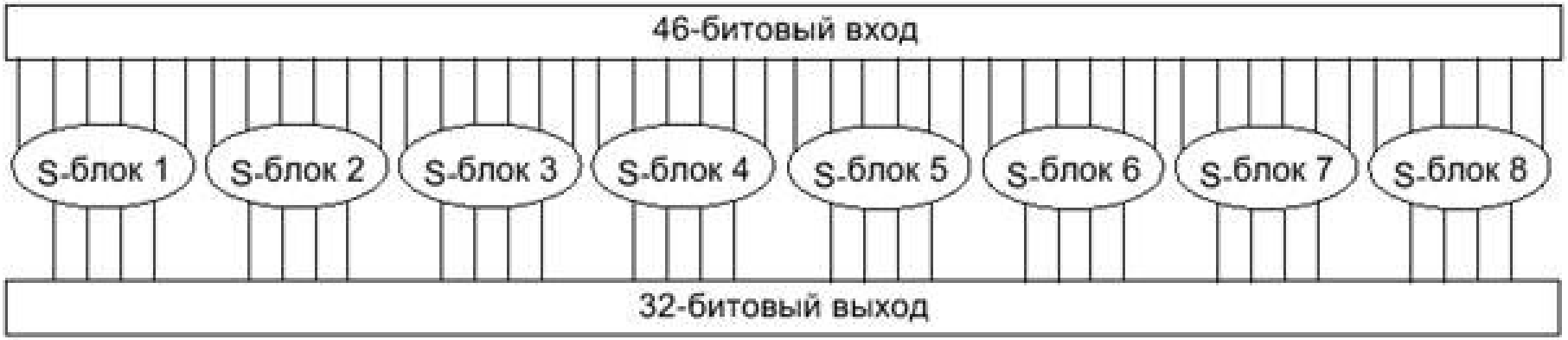
Аналитическое исследование стойкости алгоритма DES, представленного в виде битовой функции

Аспирант кафедры защиты инфромации
Южно-уральского государственного университета
Архипов Антон Дмитриевич

s-блоки



S[0]

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2.	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

$S[0]: (x_0, \underbrace{x_1, x_2, x_3, x_4}_{\text{column}}, x_5) \rightarrow (y_0, y_1, y_2, y_3)$

(1, 1, 0, 0, 1, 1): row 3, column 9, $S[0](1, 1, 0, 0, 1, 1) = 11 = (1, 0, 1, 1)$

Представление после первого раунда

C032 = D007*K009

C032 = !D007*!K009

C033 = D057*K050

C033 = !D057*!K050

C034 = D049*K033

C034 = !D049*!K033

C035 = D041*K059

C035 = !D041*!K059

Представление битов зашифрованного сообщения после 16 раунда

C001 = !D001*!D017*!D033*!D059*D009*D025*!K018*!K032*!K041*!K056*K008 *K013

C001 = !D001*!D017*!D033*!D059*D009*D025*!K018*!K032*!K041*!K056*K008

C001 = !D001*!D017*!D033*!D059*D009*D025*!K032*!K041*!K056*K008

C001 = !D001*!D017*!D033*D009*D025*!K032*!K041*!K056*K008

Деградация СЛУ при известных битах сообщений

При D059 = 1

C001 = !D001*!D017*!D033*!D059*D009*D025*!K018*!K032*!K041*!K056*K008 *K013 = 0

C001 = !D001*!D017*!D033*!D059*D009*D025*!K018*!K032*!K041*!K056*K008 = 0

C001 = !D001*!D017*!D033*!D059*D009*D025*!K032*!K041*!K056*K008 = 0

C001 = !D001*!D017*!D033*D009*D025*!K032*!K041*!K056*K008

Получение битов ключа

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n = b_n \end{cases}$$

Здесь aij — группа битов данных, xij — группа битов ключа, bi — бит зашифрованного сообщения

Теоретическая стойкость шифрования

Декларированная в стандарте стойкость

$$p(x)=2^{48}$$

Формула расчета неопределенности

$$p(x)=N_1*2^1+N_2*2^2+N_3*2^3+N_4*2^4+N_5*2^5+N_1*6^6$$

Полученная неопределенность

$$p(x)>200^6$$

Выводы

Полученные результаты обусловлены специфическим выбором S-блоков в преобразовании Фейстеля.

Уменьшенное количество битов ключа, содержащееся в битах шифрованного сообщения, ведет к снижению теоретической стойкости алгоритма.

Полученный подход позволяет быстро строить компактные радужные таблицы для сообщений с известными шифруемыми данными для решения задачи поиска ключа расшифрования.