL атаки. Пусть D=2, 3,… – параметр XL алгоритма. Алгоритм основан на умножении всех уравнений системы (m) на произведения переменных (n) в степени D–2. В результате умножения получаем примерно $R \approx \binom{n}{D-2} m$ новых уравнений. Общее число одночленов, встречающихся в этих уравнениях, составляет $T = \binom{n}{D}$. Большинство из полученных уравнений являются линейно независимыми. В этом случае нужно выбрать достаточно большое D такое, что выполняется условие (3):

$$R = \binom{n}{D-2} m \ge \binom{n}{D} = T \cdot \qquad (3)$$

Очевидно, что число линейно независимых уравнений не может превышать число одночленов T. Если система имеет единственное решение, то существует значение D, для которого выполняется неравенство $R \geq T$. Причем число линейно независимых уравнений из R будет достаточно близко к T. Если разность числа одночленов (T) и линейно независимых уравнений не велика, то система будет решаема. Наиболее легко система будет решена при очень маленьком значении данной разности.

Ожидается, что значение D, при котором применим метод XL, будет равным или близким к теоретическому значению параметра D. В этом случае, XL алгоритм будет эффективен при условии (4).

$$R \geq T \quad \Rightarrow \quad m \geq \binom{n}{D} / \binom{n}{D-2} \approx n^2 / D^2. \tag{4}$$

Из формулы (4) получаем, что параметр атаки D вычисляется по формуле (5):

$$D \approx \frac{n}{\sqrt{m}}. \tag{5}$$

Алгебраический криптоанализ ГОСТ⊕. Составим систему уравнений, описывающую преобразования в блоке замены 4x4, заданном табл. 3.

Таблица 3

Блок замены для составления системы уравнений

Вход блока замены	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Выход блока замены	4	10	9	2	13	8	0	14	6	11	1	12	7	15	5	3

Для данного блока всего можно составить 2^{37}=137438953472 уравнений вида (1). Составим таблицу истинности для проверки соответствия уравнений преобразованиям в блоке. Таблица истинности представлена на рис. 3.

x4	x3	x2	x1	y4	y3	y2	y1	x4x3	x4x2	x4x1	x3x2	x3x1	x2x1	y4y3	y4y2	y4y1	y3y2	y3y1	y2y1	x4y4	x4y3	x4y2	x4y1	x3y4	x3y3	x3y2	x3y1	x2y4	x2y3	x2y2	x2y1	x1y4	x1y3	x1y2	x1y1
0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	1	1	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	
0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	
0	0	1	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	
0	1	0	0	1	1	0	1	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	
0	1	0	1	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	
0	1	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
0	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1	0	1	0	0	0	0	0	0	1	1	1	0	1	1	1	0	1	1	1	0
1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	1	1	0	1	1	0	0	1	0	0	0	0	1	1	0	0	1	1	0	1	1	0	0	0	0	0	0	0	0	1	0	1	1
1	0	1	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	
1	0	1	1	1	1	0	0	0	1	1	0	0	1	1	0	0	0	0	0	1	1	0	0	0	0	0	1	1	0	0	1	1	0	0	
1	1	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	1	1	1	0	1	1	1	0	1	1	1	1	0	0	0	0	0	0	
1	1	0	1	1	1	1	1	1	0	1	0	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	
1	1	1	0	0	1	0	1	1	1	0	1	0	0	0	0	1	0	0	1	0	1	0	1	0	1	0	1	0	1	0	0	0	0	0	
1	1	1	1	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1

Рис. 3. Таблица истинности исследуемого блока замены 4x4 бита

При проверке возможных 2^{37} уравнений верными таблице истинности оказались 2 097 151 уравнения. Выделение из общего числа уравнений только линейно независимых выполним с помощью алгоритма Гаусса (прямой ход). Для исследуемого нами блока замены после преобразования системы по алгоритму Гаусса получено 21 линейно независимое уравнение (6).

$$x_4+x_4y_2+x_3y_3+x_3y_1+x_2y_4+x_2y_1=0$$

$$x_3+x_3x_2+x_4y_1+x_3y_3+x_3y_2+x_2y_4+x_2y_3+x_2y_2+x_2y_1+x_1y_4+x_1y_3+x_1y_2+x_1y_1=0$$

$$x_2+x_3x_2+x_2y_3+x_2y_2+x_2y_1=0$$

$$x_1+x_4y_1+x_3y_2+x_2y_4+x_2y_2+x_2y_1+x_1y_4+x_1y_3+x_1y_1=0$$

$$y_4+x_4y_1+x_3y_1+x_2y_3+x_2y_1+x_1y_4+x_1y_3+x_1y_1=0$$

$$y_3+x_3x_2+x_2y_2+x_2y_1+x_1y_4+x_1y_3+1=0$$

$$y_2+x_4y_2+x_1y_2+x_1y_1=0$$

$$y_1+x_3y_1+x_2y_3+x_2y_1+x_1y_3+x_1y_1=0$$

$$x_4x_3+x_4y_1+x_3y_4+x_3y_2+x_3y_1+x_2y_4+x_2y_2+x_2y_1+x_1y_4+x_1y_2+x_1y_1=0$$

$$x_4x_2+x_4y_1+x_3y_2+x_1y_3+x_1y_1=0$$

$$x_4x_1+x_4y_1+x_3y_4+x_3y_1+x_2y_4+x_2y_3+x_2y_2+x_2y_1+x_1y_4+x_1y_2=0 \qquad (6)$$

$$x_3x_1+x_3y_3+x_3y_1+x_2y_2+x_1y_4+x1y_3+x_1y_2=0$$

$$x_2x_1+x_4y_1+x_3y_4+x_3y_1+x_2y_4+x_2y_3+x_2y_1+x_1y_4+x_1y_2+x_1y_1=0$$

$$y_4y_3+x_4y_1+x_3y_4+x_3y_2+x_2y_4+x_2y_2+x_2y_1+x_1y_4+x_1y_3+x_1y_2+x_1y_1=0$$

$$y_4y_2+x_4y_1+x_3y_2+x_2y_4+x_2y_2+x_2y_1+x_1y_3+x_1y_2+x_1y_1=0$$

$$y_4y_1+x_3y_3+x_3y_2+x_2y_4+x_2y_3+x_1y_1=0$$

$$y_3y_2+x_4y_4+x_4y_2+x_4y_1+x_3y_3+x_3y_2+x_3y_1+x_2y_4+x_2y_1+x_1y_1=0$$

$$y_3y_1+x_4y_4+x_4y_1+x_3y_4+x_2y_4+x_2y_3+x_2y_2+x_2y_1+x_1y_4+x_1y_2=0$$

$$y_2y_1+x_4y_4+x_3y_2+x_1y_3=0$$

$$x_4y_4+x_3y_4+x_3y_3+x_3y_2+x_2y_3+x_2y_2+x_1y_4+x_1y_3+x_1y_2+x_1y_1=0$$

$$x_4y_3+x_4y_2+x_4y_1+x_3y_4+x_3y_1+x_2y_4+x_2y_2+x_2y_1+x_1y_4+x_1y_3+x_1y_2=0$$

Система, описывающая преобразования в одном раунде шифрования ГОСТ⊕, содержит 168 линейно независимых уравнения и 64 неизвестных. Число одночленов, встречающихся в системе, равно 36·8=288.

Проведем атаку на два раунда данного алгоритма шифрования. Исходные данные атаки: открытый текст

$$T=975865455312564352=$$
$$=0000110110001010111110000111011000010100011110101111000010000000_2,$$

шифротекст

$$C=4092806235576314598=$$
$$=1100011100110011011011100110100111010001111110000101010100011010_2.$$

Имеется система, описывающая преобразования одного раунда алгоритма шифрования. Система содержит 168 линейно независимых уравнения, 64 неизвестных и 288 одночленов. Используя метод линеаризации, найти решение не представляется возможным, так как система содержит недостаточное число уравнений для возможности замены всех одночленов новыми переменными. Число уравнений в системе в данном случае должно быть больше, либо равно 288.

Структура исследуемого алгоритма представлена на рис. 4. На предыдущем этапе составлена система уравнений, связывающая вход и выход блоков замены. Как видно из рисунка 4, при атаке на два раунда алгоритма ГОСТ⊕ можно представить выходное значение блоков замены (Y) как сумму известных открытого текста и шифротекста по формуле (7).

$$Y_1=(T_L \oplus C_R)>>>11, \text{ для первого раунда}$$
$$Y_2=(T_R \oplus C_L)>>>11, \text{ для второго раунда.} \quad (7)$$

Выполнив замену Y в двух раундах на конкретное значение, соответствующее заданным открытому тексту и шифротексту, мы получаем, что число неизвестных в системах будет сокращено с 64 (x_{32}–x_1, y_{32}–y_1) до 32 (x_{32}–x_1). А число одночленов, встречающихся в системах, уменьшится до 80.

Вычислим выходное значение блока замены по формуле (7). Выходное значение для первого раунда шифрования будет равно

$$Y_1=(T_L \oplus C_R)>>>11=$$
$$=(00001101100010101111100001110110_2 \oplus 11010001111110000101010100011010_2)>>>11=$$
$$=11011100011100101010110101101100_2>>>11=$$
$$=10101101100110111000111001010101_2.$$

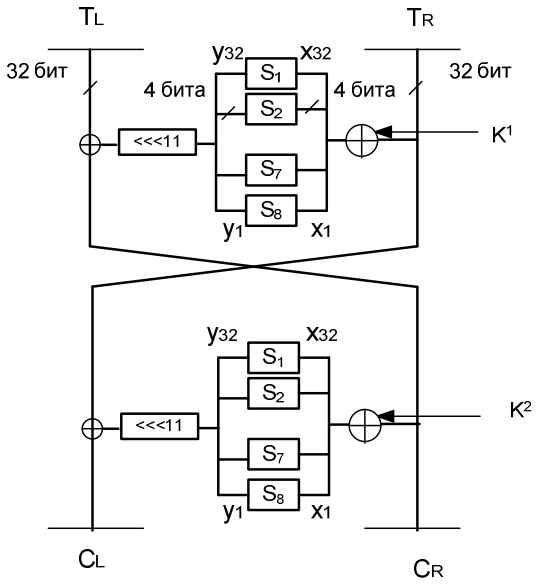

Рис. 4. Два раунда алгоритма шифрования ГОСТ⊕

Выполним подстановку значения Y_1 в систему уравнений (6), описывающую преобразования первого раунда шифрования. Решением данной системы является значение X_1= $0001010000101001010101111111011 10_2$.

Тогда из структуры алгоритма шифрования ГОСТ⊕ следует, что ключ первого раунда (K_1) вычисляется по формуле (8).

$$K_1=X_1 \oplus T_R \quad (8)$$
$$K_1=00010100001010010101011111101110_2 \oplus 00010100011110101111000010000000_2=$$
$$=01010011101001110110111 0_2=5482350.$$

Рассчитаем выходное значение блока замены Y_2 для второго раунда по формуле (7).

$$Y_2=(C_L \oplus T_R)>>>11=$$
$$=(11000111001100110111011100110100 1_2 \oplus 00010100011110101111000010000000_2)>>>11=$$
$$=11010011010010011001111011101001_2>>>11=$$
$$=11011101001110100110100100110011_2.$$

Тогда решением системы для второго раунда является значение

$$X_2= 01000100111100011000001011111111_2.$$

Как видно из структуры алгоритма шифрования ГОСТ⊕, ключ второго раунда ($К_2$) может быть вычислен по формуле (9).

$$K_2=X_2 \oplus C_R \quad (9)$$
$$K_2=X_2 \oplus C_R=$$
$$=01000100111100011000001011111111_2 \oplus 11010001111110000101010100011010_2=$$
$$=10010101000010011101011111100101_2=2500450277.$$

Выполнена проверка полученных ключей путем зашифрования исходного открытого текста. В результате подтверждено, что найден искомый секретный ключ шифрования.

Криптоанализ трех и более раундов ГОСТ⊕. Аналогично атаке на два раунда алгоритма шифрования ГОСТ⊕ система, описывающая преобразования в блоках замены, задана уравнениями (6). Однако для трех и более раундов шифрования сразу выразить выход блоков замены в виде числа через сумму открытого текста и шифротекста будет невозможно. Следовательно, сократить число неизвестных в системе таким образом не удастся.

Рассмотрим три раунда шифрования. Система содержит 3·21·8=504 уравнения, 192 неизвестных и 36·8·3=864 одночлена. Применение метода линеаризации, используемого при анализе двух раундов, не позволяет однозначно найти решение системы. Обратимся к методу eXtended Linearization (XL) для получения дополнительных линейно независимых уравнений. В данном исследовании метод XL применялся отдельно к системе, сформированной для каждого блока замены. То есть производилось домножение уравнений, составленных для конкретного блока замены, на одночлены, встречающиеся в уравнениях данного блока замены. В этом случае D для любого из используемых блоков замены вычисляется по формуле (10) и будет равно:

$$D \approx \frac{8}{\sqrt{21}} \approx 1{,}75. \quad (10)$$

То есть, следует использовать D=3, так как должно выполняться условие D>2. Для каждого блока замены мы имеем дополнительно 21·8=168 уравнений. Система, описывающая работу одного блока замены, содержит 189 уравнений (21 исходное и 168 дополнительно полученных методом XL), 8 неизвестных и число уникальных одночленов, равное $t'=\binom{8}{3}+\binom{8}{2}+8=92$. Система, описывающая преобразования в одном раунде шифрования, будет содержать 8·189=1512 уравнения, 64 неизвестных и не более 9 472 уникальных одночленов (которые затем рассматриваются как новые переменные).

Тогда, возвращаясь к анализу трех раундов алгоритма ГОСТ⊕, получаем систему из 1 512·3=4 536 уравнений с 192 неизвестными и 2 208 уникальными одночленами.

Для N раундов шифрования система будет содержать 1 512·N уравнений с 64·N неизвестными и 736·N уникальными одночленами. Рассчитаем данные характеристики для полного алгоритма ГОСТ⊕ (32 раунда): число уравнений равно 48 384, число неизвестных – 2 048, число одночленов – 23 552.

Сложность атаки полагается равной сложности решения системы линейных уравнений. Сложность решения методом Гаусса системы, описывающей зашифрование в 32 раундах, составит $(23552)^3 \approx (2^{15})^3 = 2^{45}$.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Courtois N., Pieprzyk J.* Cryptanalysis of block ciphers with overdefined systems of equations / N. Courtois, J. Pieprzyk // ASIACRYPT. – 2002. – P. 267-287.
2. *Courtois N., Gregory V. Bard.* Algebraic Cryptanalysis of the Data Encryption Standard // 11-th IMA Conference, 2007. – P. 152-169.
3. *Панасенко С.П.*Стандарт шифрования ГОСТ 28147-89. Обзор криптоаналитических исследований. // http://www.cio-world.ru/–15 Августа, 2007.
4. *Бабенко Л.К., Маро Е.А.* Криптоанализ блочных алгоритмов шифрования // Системы высокой доступности. – 2011. – № 2 (7). – С. 13-16.
5. *Courtois N., Klimov A., Patarin J., Shamir A.* Efficient algorithms for solving overdefined systems of multivariate polynomial equations // EUROCRYPT. – 2000. – P. 392-407.
6. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М.: Изд-во стандартов, 1989. – 28 с.
7. *Шеннон К.* Теория связи в секретных системах // http://www.enlight.ru/crypto/articles/shannon/shann__i.htm.
8. *Маро Е.А.* Алгебраический криптоанализ упрощенного алгоритма шифрования Rijndael // Известия ЮФУ. Технические науки. – 2009. – № 11 (110). – С. 187-199.
9. *Kipnis A., Shamir A.,* Cryptanalysis of the HFE public key cryptosystem by relinearization // Advances in Cryptology–Crypto'99. – Springer, 1999. – (Lect. NotesComput. Sci. Vol. 1666). – P. 19-30.
10. *Kleiman E.,* The XL and XSL attacks on Baby Rijndael //http://orion.math.iastate.edu/dept/thesisarchive/MS/EKleimanMSSS05.pdf.
11. *Бабаш А.В., Шанкин Г.П.* Криптография. Аспекты защиты. – М.: Издательский дом «Солон-Р», 2002. – 511 с.

Статью рекомендовал к опубликованию д.т.н., профессор Н.И. Витиска.

Бабенко Людмила Климентьевна
Технологический институт федерального государственного автономного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: blk@fib.tsure.ru.
347928, г. Таганрог, ул. Чехова, 2.
Тел.: 88634312018.
Кафедра безопасности информационных технологий; д.т.н.; профессор.

Маро Екатерина Александровна
E-mail: marokat@gmail.com.
Тел.: +79185209219.
Кафедра безопасности информационных технологий; аспирантка.

Babenko Lyudmila Klimentevna
Taganrog Institute of Technology – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education "Southern Federal University".
E-mail: blk@fib.tsure.ru.
2, Chekhov Street, Taganrog, 347928, Russia.
Phone: +78634312018.
The Department of Security of Information Technologies; Dr. of Eng. Sc.; Professor.

Maro Ekaterina Aleksandrovna
E-mail: marokat@gmail.com.
Phone: +79185209219.
The Department of Security of Information Technologies; Postgraduate Student.