УДК 681.03.245

Л.К. Бабенко, Е.А. Маро

АЛГОРИТМЫ ОЦЕНКИ СТОЙКОСТИ МЕТОДАМИ АЛГЕБРАИЧЕСКОГО АНАЛИЗА

Проведено исследование методов алгебраического криптоанализа, выделены основные этапы проведения оценки стойкости блочных алгоритмов шифрования. Получены системы уравнений для различных размеров таблиц нелинейных преобразований замены упрощенного алгоритма шифрования ГОСТ28147-89, а также выполнено решение одной из систем методом XL. 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 восьми блоков замены. Представлен алгоритм подготовительного этапа анализа, направленный на вычисление блоков замены алгоритма шифрования ГОСТ 28147-89. Для алгоритма ГОСТ 28147-89 вычисление блоков замены потребует выполнения не более 2^{32} операций зашифрования для однозначного определения таблиц замены. Рассматривается возможность повышения эффективности существующих методов криптоанализа применительно к российскому стандарту симметричного шифрования ГОСТ 28147-89. В результате для фиксированных ключей шифрования найдены открытые тексты, позволяющие сократить реально осуществляемое шифрование до 16 раундов вместо 32.

Алгебраический криптоанализ; XL метод; нелинейные преобразования замены; линеаризация нелинейных систем; метод исключения Гаусса; криптографический ключ; алгоритм шифрования ГОСТ28147-89.

L.K. Babenko, E.A. Maro

ALGORITHMS OF RESISTANCE EVALUATION CIPHERS BY ALGEBRAIC CRYPTANALYSIS METHOD

The research of algebraic cryptanalysis method was carried out in this work, we specified basic stages of resistance analysis for block encryption algorithms. Systems of the equations for tables of various sizes of nonlinear transformations of substitution for simplified model of GOST 28147-89 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 eight blocks of substitution. We presented algorithm for finding substitution blocks of GOST 28147-89. It has required at most 2^{32} operations encoding for encryption algorithm GOST 28147-89. The authors consider the possibility of increasing the effectiveness of existing methods of cryptanalysis applied to the Russian standard GOST 28147-89. We found plain texts for fixed keys, which reduce the actual encryption of up to 16 rounds instead of 32.

Algebraic cryptanalysis; XL method; nonlinear transformations of substitution; linearization nonlinear systems; Gauss elimination method; a cryptographic key; GOST28147-89 encryption algorithm.

Задача анализа надежности используемых криптографических алгоритмов является одной 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 (T) и шифротекста (C) равна 64 бита (8 байт), сек-

ретный 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 2^{32};
- 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.

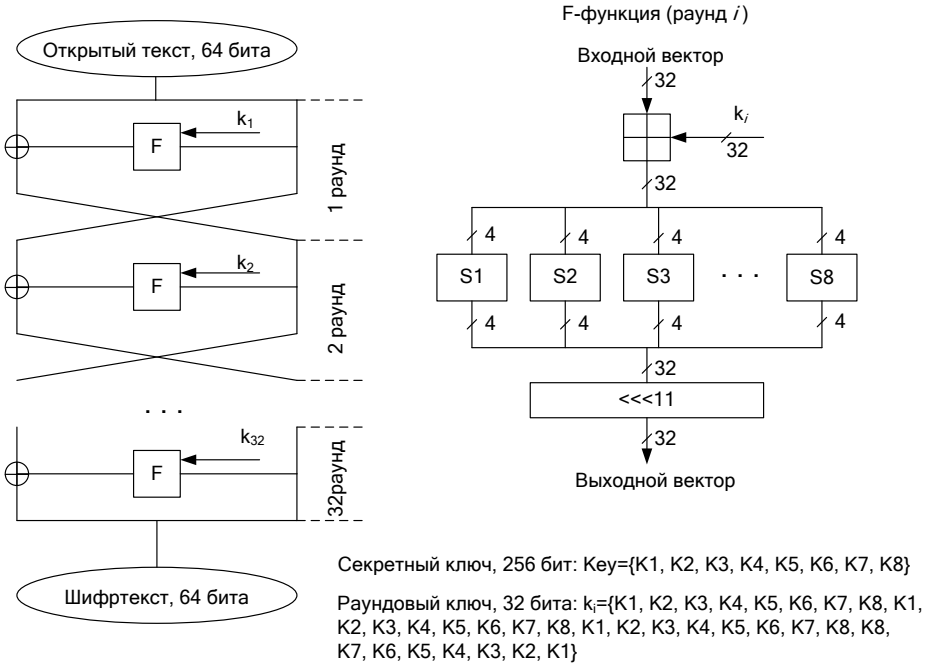

Рис. 1. Алгоритм шифрования ГОСТ 28147-89

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.

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 $\oplus$. Необходимо составить систему уравнений для 8-ми параллельно используемых S-блоков. Выполним составление уравнений для одного блока, заданного табл. 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

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

Число таких уравнений равно 2^{37}=137438953472, число одночленов в них – 37, число переменных – 8.

Затем выполним выбор уравнений, верных для исследуемого S-блока, для этого была составлена таблица истинности.

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.

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.

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

Исходя из структуры одного раунда ГОСТ $\oplus$, выразим выход блока замены через известные данные по формуле

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

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$\oplus$ 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 однораундовую 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

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

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

$$\begin{cases} x_{n,i} = k_{n,i} \oplus t_{Ri} \oplus \sum_{j=2}^{n-1} y_{j,i<<11}, & \textit{если n нечетное}; \\ x_{n,i} = k_{n,i} \oplus t_{Li} \oplus \sum_{j=1}^{n-1} y_{j,i<<11}, & \textit{если n четное}. \end{cases} \quad (4)$$

Для последнего раунда ГОСТ$\oplus$ можно выполнить замену по формулам

$$x_{32.i} = c_{R_i} \oplus k_{32.i}; \quad (5)$$

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

Предложен алгоритм повышения эффективности анализа алгоритма ГОСТ 28147-89. Поскольку сложность анализа во многом зависит от числа анализируемых раундов, то используется метод сокращения числа раундов. Рассмотрим раунды шифрования ГОСТ 28147-89 в режиме простой замены с 17 по 32. Как отмечено ранее, в последних восьми раундах ключи подаются в обратном порядке. Если на входе 25 раунда левая и правая части входного значения будут равны, то в последних восьми раундах будет выполнено расшифрование предыдущих восьми раундов. Следовательно, если найти такой открытый текст, который в 24 раунде на выходе дает совпадающие правые и левые части, то, учитывая порядок следования ключей, полученный шифртекст будет равен входному значению 17 раунда. Таким образом, атака с выбранным открытым текстом методом дифференциального или алгебраического анализа будет выполняться всего над 16 раундами вместо 32.

Авторами предложен следующий алгоритм поиска открытых текстов, с заданным свойством реального шифрования только в 16 раундах:

1. Задание начального значения проверяемого входного 64-битного вектора 17 раунда шифрования (Тр).
2. Выполняется шифрованиеТр в 8 раундах при прямом следовании ключей.
3. Сравнение полученных левых и правых частей после 8 раундов шифрования.
4. Если левые и правые части совпадают, то вычисление искомого открытого текста (Т) путем обмена местами правой и левой частей Тр и шифрования полученного значения в 16 раундах при обратном следовании ключей.
5. Сохранение найденного Т.

6. Если $Tp<2^{64}-1$, то увеличение значения Tp на 1 и переход на пункт 1, иначе конец.

Проанализированы порядка 2^{38} открытых текстов для нулевого ключа и найдены 69 открытых текста, удовлетворяющих условиям поиска. Также для фиксированного ненулевого ключа выполнена проверка порядка 2^{63} текстов на отрезках $[1; 2^{33}]$ и $[2^{60};2^{64}-1]$, в результате которой найдено 24 текста, сокращающих число раундов шифрования. Для фиксированного шифртекста при проверке порядка 2^{38} ключей шифрования было найдено 63 ключа, позволяющих упростить преобразование шифрования.

Выводы. Предложен алгоритм генерации системы уравнений, описывающей преобразования нелинейных блоков замены шифра ГОСТ 28147-89. Подробно рассмотрена атака на блочные шифры методом алгебраического анализа – eXtended Linearization, направленная на получение ключа шифрования. Проведена экспериментальная проверка предлагаемой атаки на два раунда шифрования ГОСТ 28147-89. Отмечена возможность повышения эффективности атаки путем применения методов распараллеливания задачи составления и решения системы линейных алгебраических уравнений. Предложен метод для сокращения анализируемых во время атаки раундов шифра ГОСТ, который позволяет значительно повысить эффективность алгебраического анализа при атаке на выбранном открытом тексте.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

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. – P. 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. Т. 3. – М.: Физматлит, 2011.– 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. – P. 80-84.

Статью рекомендовал к опубликованию д.т.н., профессор Я.Е. Ромм.

Бабенко Людмила Климентьевна – Южный федеральный университет; e-mail: blk@fib.tsure.ru; 347928, г. Таганрог, ул. Чехова, 2, корпус "И"; тел.: 88634312018; кафедра безопасности информационных технологий; профессор.

Маро Екатерина Александровна – e-mail: marokat@gmail.com; тел.: 88634371905; кафедра безопасности информационных технологий; ассистент.

Babenko Lyudmila Klimentevna – Southern Federal University; e-mail: blk@fib.tsure.ru; Block "I", 2, Chehov street, Taganrog, 347928, Russia; phone: +78634312018; the department of security of information technologies; professor.

Maro Ekaterina Aleksandrovna – e-mail: marokat@gmail.com; phone: +78634371905; the department of security of information technologies; assistant.