Математические основы информационной безопасности

Груздев Дмитрий Николаевич

Современные алгоритмы шифрования

Классификации шифров

По области применения:

ограниченного использования

общего использования

По свойствам ключа шифрования:

симметричные

асимметричные

По характеру шифрования символов:

потоковые

блочные

Симметричные шифры

Шифрование и расшифрование данных производится на одном ключе.

Блочные

Потоковые

Блочные шифры

Исходные данные разбиваются на блоки одинакового размера. К полученным блокам применяется одинаковая процедура шифрования.

Являются шифрами простой замены с алфавитом размера 2^L (L - длина блока в битах) при фиксированном ключе.

Шифр простой замены

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж

А – (0,0,0,0,0), Б – (0,0,0,0,1), …, Я – (1,1,1,1,1)

Размер блока (буква) – 5 бит

Размер алфавита – 32 символа

Шифр Хилла

Предложен в 1929г. математиком Лестером Хиллом.

Текст шифруется блоками из n символов.

$c_i = p_i * A, \quad p_i = c_i * A^{-1}$

Размер блока – 5*n бит.

Размер алфавита 2^{5*n} символов.

Атака по открытому тексту

Производится, когда в шифротексте присутствуют отрывки, известные аналитику.

Выполняется для восстановления ключа шифрования.

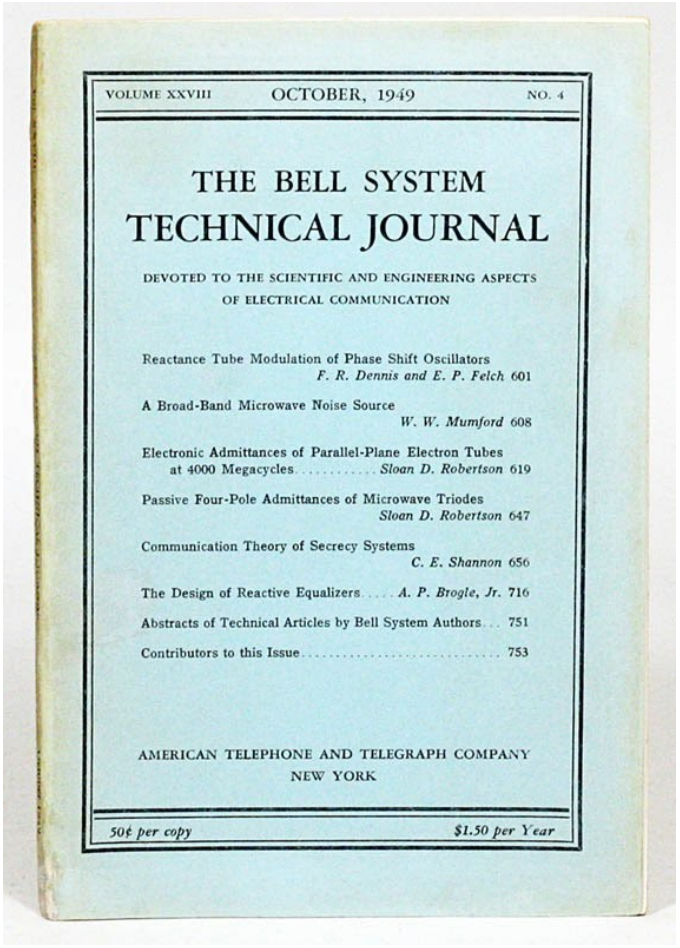
Все рассмотренные шифры замены и гаммирования были подвержены этой атаке.

Требования к шифрам

Шифротекст должен скрывать избыточность данных открытого текста.

Обладая парами отрытый текст – шифротекст аналитик не должен иметь возможности восстановить ключ шифрования.

Статья Клода Шеннона



VOLUME XXVIII OCTOBER, 1949 NO. 4

THE BELL SYSTEM
TECHNICAL JOURNAL

DEVOTED TO THE SCIENTIFIC AND ENGINEERING ASPECTS
OF ELECTRICAL COMMUNICATION

AMERICAN TELEPHONE AND TELEGRAPH COMPANY
NEW YORK

50¢ per copy *$1.50 per Year*

Первым произвел описание криптографии с математической точки зрения.

Дал описание криптостойких систем на основе простых операций, ввел понятия диффузии и конфузии.

Диффузия

Диффузия – метод, при котором выходные данные скрывают избыточность в статистике входных данных.

Для обеспечения хорошей диффузии необходимо, чтобы каждый бит входных данных влиял на каждый бит выходных данных.

Конфузия

Конфузия – метод, при котором зависимость ключа и выходных данных делается как можно более сложной (в частности, нелинейной).

Достигается применением нелинейных преобразований в процессе шифрования.

Лавинный эффект

Изменение малого количества бит во входном тексте или ключе ведет к “лавинному” изменению бит выходного шифртекста.

Является следствием хорошей диффузии и конфузии.

Лавинный эффект

AES(ключ = "aaaaaaaaaaaaaaaa", "aaaaaaaaaaaaaaaa") = '5188c6474b228cbdd242e9125ebe1d53'

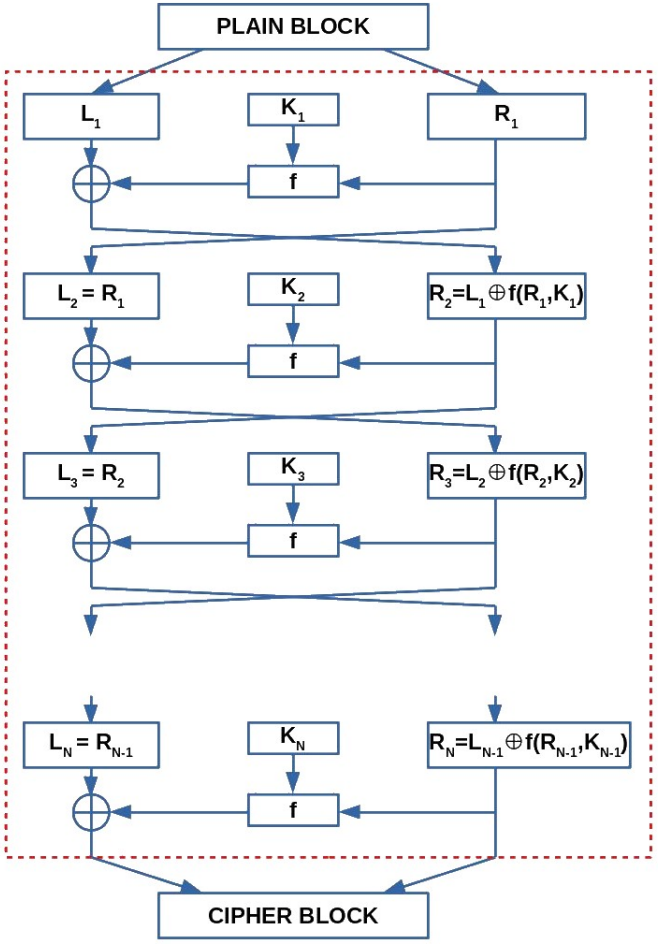
AES(ключ = "aaaaaaaaaaaaaaaa", "aacaaaaaaaaaaaaa") = 'f7e5c1118f5cb86198e37ff7a29974bc'

AES(ключ = "aacaaaaaaaaaaaaa", "aaaaaaaaaaaaaaaa") = '2c50b5cac9c755d67aa61b87c26248eb'

Caesar(ключ = 3, "aaaaaaaaaaaaaaaa") = 'dddddddddddddddd'

Caesar(ключ = 3, "acaaaaaaaaaaaaaa") = 'dfddddddddddddd'

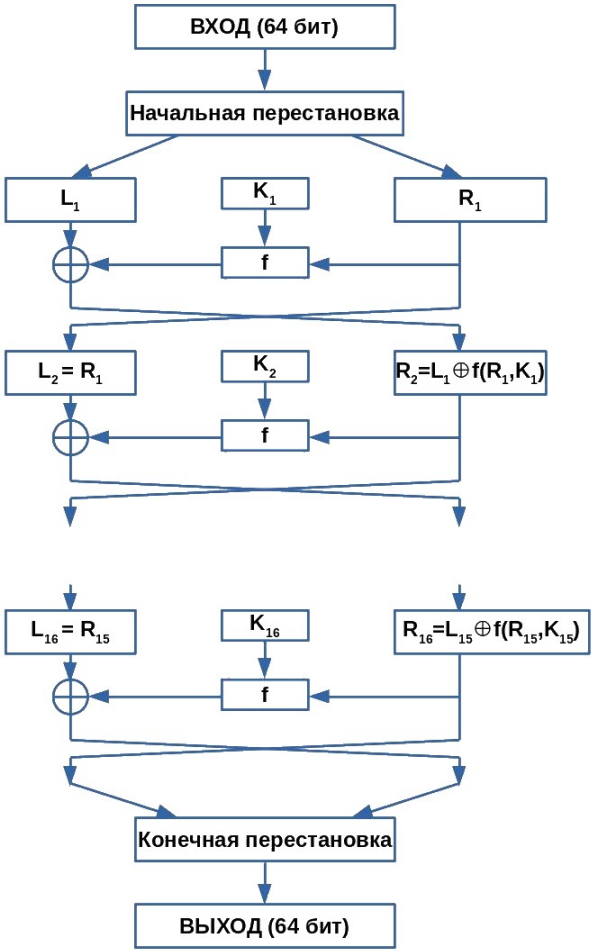
Сеть Фейстеля



Примеры:

DES, ГОСТ 28147-89, Blowfish, CAST, FEAL, IDEA, Khufu, Twofish

DES



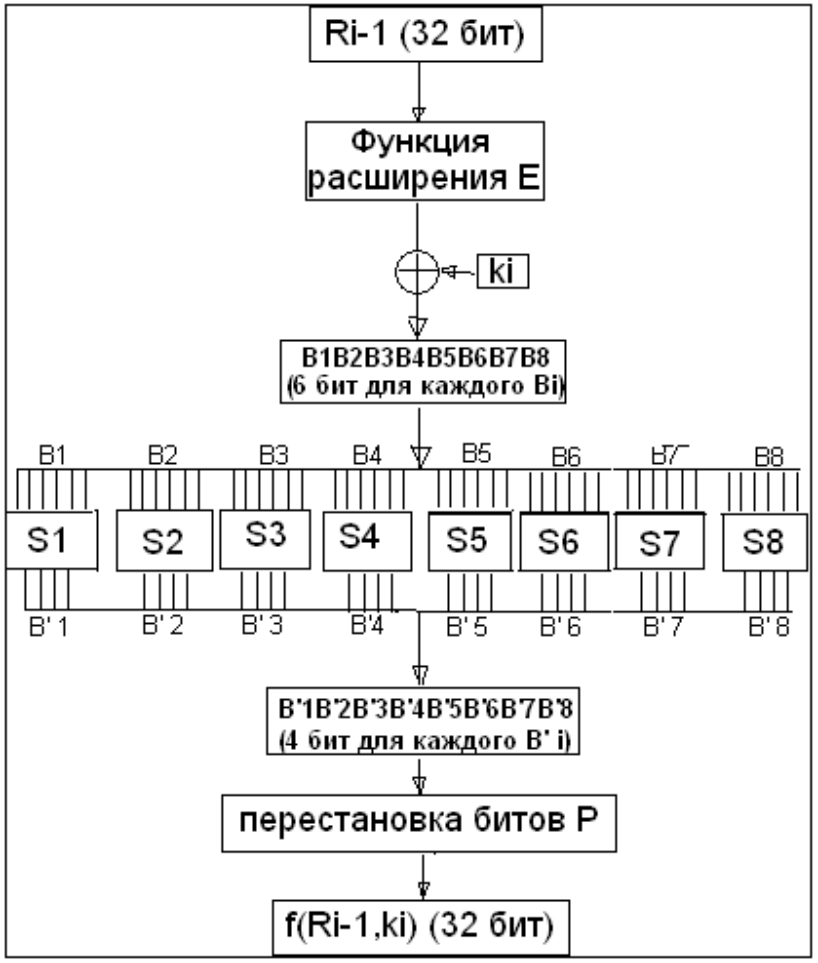
Опубликован в 1977 г.

Размер блока – 64 бита

Размер ключа – 56 бит

Количество раундов шифрования – 16

Функция Фейстеля



E – расширяет 32-бита в 48 бит, дублируя некоторые биты.

S-блоки

Обеспечивают лавинный эффект и нелинейность шифрования.

$(a_1,a_2,a_3,a_4,a_5,a_6) – (b_1,b_2,b_3,b_4)$

$(a_1,a_6) = y$, $(a_2,a_3,a_4,a_5) = x$

$(b_1,b_2,b_3,b_4) = S[y,x]$

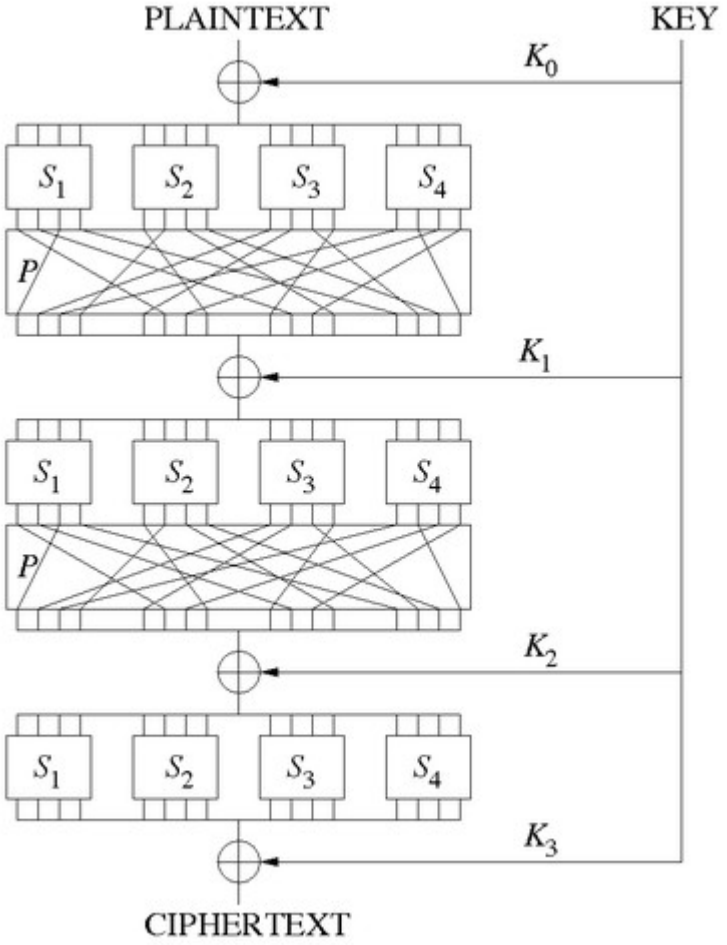
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	10	3	14	10	0	6	13

S-блоки

Пример S-блока, не обеспечивающего нелинейности преобразований $(b_1,b_2,b_3,b_4) = (a_2,a_3,a_4,a_5)$.

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

SP-сеть



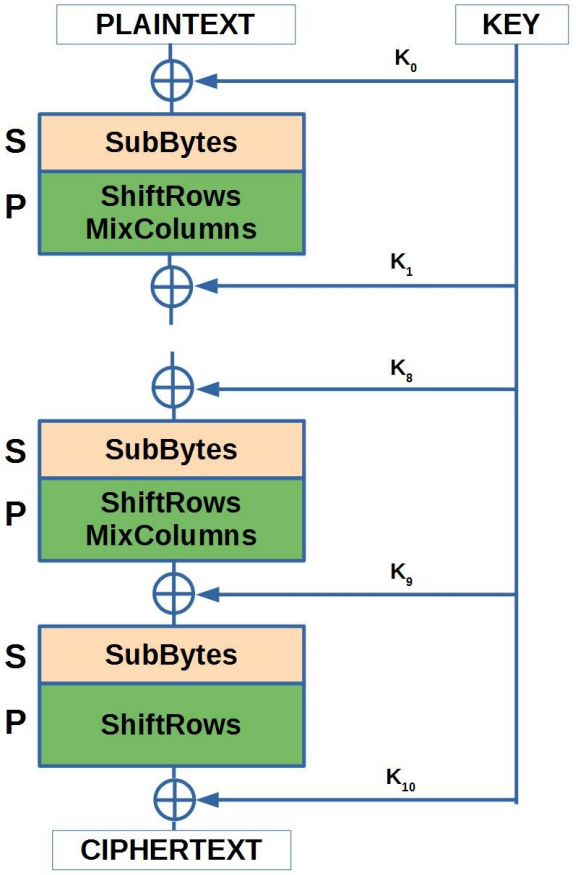
S – substitution stage

P – permutation stage

Примеры:

AES, Lucifer, SAFER, Rainbow, Threefish, Кузнечик.

AES (Rijndael)



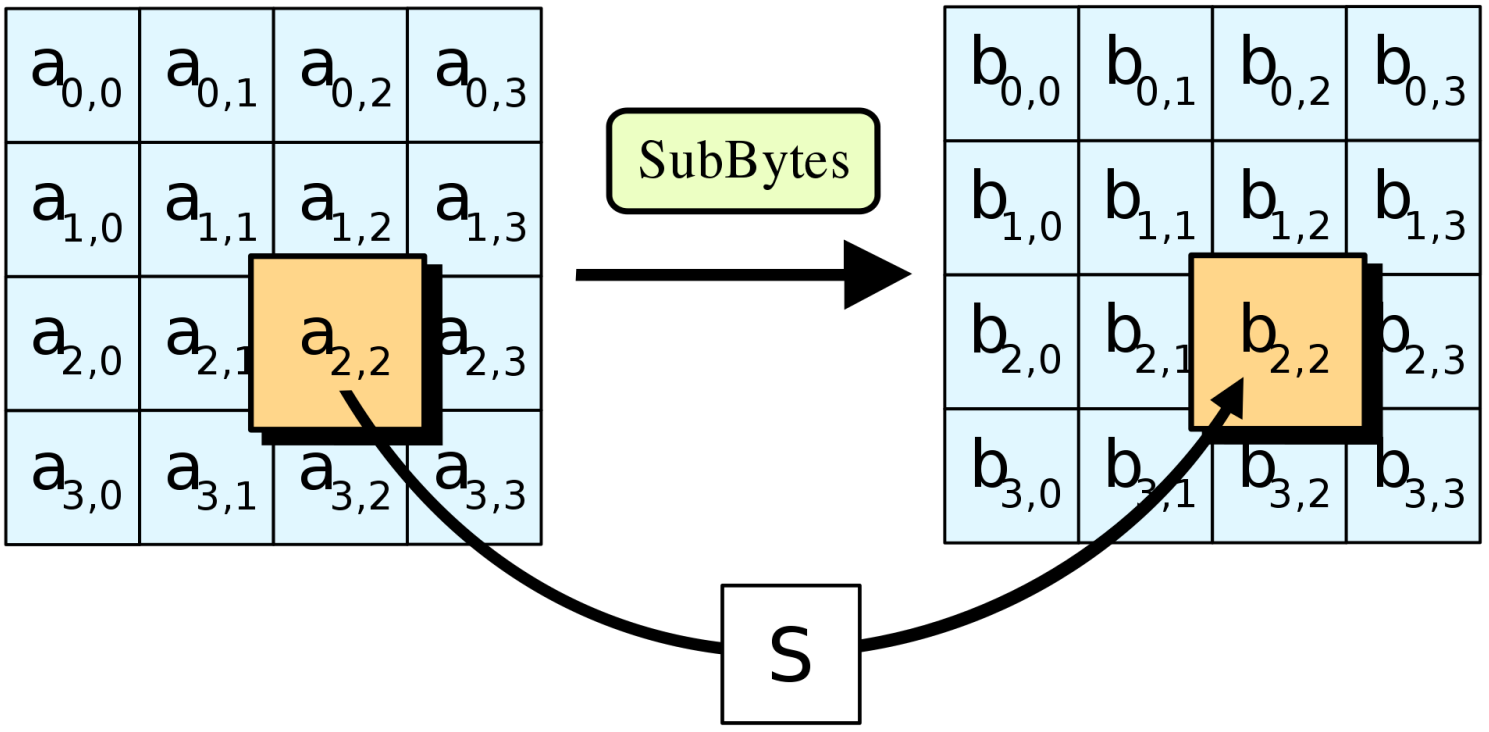
Создан в 1998 г.

Размер блока – 128 бит.

Размер ключа – 128/196/256 бит.

Количество раундов шифрования – 10/12/14

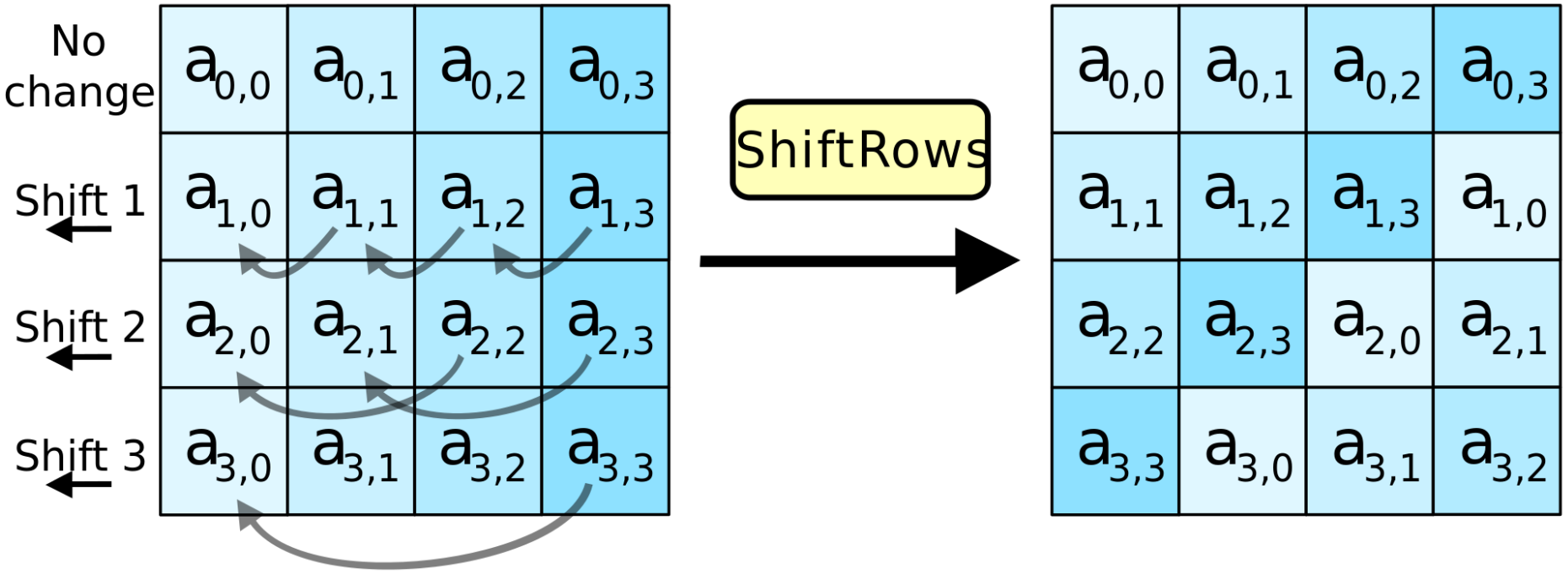
SubBytes


a0,0 a0,1 a0,2 a0,3
a1,0 a1,1 a1,2 a1,3
a2,0 a2,1 a2,2 a2,3
a3,0 a3,1 a3,2 a3,3
SubBytes
b0,0 b0,1 b0,2 b0,3
b1,0 b1,1 b1,2 b1,3
b2,0 b2,1 b2,2 b2,3
b3,0 b3,1 b3,2 b3,3
S

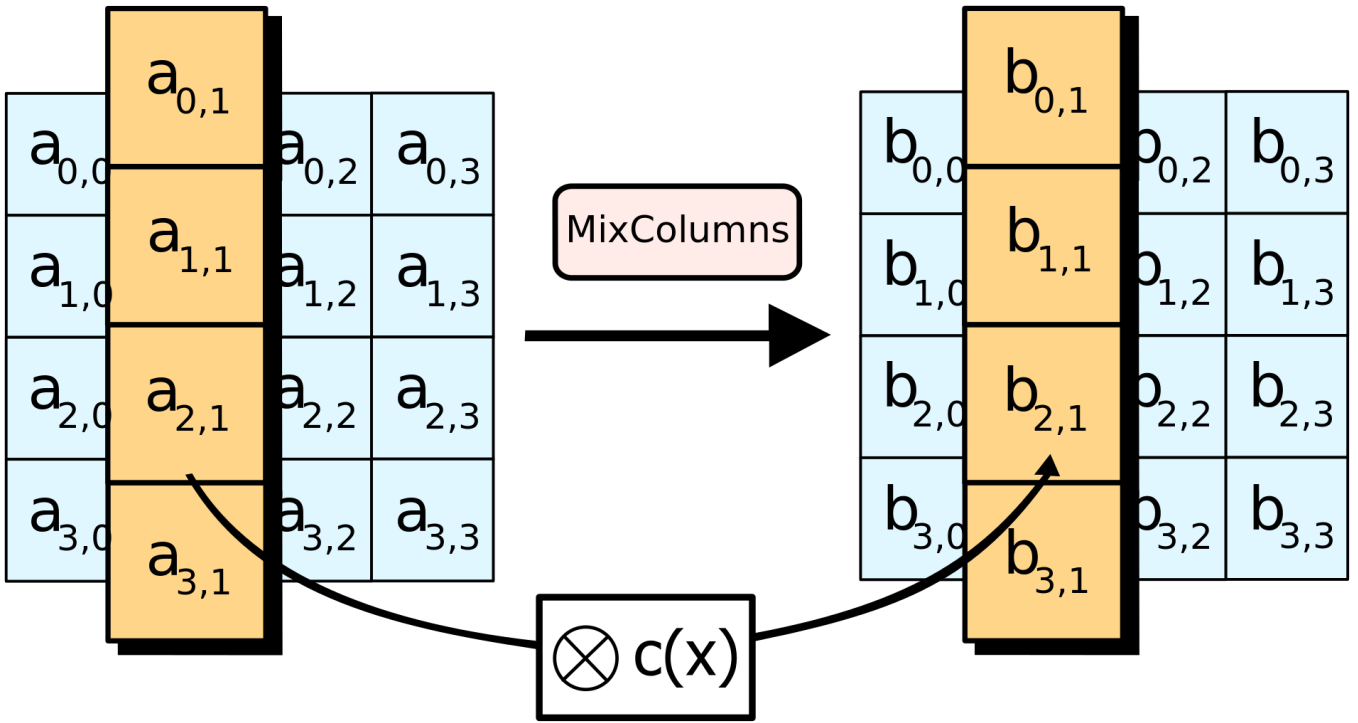
SubBytes

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

ShiftRows

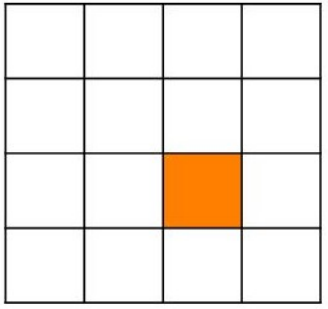

No change
Shift 1
Shift 2
Shift 3
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
ShiftRows
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,1}$ $a_{1,2}$ $a_{1,3}$ $a_{1,0}$
$a_{2,2}$ $a_{2,3}$ $a_{2,0}$ $a_{2,1}$
$a_{3,3}$ $a_{3,0}$ $a_{3,1}$ $a_{3,2}$

MixColumns

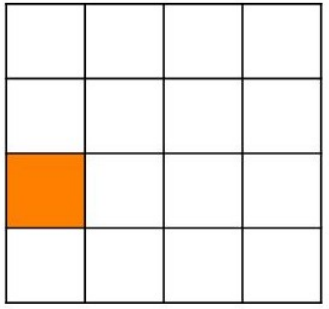


Умножение многочлена с коэффициентами ($a_{0,i}$,$a_{1,i}$,$a_{2,i}$,$a_{3,i}$) на $c(x) = 3x^3+x^2+x+2$ по модулю x^4+1.

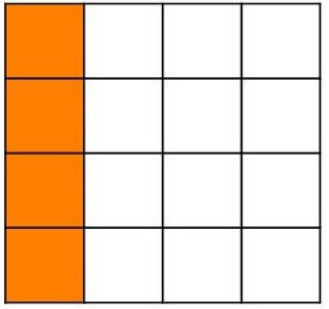
Лавинный эффект в AES



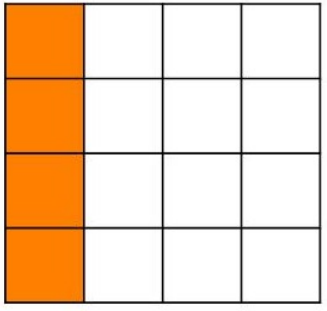
SubBytes



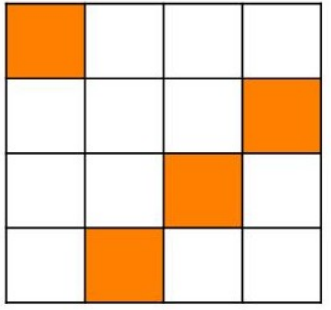
ShiftRows



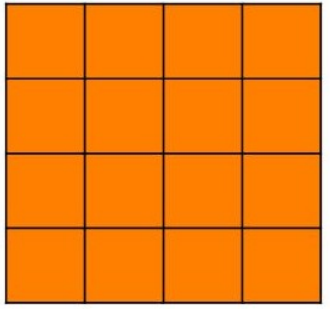
MixColumns



SubBytes



ShiftRows



MixColumns

Режимы шифрования

ECB (Electronic Code Book)
каждый блок шифруется независимо

CBC (Cipher Block Chaining)
перед шифрованием блок “ксорится” с предыдущим зашифрованным блоком

Требования к блочным шифрам

Требования конкурса AES 2000 г.:

использовать операции, легко реализуемые аппаратно (в микрочипах) и программно;

ориентироваться на 32-разрядные процессоры;

простота структуры шифра.

Проверялись в том числе:

оптимизация выполнения кода на различных архитектурах (от ПК до смарт-карт и аппаратных реализаций);

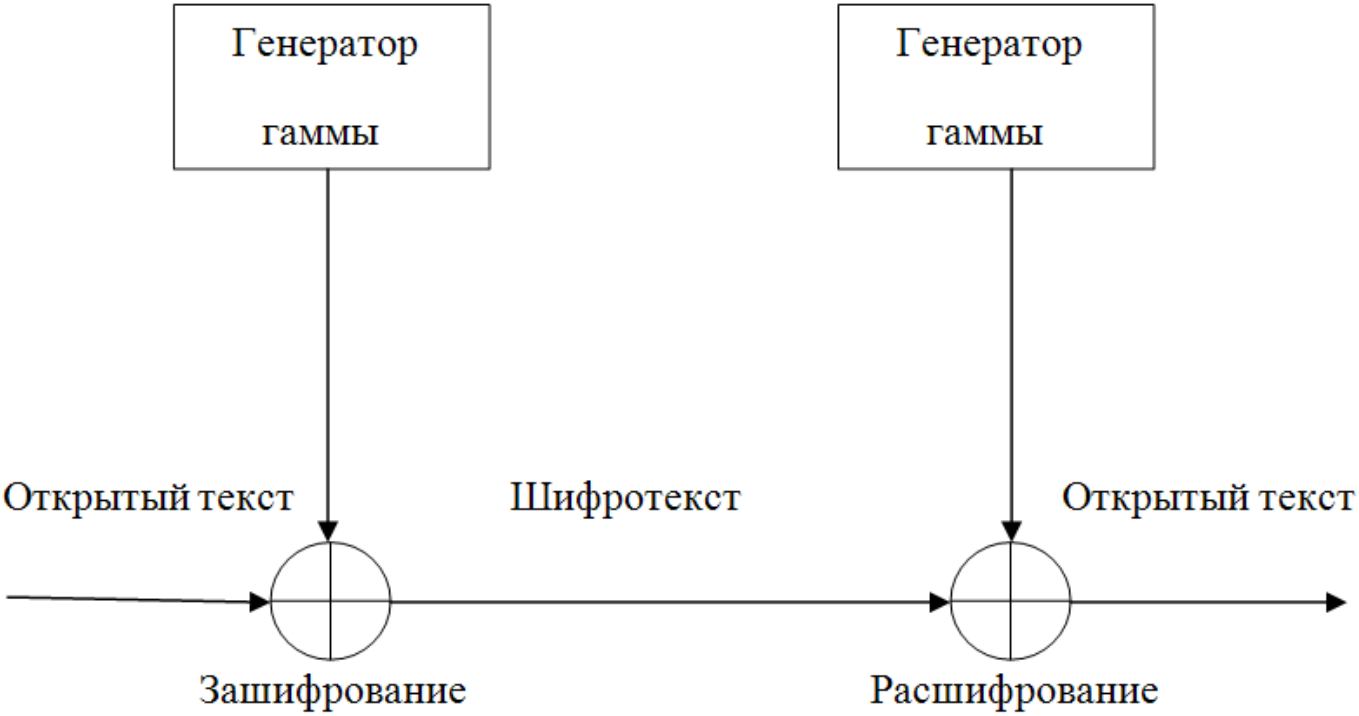
оптимизация размера кода;

возможность распараллеливания.

Потоковые шифры

Потоковый (поточный) шифр – симметричный шифр, в котором каждый символ открытого текста шифруется в зависимости от ключа шифрования и расположения в потоке открытого текста.

Потоковые шифры

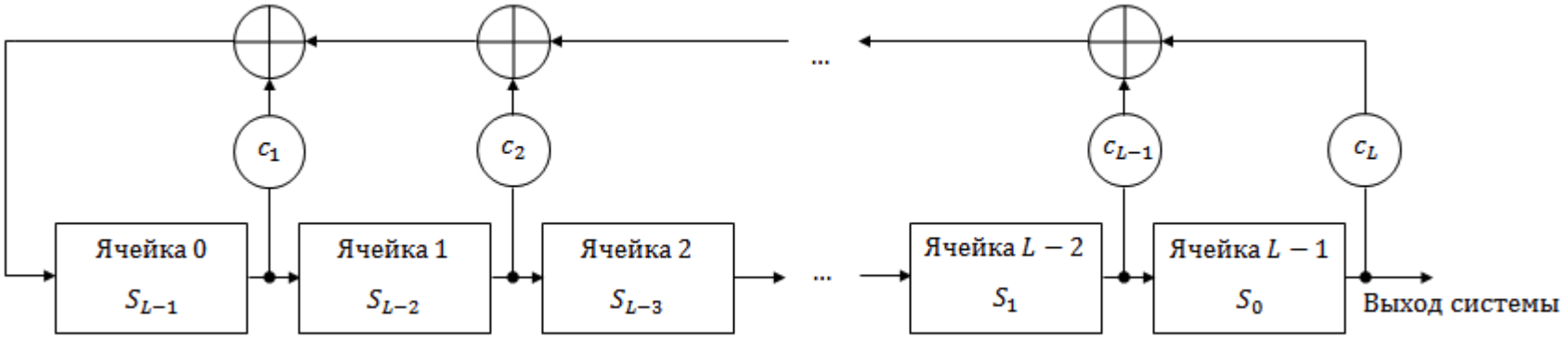


Генерация гаммы

Синхронные потоковые шифры – гамма генерируется независимо от открытого текста и шифротекста (A5, RC4, SEAL, Phelix).

Асинхронные (самосинхронизирующиеся) потоковые шифры – гамма создается функцией ключа и фиксированного числа знаков шифротекста (WAKE, Sapphire II).

РСЛОС



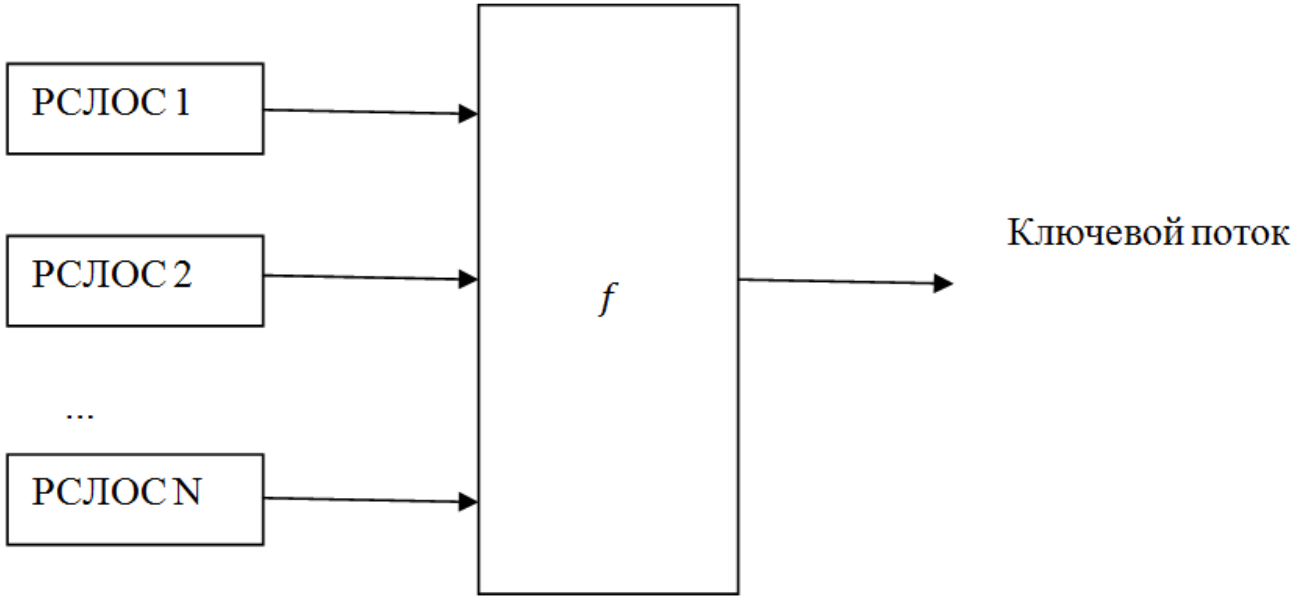
$S_{L-1} = (c_1 * S_{L-1}) \oplus (c_2 * S_{L-2}) \oplus (c_3 * S_{L-3}) \oplus \ldots \oplus (c_L * S_0)$

$S_{вых} = S_0$

Регистр сдвига с линейной обратной связью:

- высокое быстродействие
- простота аппаратной реализации
- высокие криптографические свойства
- легкость анализа

Нелинейные комбинации РСЛОС

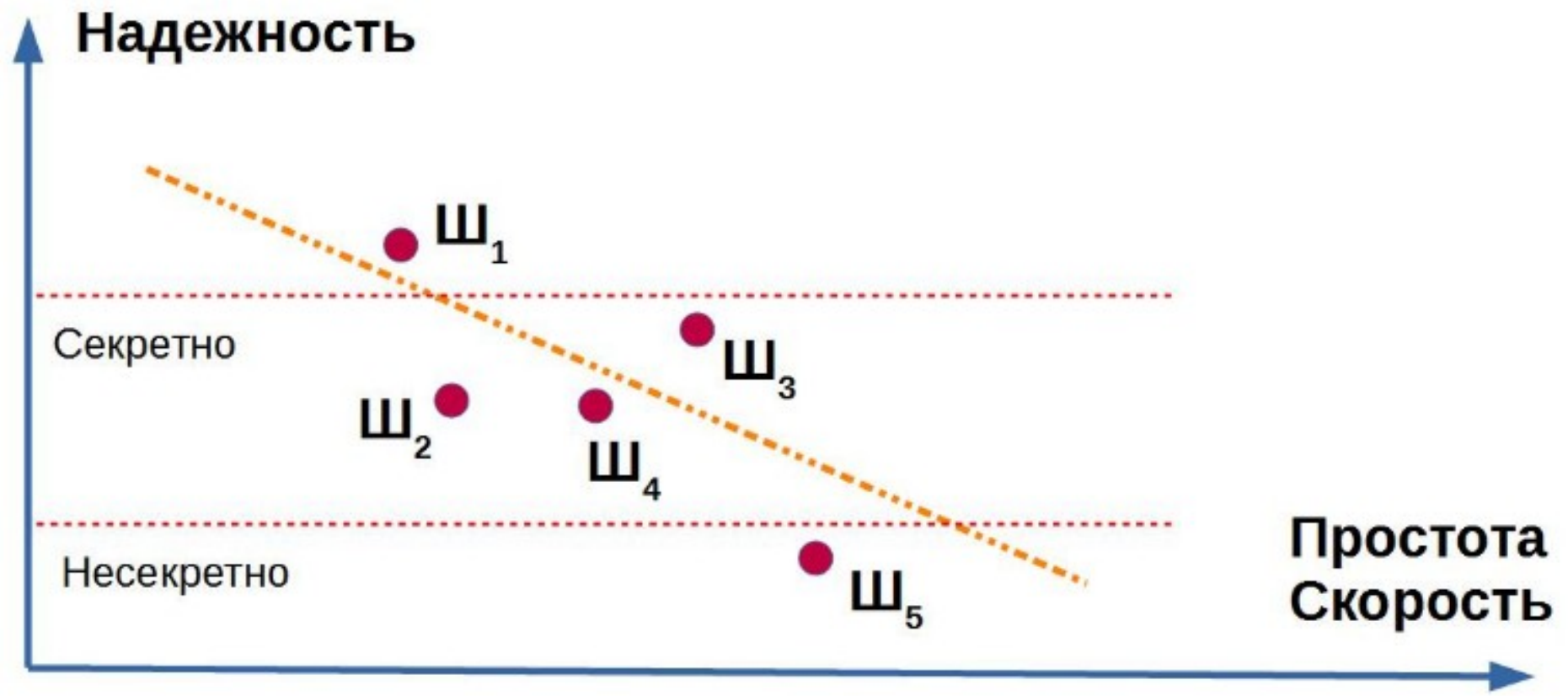


Например: $f(x_1,x_2,x_3,x_4) = x_1 \oplus x_1x_2 \oplus x_2x_3x_4$

Особенности поточных шифров

- Высокая скорость шифрования (наиболее пригодны для оперативного кодирования аудио- и видеоинформации).
- Простота аппаратной реализации.
- Подвержены большему количеству криптографических атак.

Выбор алгоритма шифрования



Асимметричные шифры

Шифры с открытым ключом

Сообщение шифруется на одном ключе, а расшифровывается на другом ключе.

Открытый – ключ, находящийся в общем доступе, используется для шифрования сообщения.

Закрытый – ключ, хранящийся у получателя сообщения, используется для расшифрования сообщения.

Восстановление закрытого ключа на основе открытого – вычислительно сложная задача.

Односторонние функции

- Разложение числа на множители.
- Вычисление дискретного логарифма в конечном поле ($a^x = b(p)$).
- Вычисление дискретного логарифма на группах точкек эллиптических кривых.
- Задача об укладке рюкзака.

RSA

Опубликована в 1977 г. (Rivest, Shamir и Adleman)

Формирование ключей

	Операция	Пример
1	Выбираются два простых числа **p** и **q.**	p = 7, q = 13
2	Вычисляется **n** = p * q.	n = 91
3	Вычисляется функция Эйлера **φ(n)** = (p – 1) * (q – 1).	φ(n) = 72
4	Выбирается произвольное **e** (0 < e < n) взаимно простое с φ(n).	e = 5
5	Вычисляется **d** такое, что e * d = 1 mod φ(n).	d = 29 (29 * 5 = 1 mod 72)
6	**(e, n)** – открытый ключ, **d** – закрытый ключ.	

RSA

Процедура шифрования:

$b = a^e \bmod n$

$a = b^d \bmod n$

Пример:

$(n = 91, e = 5), d = 29$

$a = 3$

$b = 3^5 \bmod 91 = 61$

$a = 61^{29} \bmod 91 = 3$

https://sesc-infosec.github.io/