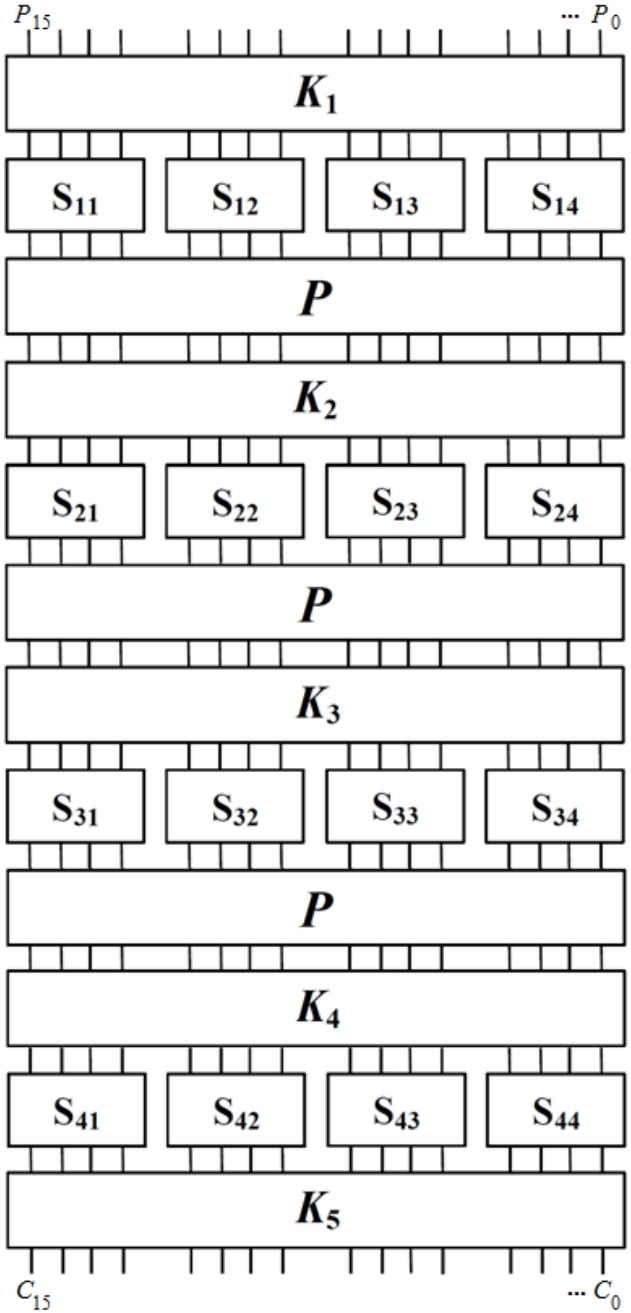
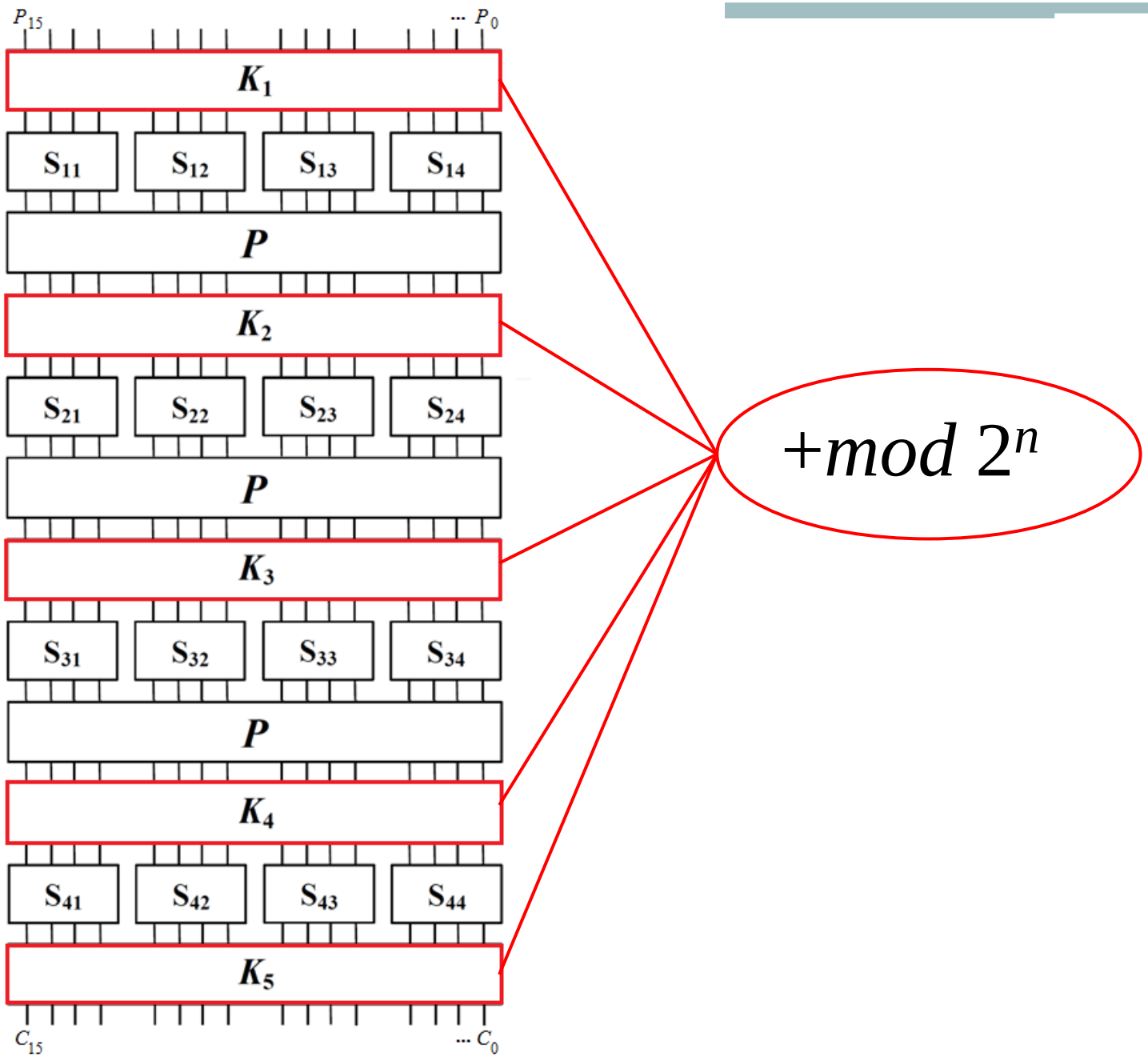
Сложение по модулю 2^n в блочном шифровании

Карондеев А.М.
Козлов А.А.
Силков А.А.

МГТУ им. Н.Э. Баумана


P_{15}
... P_0
K_1
S_{11} S_{12} S_{13} S_{14}
P
K_2
S_{21} S_{22} S_{23} S_{24}
P
K_3
S_{31} S_{32} S_{33} S_{34}
P
K_4
S_{41} S_{42} S_{43} S_{44}
K_5
C_{15}
... C_0


P_{15}
... P_0
K_1
S_{11} S_{12} S_{13} S_{14}
P
K_2
S_{21} S_{22} S_{23} S_{24}
P
K_3
S_{31} S_{32} S_{33} S_{34}
P
K_4
S_{41} S_{42} S_{43} S_{44}
K_5
C_{15}
... C_0
$+mod\ 2^n$

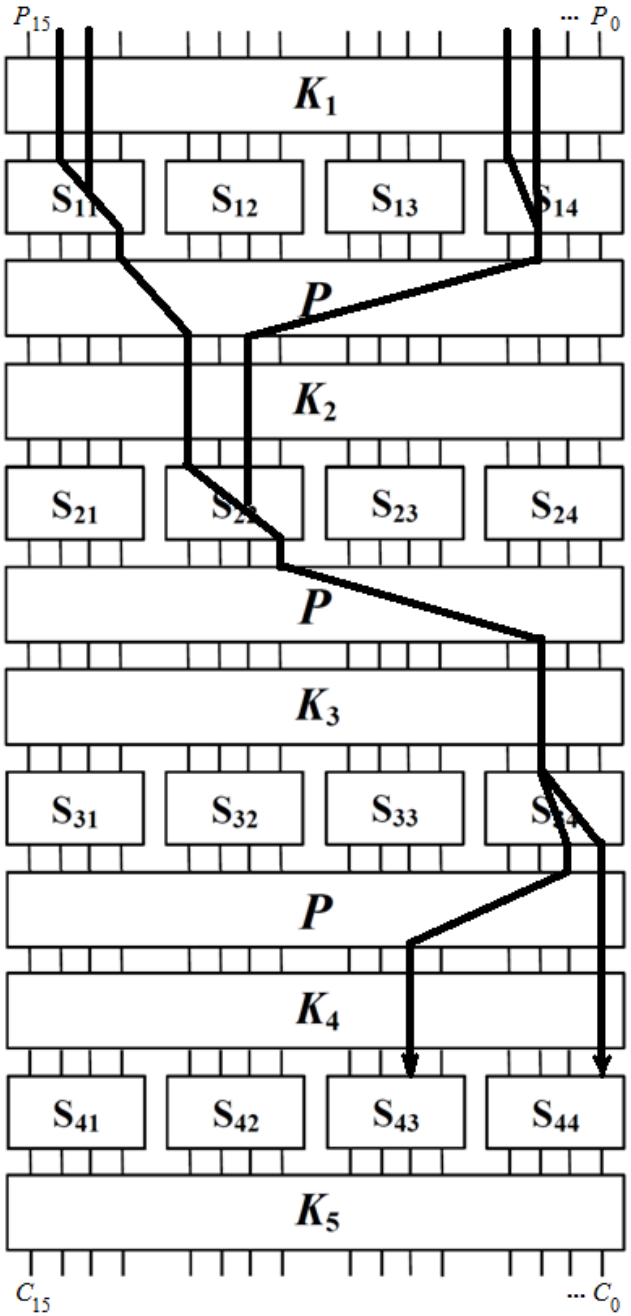
Known Plaint Text Attack

Известно:

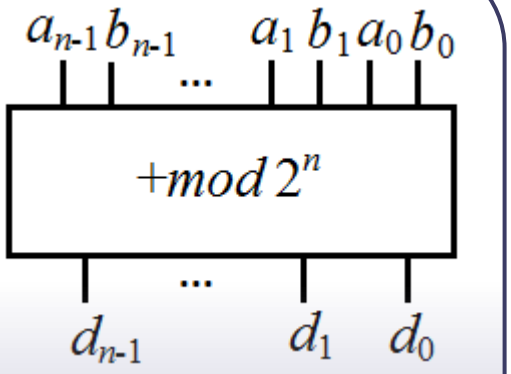
- Алгоритм шифрования
- Пары открытый текст/шифртекст, полученные на фиксированном ключе

Требуется:

- Восстановить ключ


P_{15}
... P_0
K_1
S_{11}
S_{12}
S_{13}
S_{14}
P
K_2
S_{21}
S_{23}
S_{24}
P
K_3
S_{31}
S_{32}
S_{33}
P
K_4
S_{41}
S_{42}
S_{43}
S_{44}
K_5
C_{15}
... C_0

Сложение по модулю 2^n



$$A + B = D \ mod \ 2^n$$

$$Add: \mathbb{Z}_2^{2n} \to \mathbb{Z}_2^n$$

$$d_i = a_i \oplus b_i \oplus p_i$$

$$p_i = a_{i-1}b_{i-1} \oplus a_{i-1}p_{i-1} \oplus b_{i-1}p_{i-1}$$

Свойства переноса

- $p_i(a_{i-1}, b_{i-1}, \dots, a_0, b_0) \notin aff\ , \forall i > 0$
- $\max_{\mathbf{u} \in \mathbb{Z}_2^{2i}} |W_{\hat{p_i}}(\boldsymbol{u})| < 2^{2i}$
- p_i не имеет фиктивных переменных

Линейная аппроксимация переноса

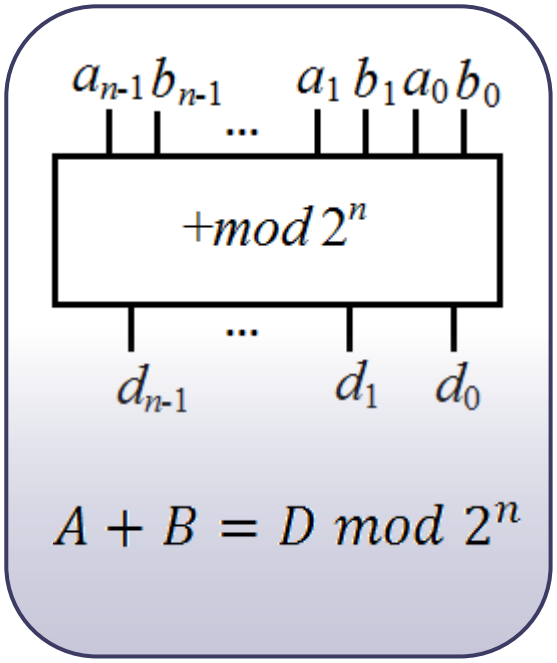
$$\forall i > 0 \quad \max_{\mathbf{u} \in \mathbb{Z}_2^{2i}} Prob\,(p_i = \langle \boldsymbol{u}, \boldsymbol{x} \rangle + c) \leq 0.75$$

причем равенство достигается на двух линейных функциях a_{i-1} и b_{i-1}

$a_{i-1}\ b_{i-1}\ \dots\ a_0\ b_0$	p_i	$\hat{p}_i$	$\dots$			$W_{\hat{p}_i}$
0 0 0 … 0 0	0	1		2^{2i-2}	$2^{2i-2} + W_{\hat{p}_{i-1}}(\mathbf{0})$	
				0		
	…	…		…	$W_{\hat{p}_{i-1}}$	$2W_{\hat{p}_{i-1}}$
0 0 1 … 1 1	0	1		0		
0 1 0 … 0 0					$2^{2i-2} - W_{\hat{p}_{i-1}}(\mathbf{0})$	2^{2i-1}
						0
	p_{i-1}	$\hat{p}_{i-1}$		$W_{\hat{p}_{i-1}}$	$-W_{\hat{p}_{i-1}}$	…
0 1 1 … 1 1						0
1 0 0 … 0 0					$W_{\hat{p}_{i-1}}(\mathbf{0}) - 2^{2i-2}$	2^{2i-1}
						0
	p_{i-1}	$\hat{p}_{i-1}$		$W_{\hat{p}_{i-1}}$	$W_{\hat{p}_{i-1}}$	…
1 0 1 … 1 1						0
1 1 0 … 0 0	1	−1		-2^{2i-2}	$2^{2i-2} + W_{\hat{p}_{i-1}}(\mathbf{0})$	
				0		
	…	…		…	$W_{\hat{p}_{i-1}}$	$-2W_{\hat{p}_{i-1}}$
1 1 1 … 1 1	1	−1		0		

$a_{i-1}\ b_{i-1}\ \dots\ a_0\ b_0$	p_i	$\hat{p}_i$	$\dots$			$W_{\hat{p}_i}$
0 0 0 … 0 0	0	1		2^{2i-2}	$2^{2i-2} + W_{\hat{p}_{i-1}}(\mathbf{0})$	
				0		
	…	…		…	$W_{\hat{p}_{i-1}}$	$2W_{\hat{p}_{i-1}}$
0 0 1 … 1 1	0	1		0		
0 1 0 … 0 0					$2^{2i-2} - W_{\hat{p}_{i-1}}(\mathbf{0})$	2^{2i-1}
						0
	p_{i-1}	$\hat{p}_{i-1}$		$W_{\hat{p}_{i-1}}$	$-W_{\hat{p}_{i-1}}$	…
0 1 1 … 1 1						0
1 0 0 … 0 0					$W_{\hat{p}_{i-1}}(\mathbf{0}) - 2^{2i-2}$	2^{2i-1}
						0
	p_{i-1}	$\hat{p}_{i-1}$		$W_{\hat{p}_{i-1}}$	$W_{\hat{p}_{i-1}}$	…
1 0 1 … 1 1						0
1 1 0 … 0 0	1	−1		-2^{2i-2}	$2^{2i-2} + W_{\hat{p}_{i-1}}(\mathbf{0})$	
				0		
	…	…		…	$W_{\hat{p}_{i-1}}$	$-2W_{\hat{p}_{i-1}}$
1 1 1 … 1 1	1	−1		0		

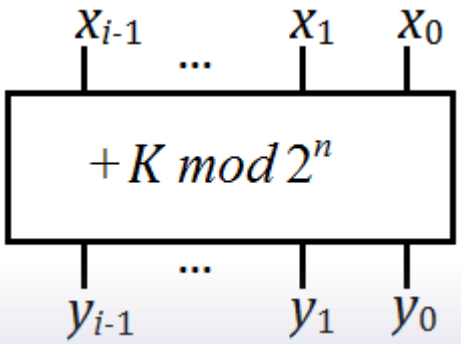
Линейная аппроксимация $+\mathrm{mod}2^n$



$$Prob(d_i = a_i \oplus b_i \oplus a_{i-1}) = 0.75$$

$$Prob(d_i = a_i \oplus b_i \oplus b_{i-1}) = 0.75$$

Линейная аппроксимация $+\mathrm{mod}2^n$

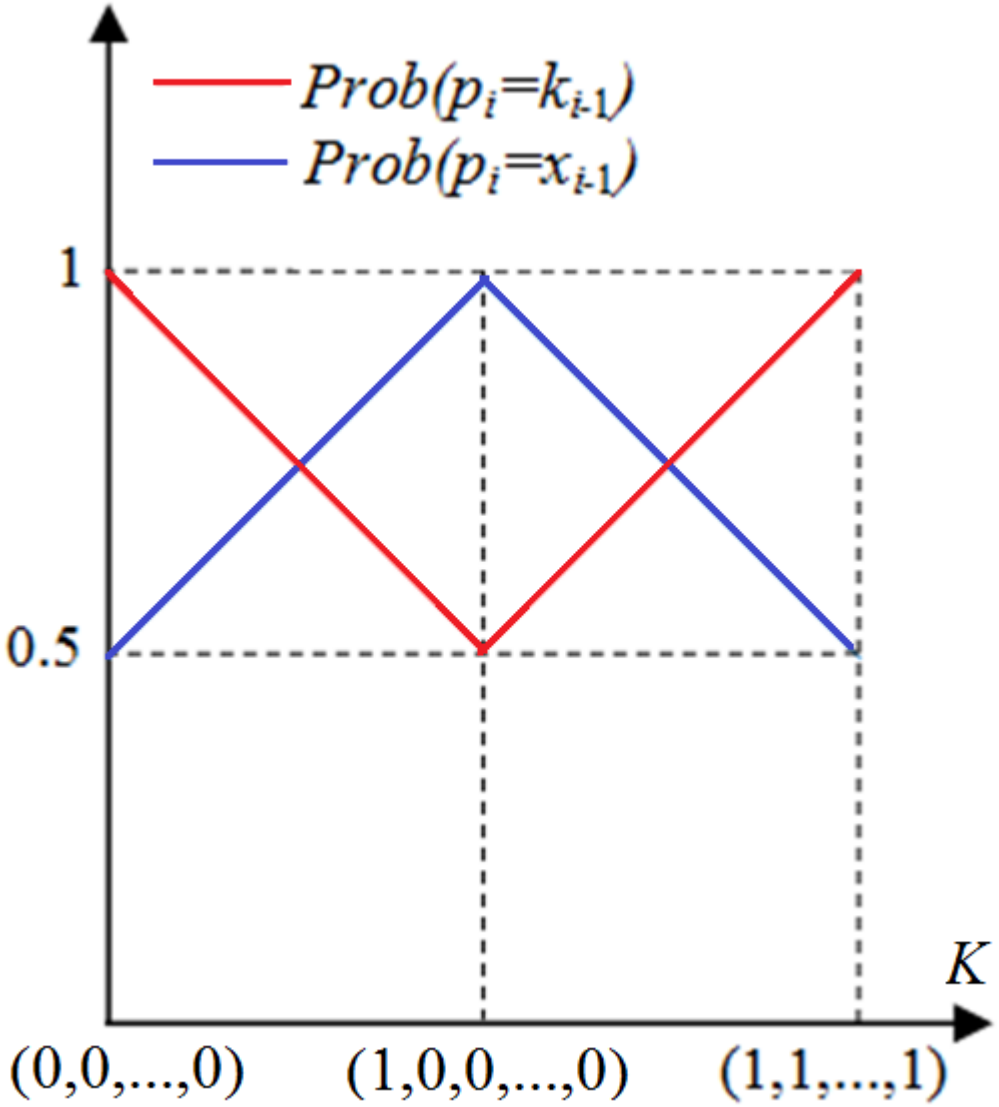


$$X + K = Y \bmod 2^n$$

$\forall\, i > 0$ и фиксированного K

$$Prob(p_i = x_{i-1}) = \frac{1}{2} + \varepsilon, \text{ где } 0 \le |\varepsilon| \le 0.5$$

$$Prob(p_i = k_{i-1}) = \frac{1}{2} + \varepsilon, \text{ где } 0 \le |\varepsilon| \le 0.5$$


Prob(p_i=k_{i-1})
Prob(p_i=x_{i-1})
1
0.5
K
(0,0,...,0)
(1,0,0,...,0)
(1,1,...,1)

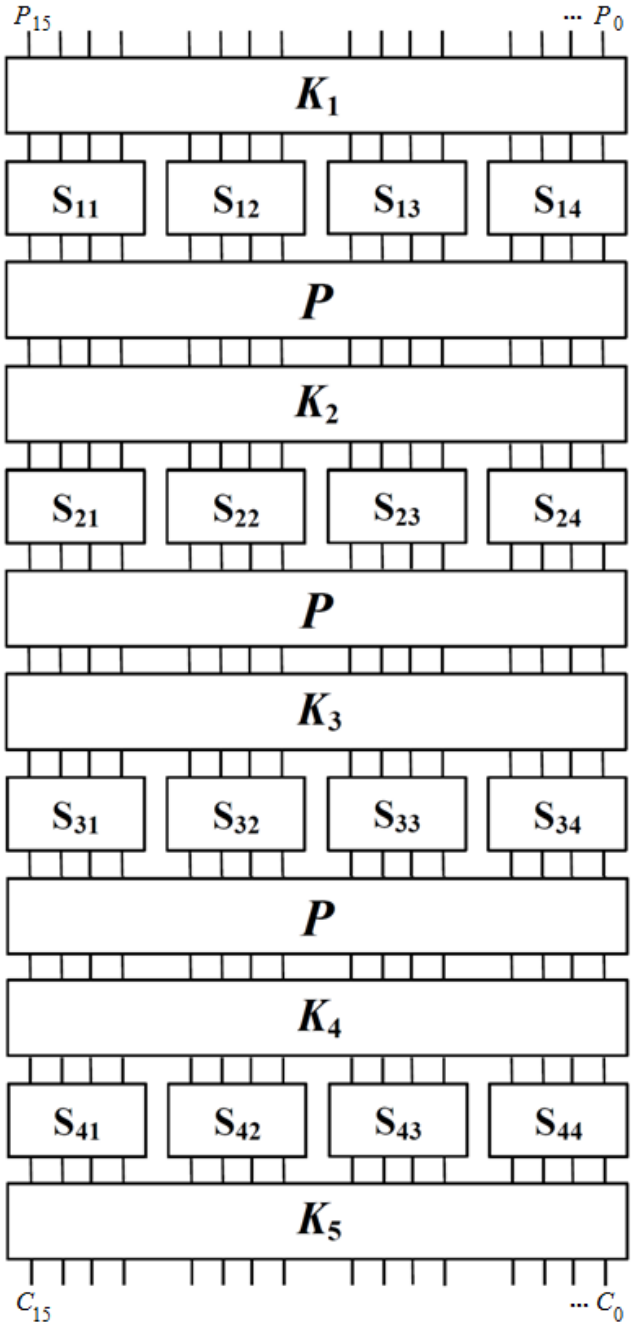
Нелинейная аппроксимация $+\mathrm{mod}2^n$

$$\forall i > 0\ \exists z:\ Prob(y_i = x_i \oplus z \cdot x_{i-1}) = \frac{1}{2} + \varepsilon, \text{где } |\varepsilon| \geq \frac{1}{4}$$

Нелинейная аппроксимация $+\bmod 2^n$

$$\forall i > 0\ \exists z:\ Prob(y_i = x_i \oplus z \cdot x_{i-1}) = \frac{1}{2} + \varepsilon, \text{где } |\varepsilon| \geq \frac{1}{4}$$

$$\forall i > 0\ \exists z:\ Prob(y_i \oplus y_{i-1} = x_i \oplus z \cdot x_{i-1}) = \frac{1}{2} + \varepsilon, \text{где } |\varepsilon| \geq \frac{1}{4}$$



Обозначения

$X_{i,j}$ – j-тый бит входа в i-тый блок смешения с подключом

$Y_{i,j}$ – j-тый бит выхода из i-того блока смешения с подключом

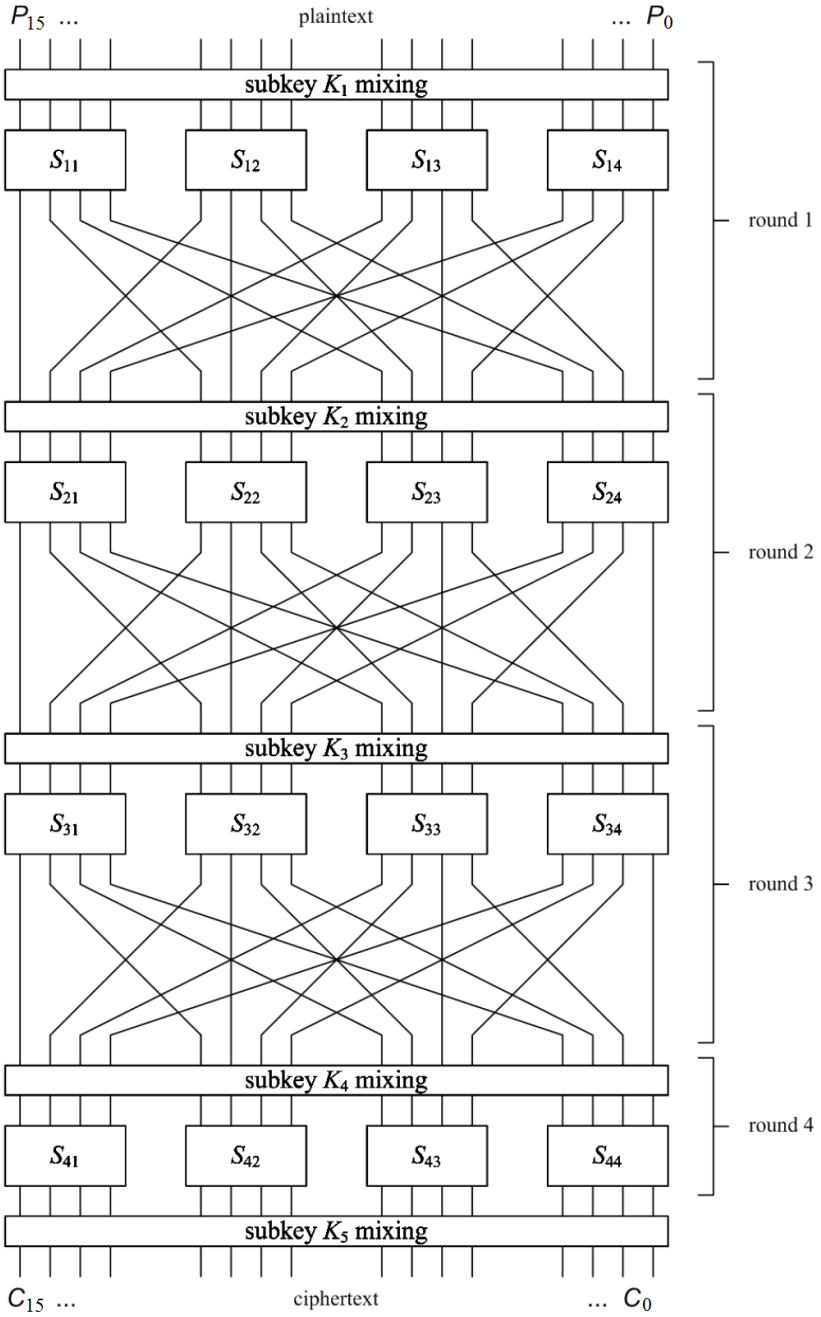
$V_{i,j}$ – j-тый бит выхода из i-того слоя S-box

Описание S-блока

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

Описание P-блока

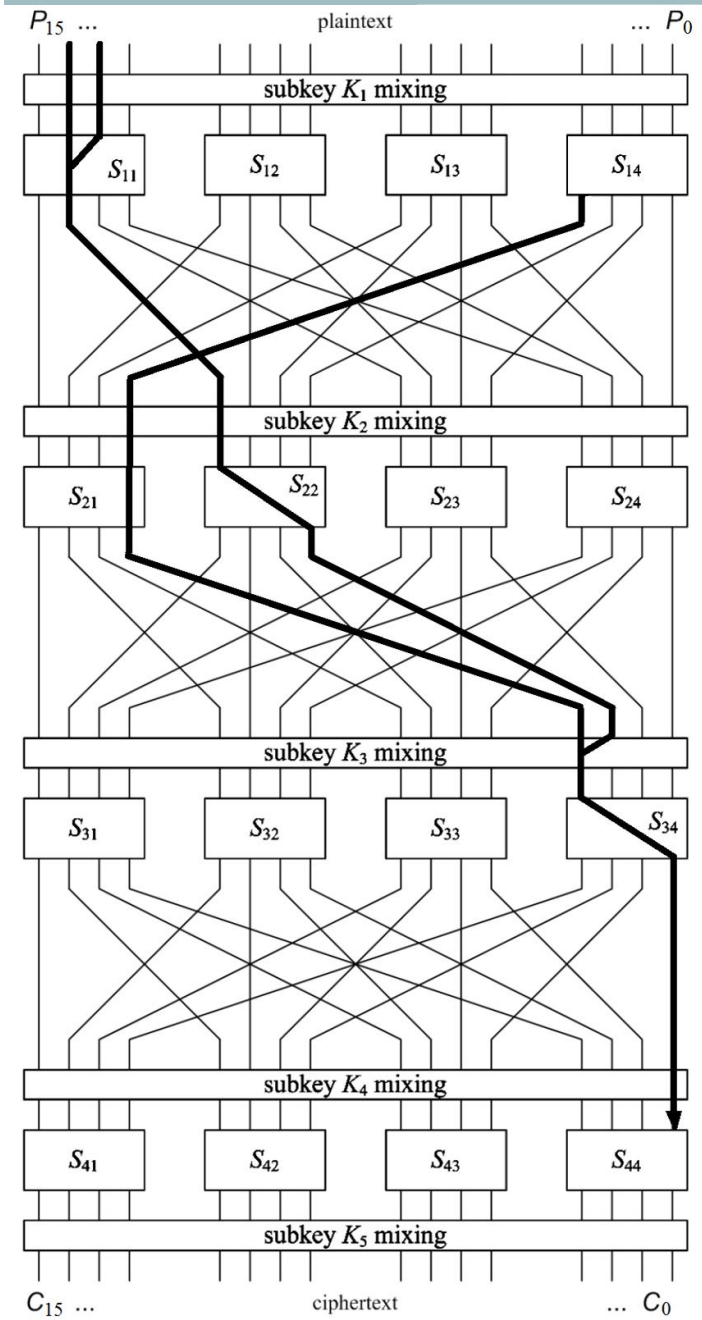
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	4	8	12	1	5	9	13	2	6	10	14	3	7	11	15


P_{15} ...
plaintext
... P_0
subkey K_1 mixing
S_{11}
S_{12}
S_{13}
S_{14}
round 1
subkey K_2 mixing
S_{21}
S_{22}
S_{23}
S_{24}
round 2
subkey K_3 mixing
S_{31}
S_{32}
S_{33}
S_{34}
round 3
subkey K_4 mixing
S_{41}
S_{42}
S_{43}
S_{44}
round 4
subkey K_5 mixing
C_{15} ...
ciphertext
... C_0

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
0000	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0001	0	-4	0	-4	-4	0	-4	0	12	0	-4	0	0	-4	0	-4
0010	0	-4	-8	4	4	0	4	-8	0	-8	-8	0	0	0	0	0
0011	0	0	0	0	8	0	0	-8	0	-8	-8	0	0	0	0	0
0100	0	0	4	-4	0	0	12	4	4	-4	0	0	-4	4	0	0
0101	0	-4	-4	0	-4	0	0	-4	0	-4	4	-8	-4	0	8	4
0110	0	4	4	0	-4	0	0	-4	0	-4	4	8	4	0	8	-4
0111	0	-8	4	4	0	0	4	-4	-4	4	0	0	-4	-4	0	-8
1000	0	0	4	4	0	-8	-4	4	0	-8	4	-4	0	0	-4	-4
1001	0	-4	4	0	4	0	0	-4	4	0	8	4	0	-4	-4	8
1010	0	-4	-4	-8	4	-8	0	4	-4	0	0	4	0	-4	4	0
1011	0	0	4	4	0	0	4	4	0	0	-4	-4	8	-8	4	4
1100	0	0	0	-8	0	8	0	0	-4	-4	4	-4	4	-4	-4	-4
1101	0	-4	8	-8	4	0	-4	0	0	4	0	-4	4	8	4	0
1110	0	4	0	-4	-4	-8	4	-8	0	4	0	-4	4	0	-4	0
1111	0	8	0	0	8	0	0	0	4	4	4	-4	-4	-4	4	-4

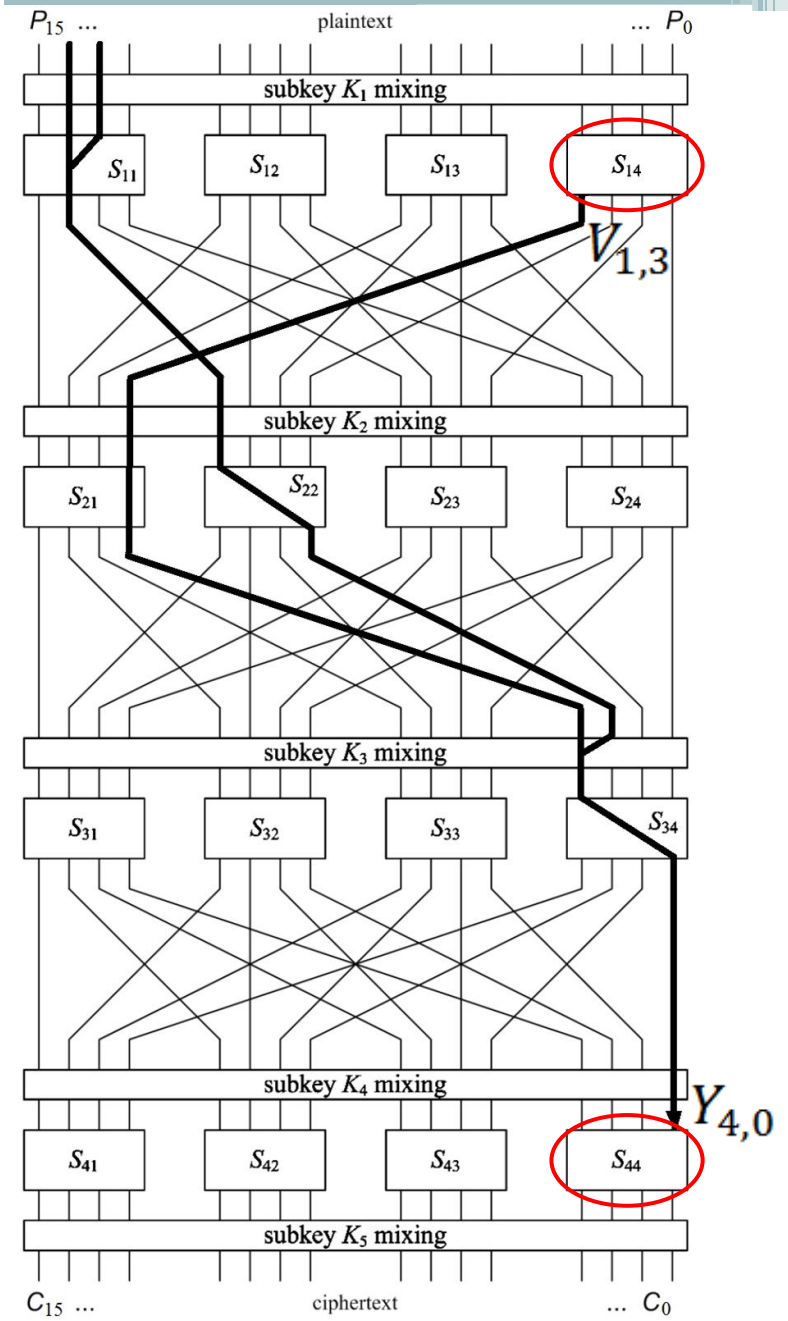
	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
0000	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0001	0	-4	0	-4	-4	0	-4	0	12	0	-4	0	0	-4	0	-4
0010	0	-4	-8	4	4	0	4	-8	0	-8	-8	0	0	0	0	0
0011	0	0	0	0	8	0	0	-8	0	-8	-8	0	0	0	0	0
0100	0	0	4	-4	0	0	12	4	4	-4	0	0	-4	4	0	0
0101	0	-4	-4	0	-4	0	0	-4	0	-4	4	-8	-4	0	8	4
0110	0	4	4	0	-4	0	0	-4	0	-4	4	8	4	0	8	-4
0111	0	-8	4	4	0	0	4	-4	-4	4	0	0	-4	-4	0	-8
1000	0	0	4	4	0	-8	-4	4	0	-8	4	-4	0	0	-4	-4
1001	0	-4	4	0	4	0	0	-4	4	0	8	4	0	-4	-4	8
1010	0	-4	-4	-8	4	-8	0	4	-4	0	0	4	0	-4	4	0
1011	0	0	4	4	0	0	4	4	0	0	-4	-4	8	-8	4	4
1100	0	0	0	-8	0	8	0	0	-4	-4	4	-4	4	-4	-4	-4
1101	0	-4	8	-8	4	0	-4	0	0	4	0	-4	4	8	4	0
1110	0	4	0	-4	-4	-8	4	-8	0	4	0	-4	4	0	-4	0
1111	0	8	0	0	8	0	0	0	4	4	4	-4	-4	-4	4	-4

- $S_{11} : V_2 = Y_1 \oplus Y_2 \, , \, bias = \frac{3}{8}$
- $S_{21} : V_0 = Y_0 \, , \, bias = \frac{1}{8}$
- $S_{22} : V_0 = Y_3 \, , \, bias = \frac{3}{8}$
- $S_{34} : V_0 = Y_3 \, , \, bias = \frac{3}{8}$
- $\exists z_0 : X_{1,14} \oplus X_{1,13} z_0 = Y_{1,14} \oplus Y_{1,13} \, , \, bias \geq \frac{1}{4}$
- $\exists z_1 : X_{3,3} \oplus X_{3,2} z_1 = Y_{3,3} \, , \, bias \geq \frac{1}{4}$
- $\exists z_2 : X_{2,12} \oplus X_{2,11} z_2 = Y_{2,12} \oplus Y_{2,11} \, , \, bias \geq \frac{1}{4}$
- $\exists z_3 : X_{2,12} \oplus X_{2,11} z_3 = Y_{2,12} \, , \, bias \geq \frac{1}{4}$
- $X_{4,0} = Y_{4,0} \, , \, bias = \frac{1}{2}$



Итоговое соотношение

$$V_{1,3} \oplus z_1 (P_{14} \oplus z_0 P_{13}) = Y_{4,0}$$

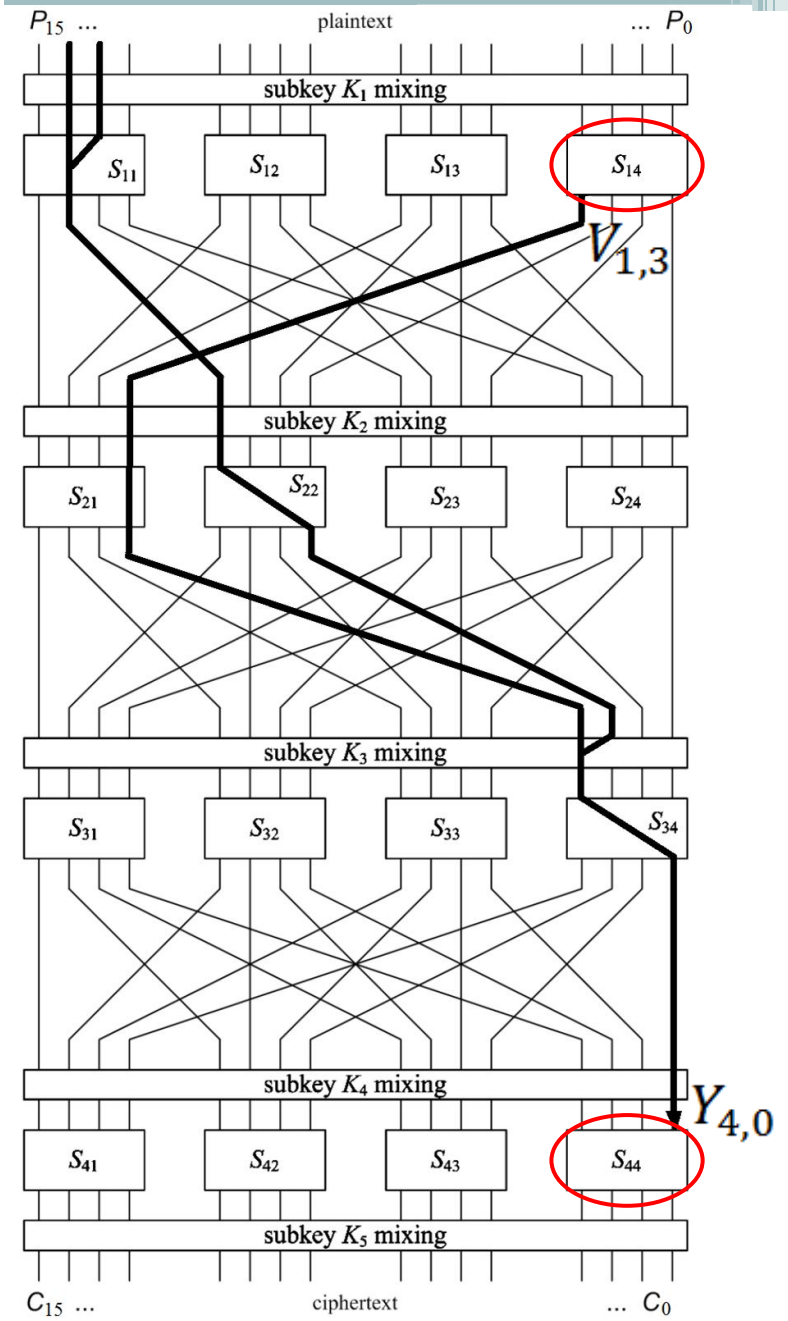


Итоговое соотношение

$$V_{1,3} \oplus z_1 (P_{14} \oplus z_0 P_{13}) = Y_{4,0}$$

$$bias \geq 2^6 \cdot \frac{1}{8} \cdot \left(\frac{3}{8}\right)^3 \cdot \left(\frac{1}{4}\right)^3 = \frac{27}{4096}$$

$$\left(\frac{27}{4096}\right)^{-2} = 23\,000$$



Описание анализа

- Генерируется 23 000 пар открытый текст/шифртекст
- Перебираются всевозможные значения $K_{1,0}, K_{1,1}, K_{1,2}, K_{1,3}, K_{5,0}, K_{5,1}, K_{5,2}\ K_{5,3}$ и z_0, z_1 и для каждого вычисляется *bias* соотношения $V_{1,3} \oplus z_1 (P_{14} \oplus z_0 P_{13}) = Y_{4,0}$
- Значения, на которых получено наибольшее преобладание принимаются за истинные биты ключа

Результаты расчета на ЭВМ

K_1=55ad K_2=46d6 K_3=e5e1 K_4=7e28 K_5=b08b

№	*bias*	$K_{1,3}K_{1,2}K_{1,1}K_{1,0}$	$K_{5,3}K_{5,2}K_{5,1}K_{5,0}$
1	0.0534	d	b
2	0.0353	d	8
3	0.0247	d	a
4	0.0206	d	9
5	0.0194	d	c

Результаты расчета на ЭВМ

K_1=fe23 K_2=2fed K_3=daa4 K_4=52e6 K_5=936c

№	*bias*	$K_{1,3}K_{1,2}K_{1,1}K_{1,0}$	$K_{5,3}K_{5,2}K_{5,1}K_{5,0}$
1	0.0513	3	c
2	0.0463	3	a
3	0.0336	3	b
4	0.0297	3	9
5	0.02667	b	c
6	0.0254	3	6

Результаты расчета на ЭВМ

K_1=bc7f K_2=4978 K_3=74cb K_4=a488 K_5=46df

№	*bias*	$K_{1,3}K_{1,2}K_{1,1}K_{1,0}$	$K_{5,3}K_{5,2}K_{5,1}K_{5,0}$
1	0.0433	f	f
2	0.0339	f	e
3	0.0331	f	0
4	0.0248	f	1
5	0.0247	f	6

Выводы

При использовании $+mod\ 2^n$ вместо XOR

- Сложнее строить соотношения связывающие биты открытого текста/шифртекста и ключа
- Полученные соотношения в худшем случаи выполняются с низким преобладанием

Спасибо за внимание!

Карондеев А.М.
karondeev@yandex.ru

- [1] Debdeep Mukhopadhyay «Design and Analusis of Cellural Automata Based Cryptographic Algorithms». Kharagpur, Indian Institute of Technology, 2007
- [2] Matsui M. «Linear Cryptanalysis Method for DES Cipher» // LNCS. 1993. V.765. P.386–397