Алгебраический анализ стойкости криптографических систем защиты информации

Е.А. Маро

Задача анализа надежности используемых криптографических алгоритмов является одним из актуальных направлений в информационной безопасности. При выборе алгоритма для анализа стойкости авторы руководствовались следующими соображениями:

- Стандарт симметричного шифрования ГОСТ 28147-89 [1] используется в большинстве российских средств защиты конфиденциальной информации.
- Алгоритм ГОСТ 28147-89 рассматривается в качестве международного стандарта шифрования в ISO 18033.

Алгоритм шифрования ГОСТ 28147-89 в режиме простой замены представляет собой 32 раунда зашифрования, построенного по принципу сети Фейстеля. Длина блока открытого текста (Т) и шифротекста (С) равна 64 бита (8 байт), секретный ключ шифрования (К) - случайная последовательность длиной 256 бит. Блок открытого текста разбивается на две равные части по 32 бита каждая. Над правой частью открытого текста выполняется раундовое преобразование (F), состоящее из трех операций:

- Сложение с раундовым ключом по модулю 232;
- Замена в восьми секретных S-блоках;
- Циклический сдвиг влево на 11 позиций.

Левая часть открытого текста 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.

Раундовые ключи шифрования вычисляются из исходного секретного ключа путем разбиения его на восемь 32-битных блоков: К1, К2,К3, К4, К5, К6, К7, К8. С 1 по 24 раунд ключи используются в прямом порядке: К1, К2,

К3, К4, К5, К6, К7, К8, К1, К2, К3, К4, К5 и так далее. С 25 по 32 раунды ключи берутся в обратном порядке: К8, К7, К6, К5, К4, К3, К2, К1.

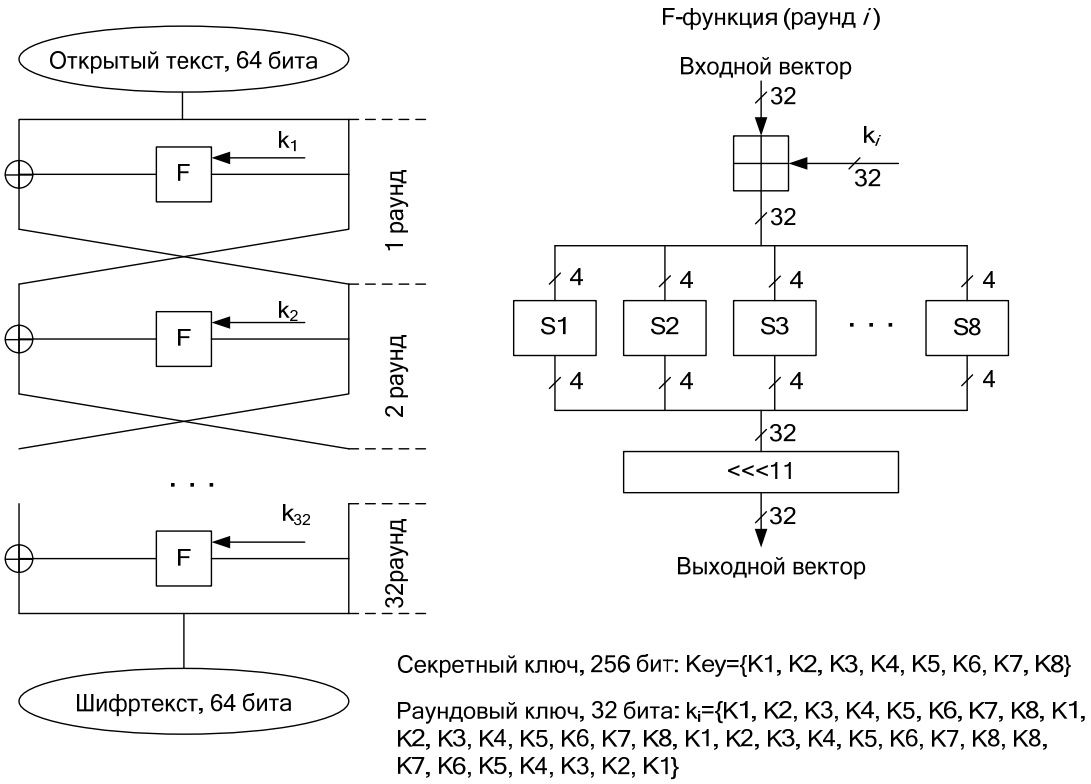

Рисунок 1 - Алгоритм шифрования ГОСТ 28147-89

Российский стандарт симметричного шифрования ГОСТ 28147-89 является стойким к большинству криптографических атак, например, методу полного перебора на ключевом пространстве, дифференциальному и линейному криптоанализам [2]. В тоже время существует вероятность, что алгоритм ГОСТ 28147-89 может быть уязвим к алгебраическим атакам [3]. Опираясь на методы алгебраического взлома алгоритма Advanced Encryption Standard [4,5], проведен анализ возможности применения алгебраических методов криптоанализа для взлома ГОСТ 28147-89, в частности в данной статье рассмотрен метод Extended Linearization (XL) [6].

Учитывая, что алгебраические атаки в основе своей используют представление нелинейных преобразований шифрования в виде системы уравнений, необходимо знать таблицы замен. Блоки замены, используемые в конкретной реализации алгоритма ГОСТ 28147-89, являются дополнительным секретным элементом. В тоже время существует метод восстановления блоков замены, с которым можно ознакомиться в работах [7-

9]. Метод основан на использовании «накрывающего» свойства сети Фейстеля. Данное свойство заключается в том, что при идентичных раундах шифрования прохождение текста через четное число раундов сети Фейстеля повлечет изменение только половины выходного блока (шифротекста). Для соблюдения требования идентичности раундов используется нулевое значение секретного ключа (атака на выбранных ключах), при этом все раундовые ключи будут также равны нулю. Первый этап атаки - нахождение нулевого вектора (z), который равен раундовому преобразованию шифрования от нулевого значения z = F(0). Второй этап - восстановление таблицы блока замены по «накрывающему» свойству. Для алгоритма ГОСТ 28147-89 атака требует выполнения не более 2^{32} операций зашифрования для однозначного определения таблиц замены.

Рассмотрим один раунд алгоритма ГОСТ⊕. Необходимо составить систему уравнений для 8-ми параллельно используемых S-блоков. Выполним составление уравнений для одного блока, заданного таблицей 1. Аналогичным образом выполняет поиск линейно независимых уравнений для оставшихся 7 блоков замены.

Таблица 1. Таблица замены S-блока

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

Сначала составляем все уравнения вида (1). Число таких уравнений равно 2^{37}=137438953472, число одночленов в них – 37, число переменных – 8.

$$\sum_{i,j=0}^{4} \alpha x_i x_j + \sum_{i,j=0}^{4} \beta x_i y_j + \sum_{i,j=0}^{4} \delta y_i y_j + \sum_{i=0}^{4} \lambda x_i + \sum_{i=0}^{4} \omega y_i + \eta = 0 \qquad (1)$$

Затем выполним выбор уравнений, верных для исследуемого S-блока, для этого составлена таблица истинности, представленная на рис. 2.

Для данного S-блока верными оказались 2097151 уравнений. Из них можно выбрать ≈37-2^4=21 линейно независимых уравнений. Предположим, что получено минимально возможное число линейно независимых уравнений

– 21. Для решения системы обратимся к алгоритму метода eXtended Lineranization. Вычислим параметр d. Так как отношение $\frac{2s}{\sqrt{r}} < 2$, то принимаем d=3. Тогда уравнения системы умножаются на одночлены в первой степени: $\{x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4\}$. Следовательно, получим 21·8=168 дополнительных уравнений. Результирующая система будет содержать 189 уравнений, 75 одночленов, которые после приведения к линейному виду рассматриваются как новые переменные.

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	n
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	1
0	0	0	1	1	0	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	1	0	1	0	1
0	0	1	0	1	0	0	1	0	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	1
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	1	1
0	1	0	0	1	1	0	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	1
0	1	0	1	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	1
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
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
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
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	1	0	1	1	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	0	1	0	0	0	0	0	0	1	0	0	0	0	1
1	0	1	1	1	1	0	0	0	1	1	0	0	1	1	0	0	0	0	1	1	0	0	0	0	0	0	1	1	0	0	1	1	0	0	1
1	1	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	1	1	1	0	1	1	1	0	0	0	0	0	0	0	0	1
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	1	1	0	0	1	0	1	1	1	0	1	0	0	0	0	0	0	1	0	0	1	0	1	0	1	0	1	0	1	0	1	0	0	0	0	1
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	1

Рисунок 2 – Таблица истинности для исследуемого блока замены

Таким образом, для одного раунда должна быть получена система из 8·189=1512 уравнений, связывающая вход и выход блока замены. Число переменных составит 64, число одночленов в данной системе равно 75·8=600. Даже если часть уравнений, полученная после умножения, окажется линейно зависимой, оставшихся уравнений будет достаточно для решения методом линеаризации. Полученную систему линейных алгебраических уравнений (СЛАУ) можно решать методами, описанными в работах [10,11].

После составления системы нужно перейти от рассмотрения входов и выходов блока замены к раундовым ключам. Для этого представим i-тый бит входного значения блока замены в виде суммы по модулю 2 бита правой части открытого текста и раудового ключа.

Исходя из структуры одного раунда ГОСТ⊕, выразим выход блока замены через известные данные по формуле (2).

$$y_i = c_{L_i >> 11} \oplus t_{L_i >> 11} \qquad (2)$$

Таким образом, при работе системой для одного раунда число переменных в нелинейной системе можно сократить в два раза, так как выходы блока замены будут однозначно определены.

При исследовании полнораундного алгоритма ГОСТ⊕ система уравнений второго порядка до применения метода XL будет содержать 21·8·32=5376 квадратных уравнения, 32·64=2048 переменных и 37·8·32=9472 одночленов. В результате умножения системы на одночлены в первой степени получим систему с 48384 кубическими уравнениями и 19200 одночленами. В первом раунде замена входных битов блоков замены будет аналогична атаке на одноraундовую версию, а выход блока замены останется без изменения неизвестным $y_{1,i}$. Во втором раунде, используя свойство сети Фейстеля, входные биты S-блока будут представлены формулой (3).

$$x_{2.i} = k_{2.i} \oplus t_{L_i} \oplus y_{1.i<<11} \tag{3}$$

Выход блока также задается неизвестным $y_{2,i}$. В последующих раундах связь входных битов блока замены и открытого текста задана формулой (4).

$$\begin{cases} x_{n,i} = k_{n,i} \oplus t_{Ri} \oplus \sum_{j=2}^{n-1} y_{j,i<<11}, & \text{если n нечетное} \\ x_{n,i} = k_{n,i} \oplus t_{Li} \oplus \sum_{j=1}^{n-1} y_{j,i<<11}, & \text{если n четное} \end{cases} \tag{4}$$

Для последнего раунда ГОСТ⊕ можно выполнить замену по формулам (5) и (6).

$$x_{32.i} = c_{R_i} \oplus k_{32.i} \tag{5}$$

$$y_{32.i} = c_{R_i>>11} \oplus t_{R_i>>11} \oplus \sum_{j=1}^{31} y_{j,i>>11} \tag{6}$$

Работа выполнена при поддержке грантов РФФИ №12-07-31032-мол_а, №12-07-33007-мол_а_вед.

Список литературы:

1. *ГОСТ 28147-89.* Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования // М.: Изд-во стандартов, 1989. – 28 с.

2. *Панасенко С.П.,* Стандарт шифрования ГОСТ 28147-89. Обзор криптоаналитических исследований. // http://www.cio-world.ru/.

3. *Courtois N.,* Security Evaluation of GOST 28147-89 In View Of International Standardisation // http://eprint.iacr.org/2011/211.

4. *Kleiman E.,* The XL and XSL attacks on Baby Rijndael. // http://orion.math.iastate.edu/dept/thesisarchive/MS/EKleimanMSSS05.pdf

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

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

7. *Saarinen M.-J.,* A chosen key attack against the secret S-boxes of GOST. // http://citeseer.ist.psu.edu – August 12, 1998.

8. *Бабенко Л.К., Маро Е.А.,* Вычисление блоков замены алгоритма шифрования ГОСТ 28147-89 // Труды конгресса по интеллектуальным системам и информационным технологиям «IS&IT'11». Научное издание в 4-х томах. – М.: Физматлит, 2011. –Т. 3. -с. 393-395.

9. *Babenko L.K., Ishchukova E.A., Maro E.A.,* Research about Strength of GOST 28147-89 Encryption Algorithm // Proceedings of the 5th international conference on Security of information and networks (SIN 2012), ACM, New York, NY, USA, pp. 80-84.

10. *Бегляров В.В., Берёза А.Н.* Гибридный эволюционный алгоритм решения систем линейных алгебраических уравнений, описывающих электрические цепи [Электронный ресурс] / В.В. Бегляров, А.Н. Берёза // «Инженерный вестник Дона», 2013-№ 1.– Режим доступа: http://ivdon.ru/magazine/archive/n1y2013/1540 (доступ свободный) – Загл. с экрана. – Яз. рус.

11. *Целигоров Н.А., Целигорова Е.Н., Мафура Г.В.* Математические модели неопределённостей систем управления и методы, используемые для их исследования [Электронный ресурс] / Н.А. Целигоров, Е.Н. Целигорова,

Г.В. Мафура // «Инженерный вестник Дона», 2012 - № 4, часть 2.– Режим доступа: http://ivdon.ru/magazine/archive/n4p2y2012/1340 (доступ свободный) – Загл. с экрана. – Яз. рус.