

КРИТЕРИИ ОТБОРА ТАБЛИЦ ПОДСТАНОВОК АЛГОРИТМА ШИФРОВАНИЯ DES, УСТОЙЧИВЫХ К АТАКАМ ЛИНЕЙНОГО КРИПТОАНАЛИЗА

И.В. Лисицкая, С.А. Головашич

Харьковский государственный технический университет
радиоэлектроники

The general methodology of fulfilment of a linear cryptanalysis is stated. On an example of the code DES the properties are studied and the approaches to an evaluation of resistance of a procedure of encoding to known attacks of a linear cryptanalysis are determined. The criteria of a selection of the casual tables of substitutions ensuring stability of the algorithm DES to cryptattacks of this type are determined. The technique of construction *S*-boxes for algorithm DES invulnerable to attack of linear cryptanalysis is resulted.

Линейный криптоанализ – сравнительно новый тип криптонападения, предложенный Мацуи [1] в 1993 г. Этот метод использует линейную аппроксимацию для описания процедуры нападения на DES – подобные шифры. Она заключается в нахождении линейных соотношений, т.е. ситуаций, когда сумма по модулю 2 некоторых битов открытого текста и некоторых битов соответствующего ему зашифрованного текста равна сумме по модулю 2 некоторых битов ключа. Если такое соотношение выполняется с некоторой вероятностью $p \neq 1/2$, то имеется возможность использовать собранные открытые и соответствующие им зашифрованные тексты для определения битов ключа.

Как и при дифференциальном криптоанализе, сложность линейного криптоанализа определяется свойствами *S* блоков. Для описания этих свойств применяются так называемые линейные аппроксимационные таблицы.

Для оценки сложности осуществления рассматриваемой криптоаналитической атаки вычисляются вероятности аппроксимационных характеристик, под которыми понимаются системы взаимосвязанных линейных соотношений, распространенных на несколько циклов процедуры шифрования, и оцениваются вероятности одновременного выполнения всех линейных соотношений, попавших в цепочку.

Базовая атака, разработанная Мацуи и развитая Бихамом, обнаруживает только один бит ключа, используя для этого одноблочные характеристики [2]. Эта атака строится двукратным повторением восьмициклового минимальной итеративной характеристики, в которой на первой и второй четвёрке циклов используются идентичные характеристики, кроме того в каждой из четвёрок последний цикл является тождественным, т.е. вероятность

его выполнения равна 1. Таким образом, вероятность полной аппроксимационной характеристики определяется вероятностями p_a, p_b, p_c выполнения соотношений на первых трёх циклах. Особенностью минимальной характеристики является, то что любая другая одноблочная характеристика имеет большую результирующую вероятность.

В докладе изучаются условия отбора S блоков, обеспечивающих сложность базовой атаки, превышающую сложность «полного перебора».

Для этого вводится математическое описание многоциклового итеративной характеристики:

F – цикловая функция DES;

$\Omega_P, \Omega_T, \Omega_K$ – «маски», определяющие, соответственно, подмножества бит данных до и после цикла шифрования, а также подмножество бит ключа, участвующих в аппроксимации;

$a \zeta A \zeta b \zeta B \zeta c \zeta C \zeta$ – входные и выходные «маски» цикловой функции на первых трёх циклах, т.е. $A' = F(a')$, $C' = F(c')$, $B' = F(b')$.

Для минимальной характеристики справедливо

$$a' = c' = B' \text{ и } b' = A' \oplus C'. \quad (1)$$

Объединение l характеристик с вероятностью p_i каждая (когда это может быть выполнено), приводит к вероятности результирующей характеристики [2] равной

$$1/2 + p = 1/2 + 2^{l-1} \prod_{i=1}^l p_i. \quad (2)$$

Для вероятности указанной 8-циклового и полученной из неё полной 16-циклового характеристики получены выражения

$$P_8 = 2 \cdot (4 \cdot p_a p_b p_c)^2 = 2^5 \cdot (p_a p_b p_c)^2.$$

$$P_{16} = 2 \cdot P_8^2 = 2^{11} \cdot (p_a p_b p_c)^4.$$

В результате сделан вывод, что для защиты от атаки, использующей минимальную характеристику, достаточно выбрать таблицы S блоков, исходя из условия, что максимально возможное значение произведения вероятностей $p_a \times p_b \times p_c$ удовлетворяет требованию

$$(P_{16})^2 \leq 2^{-55} \rightarrow p_a p_b p_c \leq \sqrt[8]{2^{-77}} = 2^{-10}. \quad (3)$$

Это позволило сформулировать критерий отбора S блоков, устойчивых к атакам линейного криптоанализа в виде следующего требования.

Требование. Для обеспечения устойчивости шифра DES к известным атакам линейного криптоанализа необходимо и достаточно, чтобы максимальное значение произведения вероятностей $p_a p_b p_c$ одноциклового характеристик, соответствующих $(\Omega_P^A, \Omega_T^A, \Omega_K^A, 1/2 + p_a)$,

$(\Omega_P^B, \Omega_T^B, \Omega_K^B, 1/2 + p_b)$ и $(\Omega_P^C, \Omega_T^C, \Omega_K^C, 1/2 + p_c)$, где $\Omega_P^A = (A', 0) \rightarrow \Omega_T^A = (A', a')$, $\Omega_P^B = (a', A') \rightarrow \Omega_T^B = (a', A' \oplus b')$, $\Omega_P^C = (A' \oplus b', a') \rightarrow \Omega_T^C = (A' \oplus b', 0)$, было меньше порогового значения 2^{-10} .

Фактически это трехцикловая характеристика вида $(\Omega_P^1, \Omega_T^3, \Omega_K^A \oplus \Omega_K^B \oplus \Omega_K^C, 1/2 + 4p_a p_b p_c)$, для которой выполняется условие: для $\Omega_P^1 = \Omega_P^A = (A', 0)$ имеем $\Omega_T^3 = \Omega_T^C = (A' \oplus b', 0)$.

В соответствии с приведенным требованием предложена методика отбора S блоков устойчивых к атаке рассматриваемого вида.

Базовая атака использует однобитные характеристики. Это значит, что вход b' является однобитным, так как в соответствии с (3) $b' = F(a') \oplus F(c')$ – сумма по модулю два выходных битов одного и того же S блока ($a' = c'$). А в соответствии с правилом перестановки бит P [3], завершающей цикловую функцию, выходы идентичных S блоков могут сформировать вход в один S блок только в случае, когда сумма $F(a') \oplus F(c')$ является одним битом. Очевидно также, что должны быть однобитными и входы a' и соответственно $c' = a'$. В результате анализу подлежат все однобитные входные «маски» линейных аппроксимационных таблиц S блоков: $1_x, 2_x, 4_x, 8_x, 10_x$ и 20_x . Из этого множества сразу можно отбросить «маски» 1_x и 20_x , для которых значения во всех столбцах всегда равны 0, т.к. биты соответствующие этим двум «маскам» осуществляют выбор одной из четырёх перестановок, которые составляют S блок. При осуществлении проверки следует учитывать только те пары ячеек таблицы, для которых при одинаковой входной «маске» сумма по модулю два выходных «масок» даёт один бит. Для отобранных пар определяются соответствующие им значения p_a и p_c , по ним вычисляется значение $b' = F(a') \oplus F(c')$, затем по аппроксимационным таблицам находится значение p_b , при котором $F(b') = a'$. Найденные значения p_a, p_b и p_c проверяются на соответствие установленному критерию.

На основе изложенной методикой разработан программный комплекс генерации S блоков для алгоритма DES. С его помощью построены таблицы подстановок, устойчивых к рассматриваемой атаке.

Литература: 1. Mitsuru Matsui, *Linear Cryptanalysis Method for DES Cipher*, Abstracts of EUROCRYPT'93, pp. W112–W123, May 1993. 2. Eli Biham, *On Matsui's Linear Cryptanalysis*. Technion – Comput Science Department -Technic Report CS0813 - 1994. P 1-17. 3. National Bureau of Standards, *Data Encryption Standard*, U.S. Department of Commerce, FIPS pub. 46, January 1977.