Ежегодная международная научно-практическая конференция
«РусКрипто’2019»

Исследование алгоритмов развертывания ключа блочных шифрсистем, предназначенных для использования в средах с ограниченными ресурсами, с помощью методологии SAT

Ирина Слонкина,
НИЯУ МИФИ

Введение

SAT — задача выполнимости булевых функций

В ДНФ

- тривиально решается за линейное время

В КНФ

- в общем случае является NP-полной задачей

Каждая задача из класса NP в явном виде сводится к SAT

Этапы логического криптоанализа

Сведение алгоритма к SAT-задаче

- Трансляция алгоритмов шифрования в логические выражения
- Представление данных выражений в КНФ

Решение полученной SAT-задачи

- Подстановка известных значений переменных
- Поиск выполняющего набора с помощью SAT-решателя

Используемые программные средства

Кодировщик Transalg

- Транслирует дискретные функции на языке TA - процедурном языке программирования с С-подобным синтаксисом
- Успешно применялся для кодирования в SAT задач криптоанализа целого ряда криптографических функций

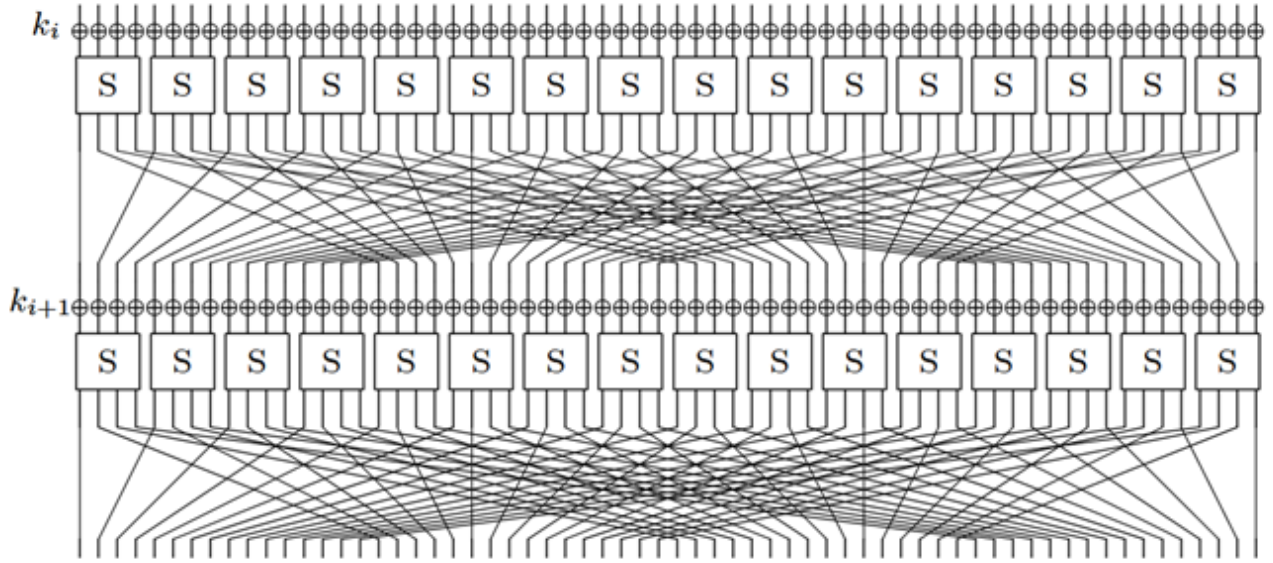
Решатель CryptominiSAT

- Реализует алгоритм CDCL
- Метод Гаусса
- Мелкозернистое распараллеливание
- Призер SAT-competition в нескольких номинациях

Present

SP-сеть, 32 раунда, длина мастер-ключа 80 или 128 бит, длина блока – 64 бита

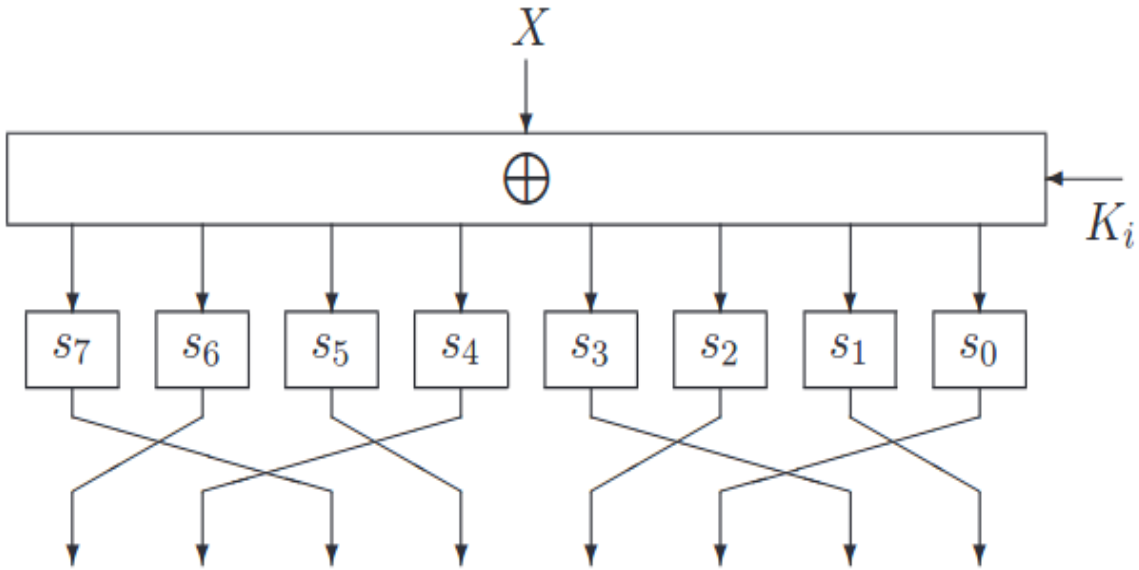
- addRoundKey – побитовое XOR с раундовым ключом;
- sBoxLayer – параллельное применение к результату 16 4-битных S-box;
- pLayer – перемешивание бит.



LBlock

Сеть Фейстеля с 32 раундами, длиной ключа 80 бит и длиной блока 64 бит

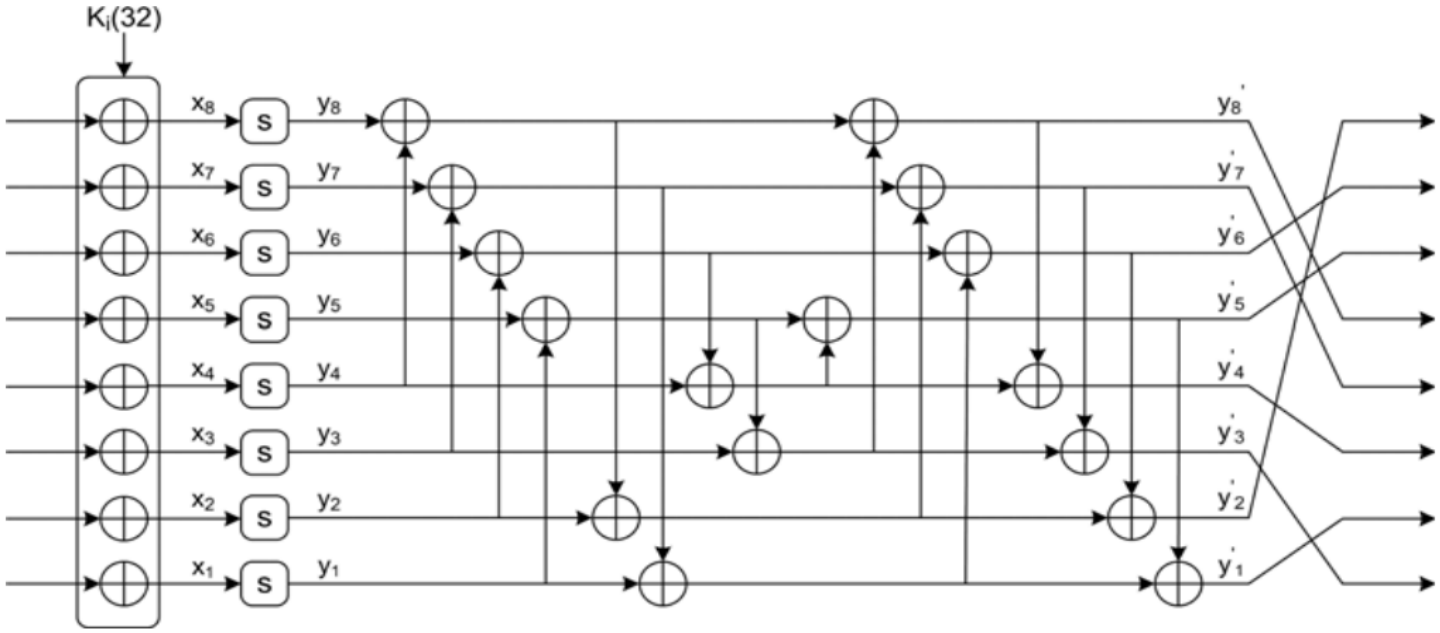
- XOR с ключом
- S — восемь параллельных 4-битных S-box
- P — перестановка полубайтов



MIBS

Сеть Фейстеля с 32-мя раундами, длиной блока 64 бита и длиной ключа 64 и 80 бит

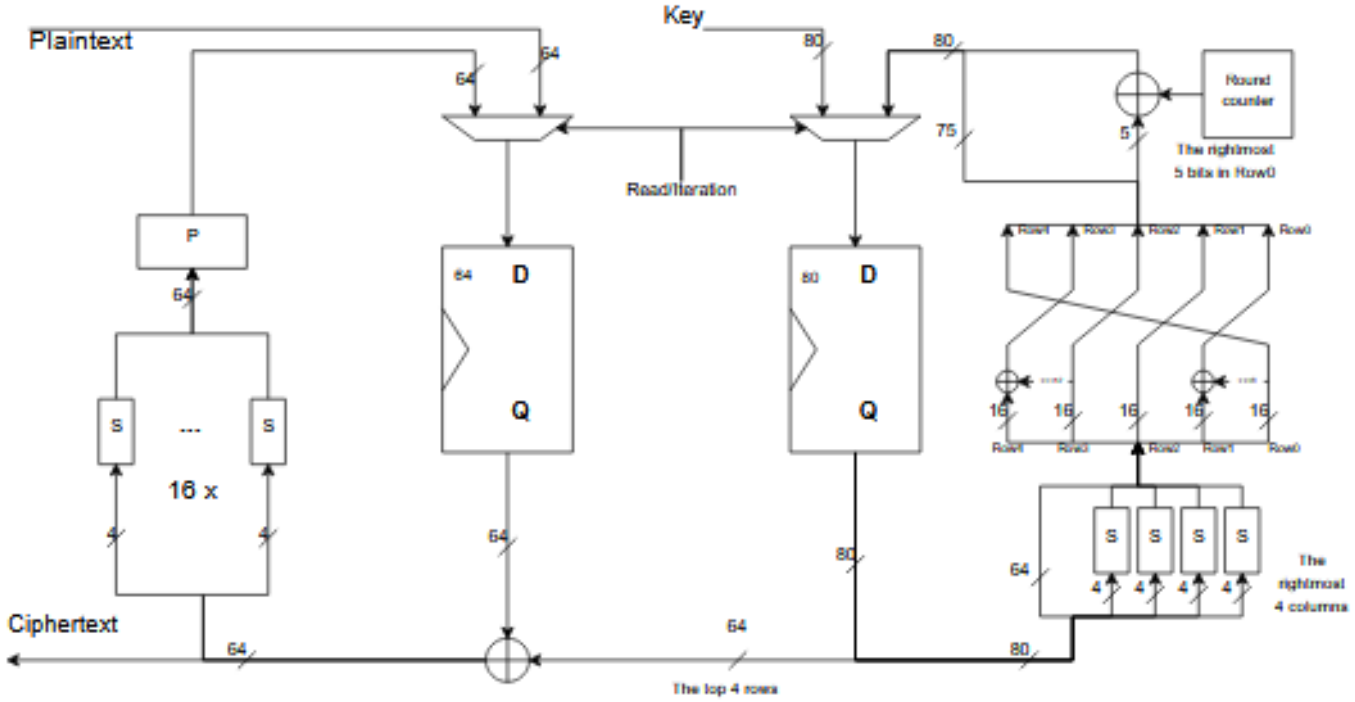
- XOR с ключом
- S — нелинейное преобразование
- M — линейное преобразование



Rectangle

25 раундов, длина ключа 80 и 128 бит. Открытый текст записывается в таблицу (4 строки, 16 столбцов).

- XOR с ключом
- Применение S-box к некоторым столбцам
- Сдвиг строк



Параметры функции развертывания ключа

Параметр	Present		LBlock	MIBS	
Длина мастер-ключа (и регистра K) в битах	80	128	80	64	80
Длина итерационного ключа в битах	64	64	32	32	32
Сдвиг	$K >>> 19$	$K >>> 67$	$K >>> 51$	$K >>> 15$	$K >>> 19$
Количество S-box	1	2	2	1	2
S-box	[C, 5, 6, B, 9, 0, A, D, 3, E, F, 8, 4, 7, 1, 2]		[8, 7, E, 5, F, D, 0, 6, B, C, 9, A, 2, 4, 1, 3] [B, 5, F, 0, 7, 2, 9, D, 4, 8, 1, C, E, A, 3, 6]	[4, F, 3, 8, D, A, C, 0, B, 5, 7, E, 2, 6, 1, 9]	
Сдвиг счетчика итераций	$i <<< 15$	$i <<< 62$	$i <<< 46$	$i <<< 11$	$i <<< 14$

Условия проведения экспериментов

- Ноутбук Lenovo Ideapad 530 S, процессор Intel Core i5-8250U (4 ядра @ 1.6~3.2GHz), 8 ГБ RAM DDR4 (одноканальный режим) и 8 ГБ SWAP
- Ubuntu GNU/Linux (4.15.0-34-generic, amd64)

Генерация КНФ

Кодирование S-box

С помощью условных операторов

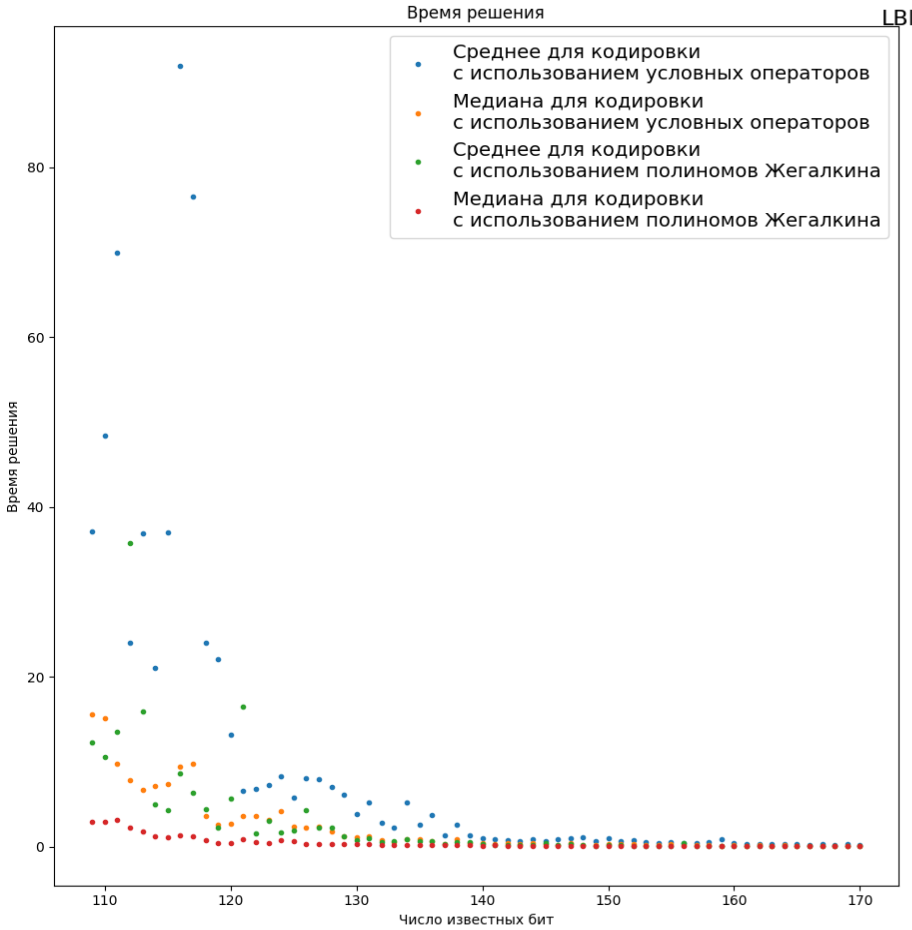
Путем выражения выходных бит S-box через входные

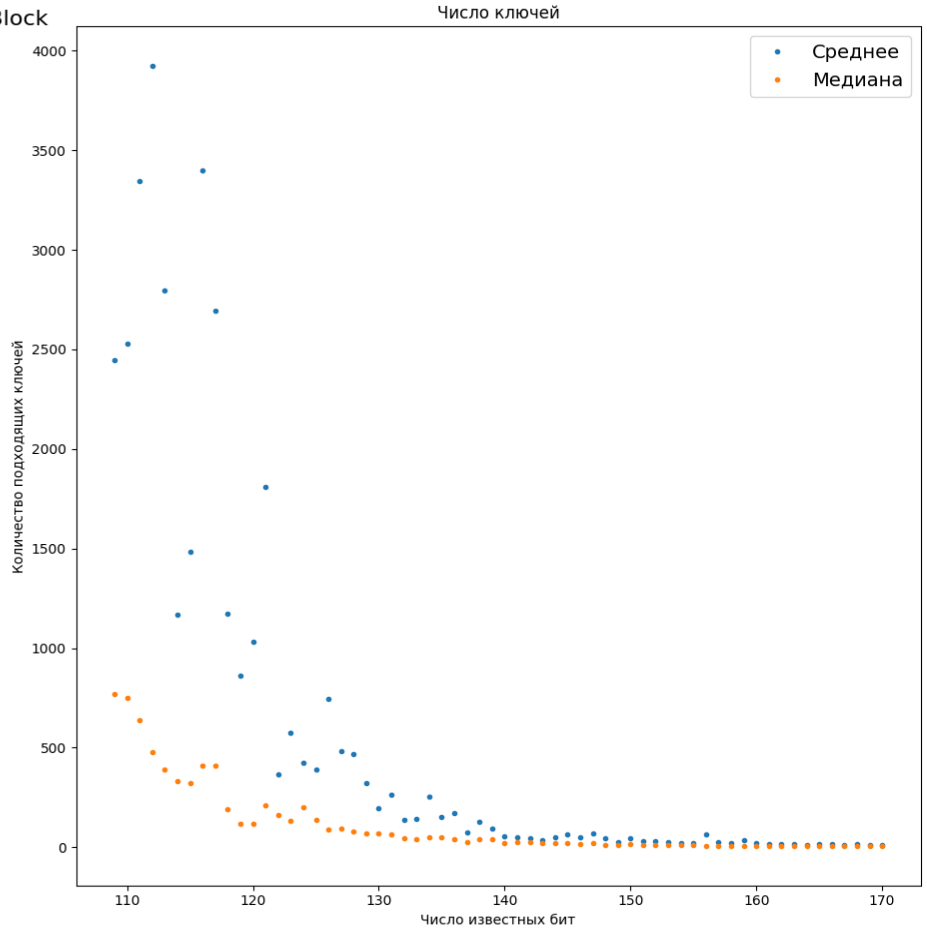
$$y_0 = x_1x_2 \oplus x_0 \oplus x_2 \oplus x_3$$
$$y_1 = x_0x_1x_3 \oplus x_0x_2x_3 \oplus x_0x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1 \oplus x_3$$
$$y_2 = x_0x_1x_3 \oplus x_0x_2x_3 \oplus x_0x_1 \oplus x_0x_3 \oplus x_1x_3 \oplus x_2 \oplus x_3 \oplus 1$$
$$y_3 = x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_2x_3 \oplus x_1x_2 \oplus x_0 \oplus x_1 \oplus x_3 \oplus 1$$

Параметры КНФ

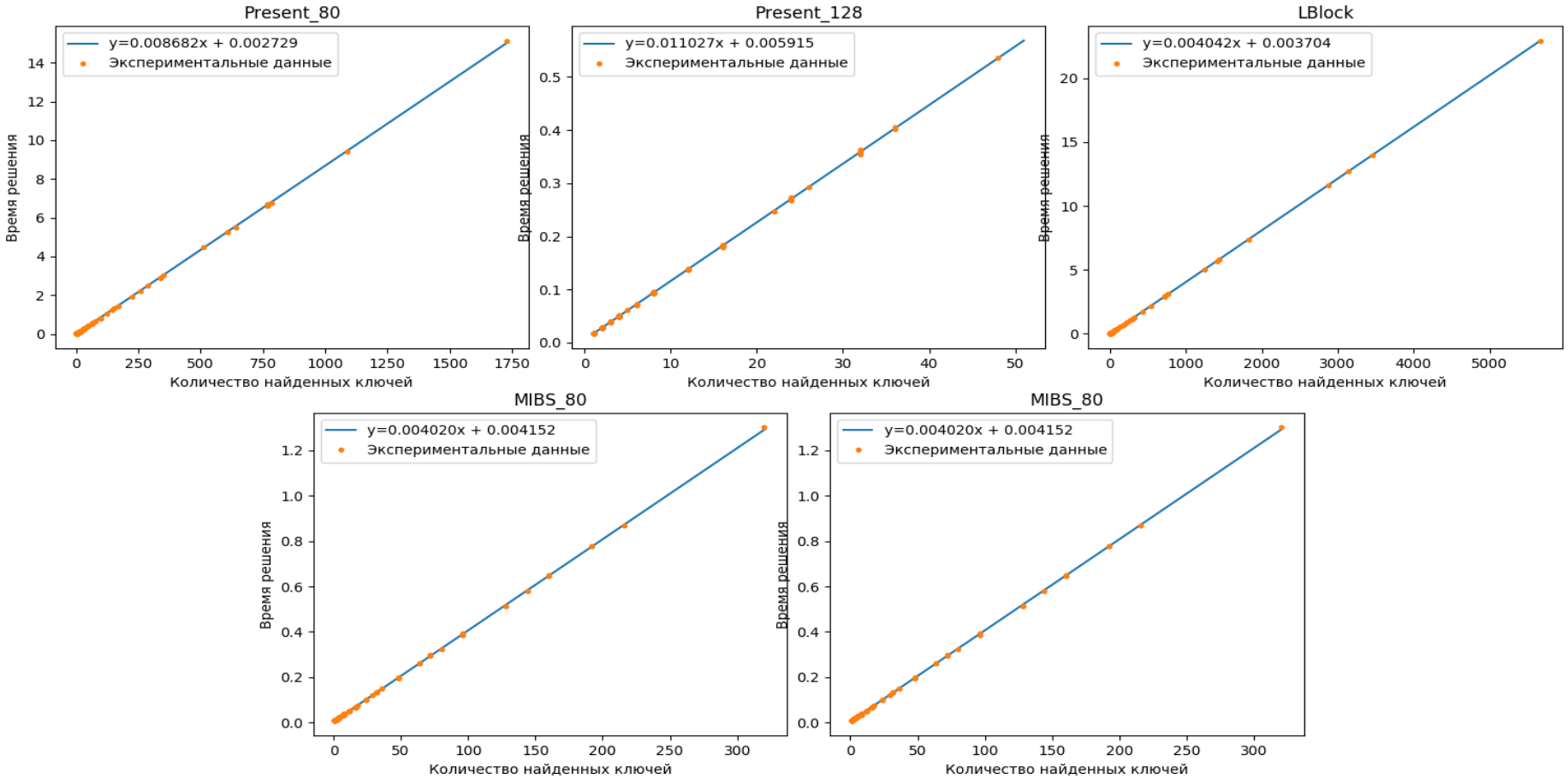
Алгоритм, длина мастер-ключа	Кодирование S-box условными операторами				Кодирование S-box полиномами Жегалкина			
	Переменных	Дизъюнктов	Литералов	Дизъюнкты / переменные	Переменных	Дизъюнктов	Литералов	Дизъюнкты / переменные
Present-80	4656	11475	25273	2.465	2889	7664	19420	2.653
Present-128	7151	18693	42033	2.614	3618	11072	30328	3.060
LBlock-80	6048	16583	37813	2.742	1430	4496	13452	3.144
MIBS-64	3518	9200	20692	2.615	1286	3481	9656	2.707
MIBS-80	5890	16205	36995	2.751	1427	4792	15020	3.358

Восстановление мастер-ключа по фрагментам итерационных ключей

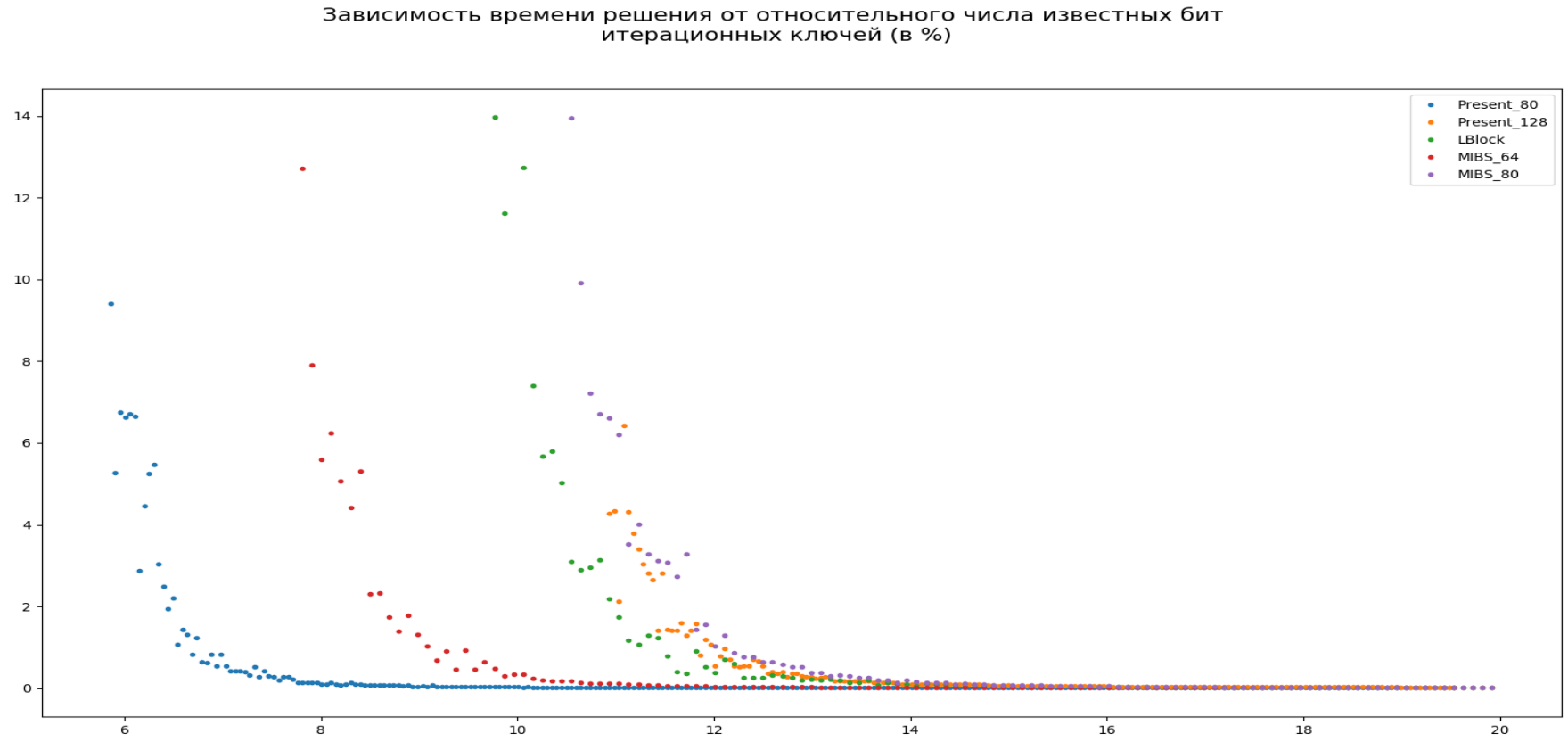




Взаимосвязь между медианой числа подходящих ключей и медианой времени поиска решения для различного числа известных бит



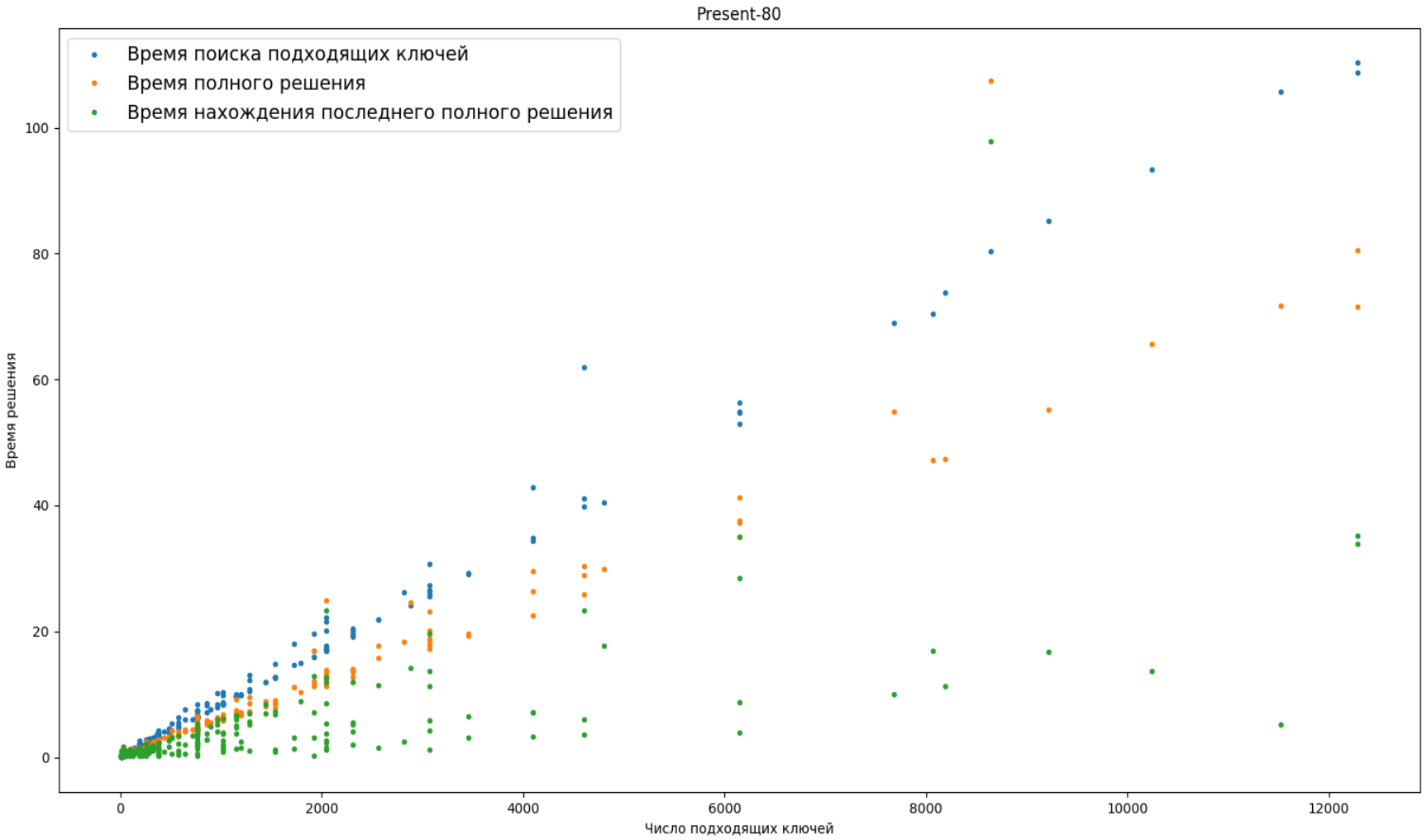
Сравнение медианы времени решения КНФ для разного относительного числа известных бит итерационных ключей



Результаты экспериментов

	Present		MIBS		LBlock	Rectangle	
	80	128	64	80	80	80	128
Количество раундов	32	32	32	32	32	25	25
Длина итерационного ключа	64	64	32	32	32	64	64
Совокупная длина итерационных ключей	2048	2048	1024	1024	1024	1664	1664
Процент бит, необходимых для однозначного восстановления ключа с вероятностью 90%	15.97 (327)	19.53 (400)	24.22 (248)	30.96 (317)	29.59 (303)	7.75 (129)	13.76 (229)
Процент бит, для которых было найдено < 1024 ключа (с вероятностью 90%)	6.79 (139)	11.77 (241)	9.77 (100)	12.79 (131)	11.91 (122)	4.93 (82)	8.95 (149)
Время поиска одного ключа	0.0091	0.0113	0.0041	0.0046	0.0046	0.0188	0.0168
Число известных бит, необходимое для восстановления ключа за 1 с (с вероятностью 90%).	7.86 (161)	13.62 (279)	10.74 (110)	14.36 (147)	13.38 (137)	5.47 (91)	10.22 (170)
Число известных бит, необходимое для восстановления ключа за 10 с (с вероятностью 90%).	6.59 (135)	11.82 (242)	9.18 (94)	12.21 (125)	11.52 (118)	4.93 (82)	9.31 (155)

Зависимость времени решения от количества подходящих ключей



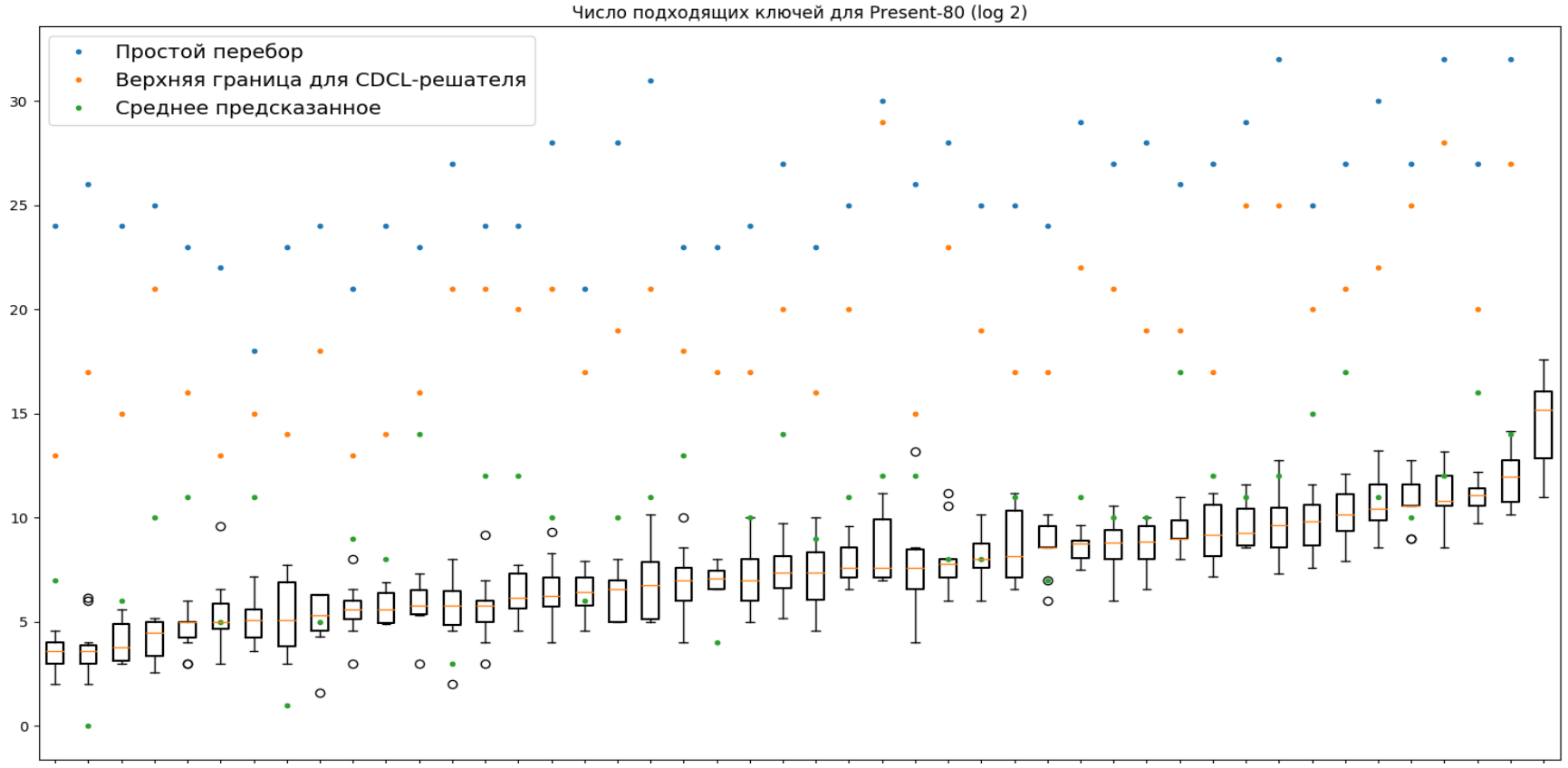
Влияние расположения известных бит на количество подходящих ключей

K_i															
k_{79}	k_{78}	k_{77}	k_{76}	k_{75}	k_{74}	…	k_{35}	k_{34}	…	k_{19}	k_{18}	…	k_{16}	k_{15}	…	k_0
K_i после сдвига																
k_{18}	k_{17}	k_{16}	k_{15}	k_{14}	k_{13}	…	k_{54}	k_{53}	…	k_{38}	k_{37}	…	k_{35}	k_{34}	…	k_{19}
K_{i+1}																
$S_{i,0}$	$S_{i,1}$	$S_{i,2}$	$S_{i,3}$	k_{14}	k_{13}	…	k_{54}	k_{53}	…	k_{38}	k_{37}	…	k_{35}	k_{34}	…	k_{19}

Среднее число подходящих назначений для известных бит на входе и выходе S-box

S-box шифра	Present	MIBS	LBlock S8	LBlock S9
Известные входные и выходные биты S-box	“10--“, “1--d”			
Количество подходящих вариантов для каждого значения d	{1: 1, 2: 1}	{1: 2}	{2: 2}	{0: 1, 2: 1}
Среднее число подходящих назначений	1.5	1.0	2.0	1.0
Известные входные и выходные биты S-box	“01--“, “1--d”			
Количество подходящих вариантов для каждого значения d	{1: 1, 2: 1}	{1: 1, 2: 1}	{0: 1, 2: 1}	{0: 1, 2: 1}
Среднее число подходящих назначений	1.5	1.5	1.0	1.0

Зависимость времени решения от количества подходящих ключей



Применение к ранее описанным атакам

- дифференциальная атака на 16-раундовый шифр Present (16 раундов шифра + 17-й неполный раунд, состоящий из одной операции AddRoundKey. K_{17} (24 бита), K_{16} (16 бит). 28 -> 27.
- атака на LBlock с использованием невозможных дифференциалов. Полубайты $K_{1,\{0,1,3,6\}}$, $K_{2,\{2,7\}}$, $K_{3,5}$, $K_{19\{1,7\}}$, $K_{20,\{0,3,5\}}$, $K_{21\{0,2,3,4,5,6,7\}}$. 37 -> 25
- атака на LBlock методом «встречи посередине». Полубайты $K_{1,\{1,2,7\}}$, $K_{2,\{1,2\}}$, $K_{3,7}$, $K_{16,3}$, $K_{17,3}$, $K_{18,3}$, $K_{19\{3,5,6\}}$. 54 –> 41.
- множественная линейная атака на шифр MIBS. 4 полубайта итерационных ключей: $K_{1,1}$, $K_{1,6}$, $K_{17,1}$, $K_{17,6}$. Для MIBS-64: 51 -> 48, MIBS-80: 68 –> 65.
- Атака на MIBS с использованием связанных ключей. $K_1[12:31]$ и $K_{15}[20:27]$. Для MIBS-64: 39 -> 36, MIBS-80: 56 -> 53.

Вопросы

Контактная информация

Электронная почта:

otrada.nsk@gmail.com

Телефон:

+7 977 872-43-31