О КРИПТОГРАФИЧЕСКИХ СВОЙСТВАХ ИТЕРАТИВНЫХ СИММЕТРИЧНЫХ БЛОЧНЫХ ШИФРОВ, ПОСТРОЕННЫХ НА ОСНОВЕ ОБОБЩЕНИЯ РАУНДОВОЙ ФУНКЦИИ ФЕЙСТЕЛЯ

конференция РусКрипто'2013 http://www.ruscrypto.ru/conference/

Конференция «РусКрипто'2013»

Pointlane ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Немного о себе

Коренева Алиса Михайловна

- Окончила НИЯУ МИФИ
  Кафедра №42 «Криптология и дискретная математика»
  (выпуск 2012) Научный руководитель Фомичев В.М.

- Ведущий специалист отдела информационной безопасности компании Pointlane

Обозначения и сокращения

- СБШ – симметричный блочный шифр
- МСЗ – матрица существенной зависимости
- *n* – длина регистра сдвига
- *r* – длина двоичного слова в ячейке регистра сдвига

Почему шифры Фейстеля?

- Высокая производительность шифрования
- Простота программной и аппаратной реализации
- Обеспечение инволютивности алгоритма шифрования
- Широта применения: DES, ГОСТ 28147-89, RC6, MARS, 2fish, LOKI и другие.

Итеративные СБШ регистрового типа

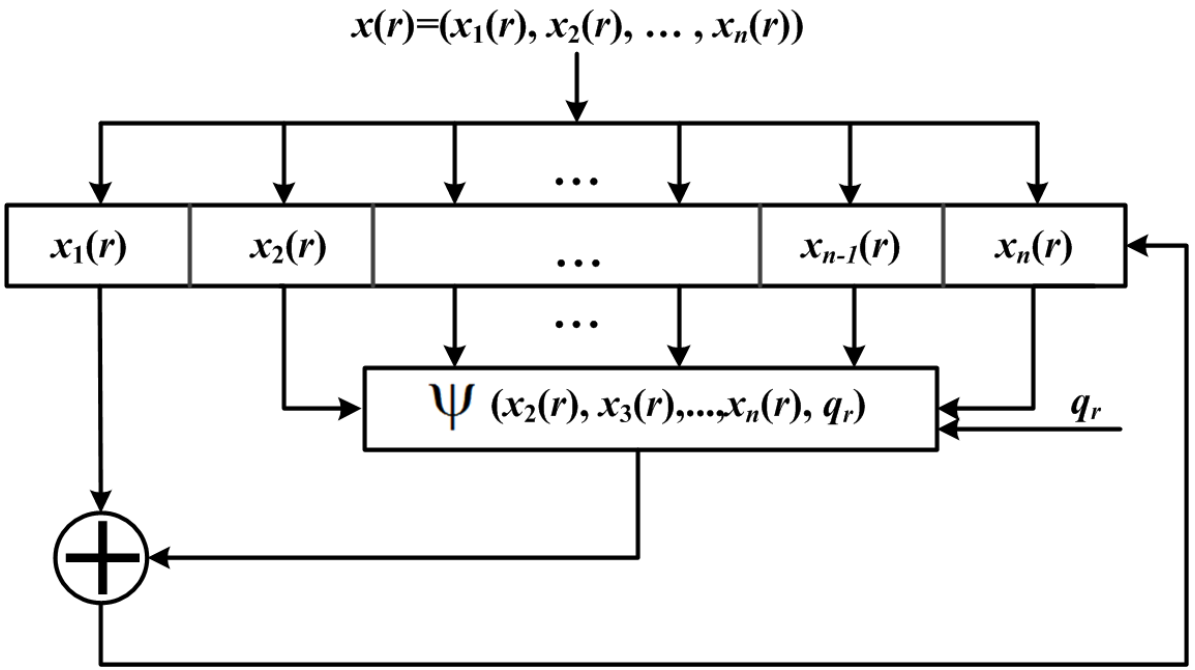


Рисунок – Схема функционирования СБШ

Преимущества:

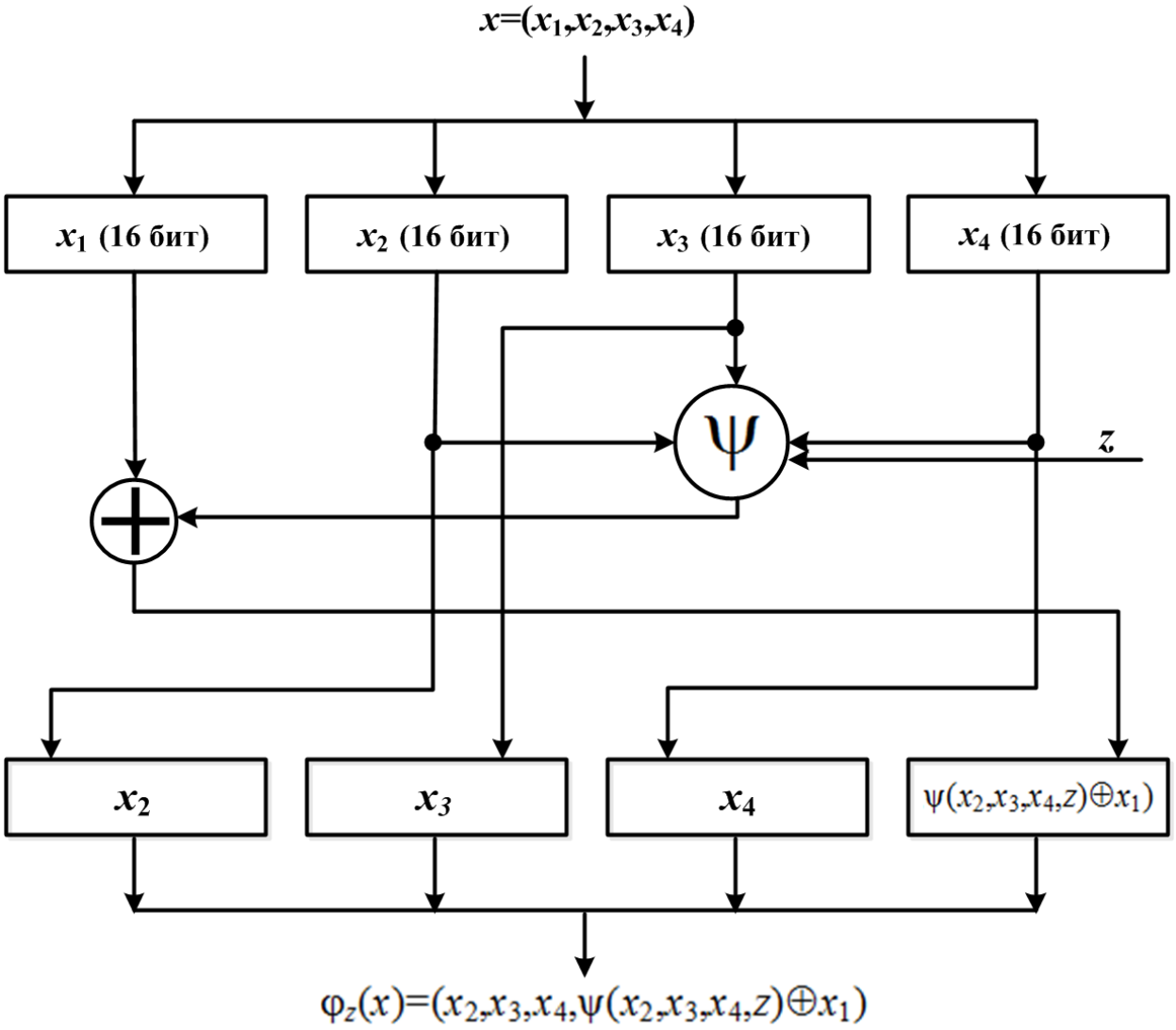
- Возможность увеличить размер входного блока данных без существенного усложнения реализации функций => увеличение производительности шифрования
- Больший выбор комбинаций базовых элементов для построения раундовой функции
- Сохранение хороших перемешивающих свойств

Инволютивность алгоритма шифрования

Подстановка f является инволюцией, если $f(f(x))=x$, для любого x.

Построен критерий инволютивности h-раундовых шифров, $h>1$, основанных на регистрах сдвига длины n, с функцией усложнения $\psi(y_2,\ldots,y_n,z)$, инвариантной относительно инволюции степени n-1.

Схема раундовой подстановки СБШ



Слои функции усложнения (инволютивного СБШ)

- Слой **расширения** 16-битового вектора $x_i(j)$ до 24-битового вектора

$$E(x_i(j)):V_{16}\rightarrow V_{24}$$

- Слой **подмешивания** $M(E(x_i(j)),z)$ 48-битового циклового ключа z путем *XOR*-суммирования. Цикловой ключ z разбивается на две части по 24 бита: $z=(z^1,z^2)$, где:

$$M(E(x_i(j)),z)=\{E(x_2(j))\ z^1,\ E(x_3(j))\ z^2,\ E(x_4(j))\ z^1\}$$

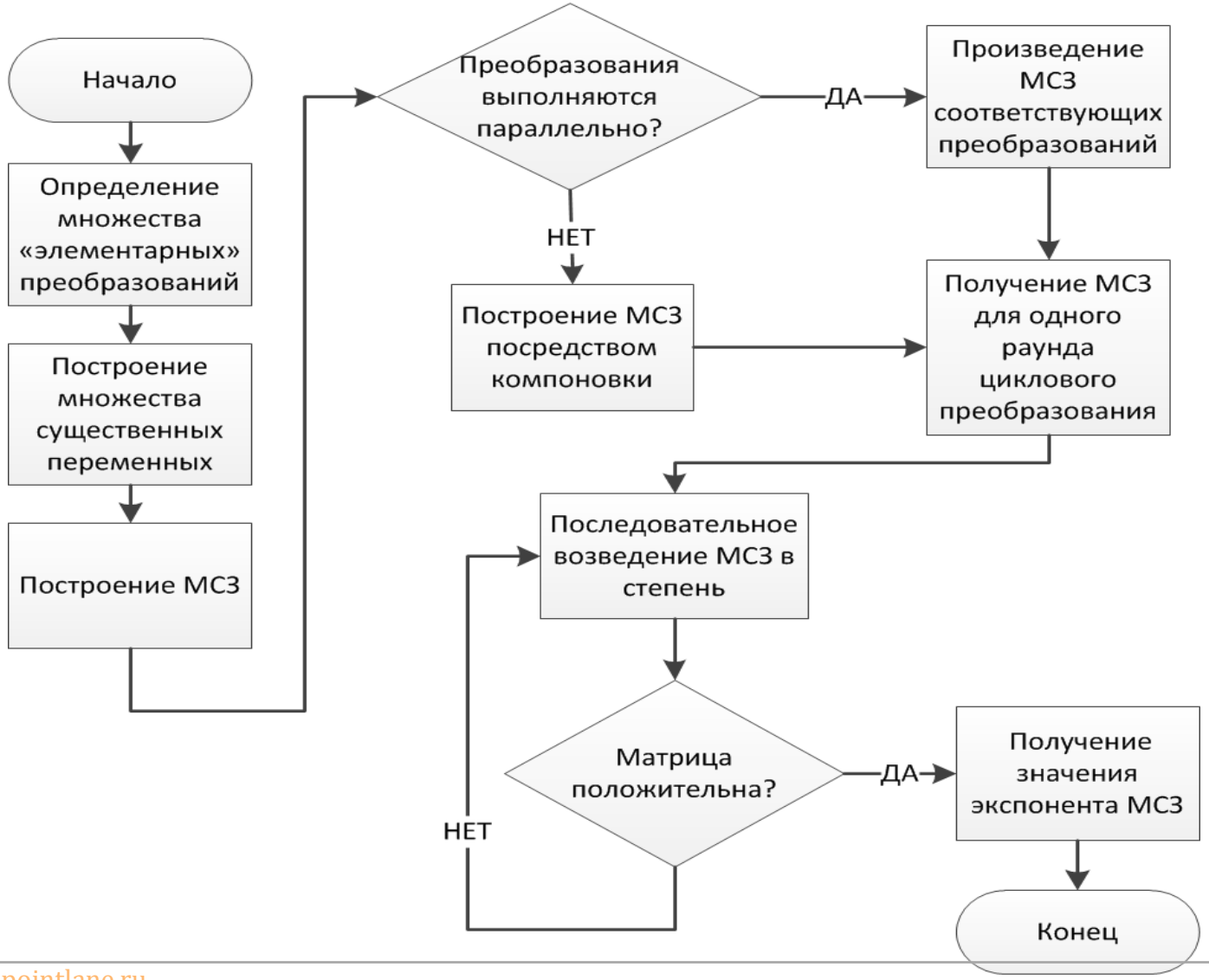
- Слой **нелинейной замены** $S(M(E(x_i(j)),z))$ 24-битового вектора на 16-битовый вектор с помощью s-блоков:

$$S_1(E(x_2(j))\ z^1),\ S_2(E(x_3(j))\ z^2),\ S_3(E(x_4(j))\ z^1)$$

- Слой **перемешивания координат** 16-битового вектора с помощью перестановки T^5 – циклического левого сдвига на 5:

$$T^5\ (a_1,a_2,\ldots,a_{16})=(a_6,\ldots,a_{16},a_1\ldots,a_5),\ \text{где}\ a_l\ –\ \text{один бит вектора.}$$

Получение оценки числа раундов шифрования

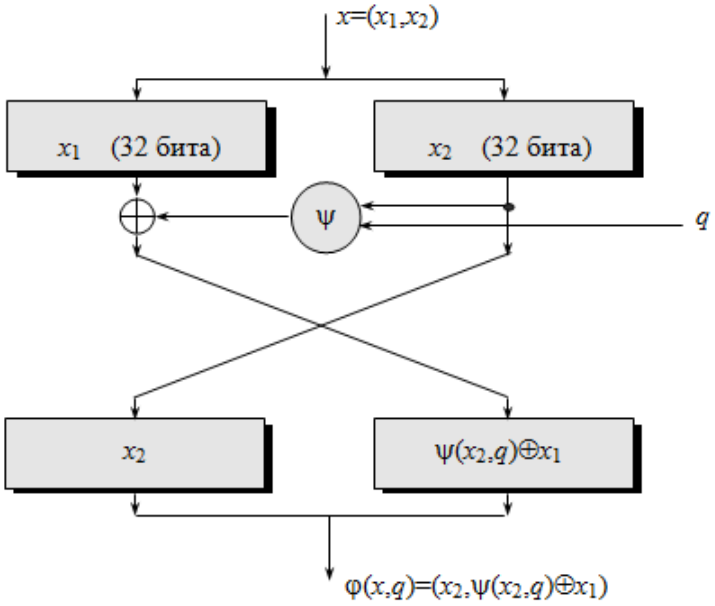


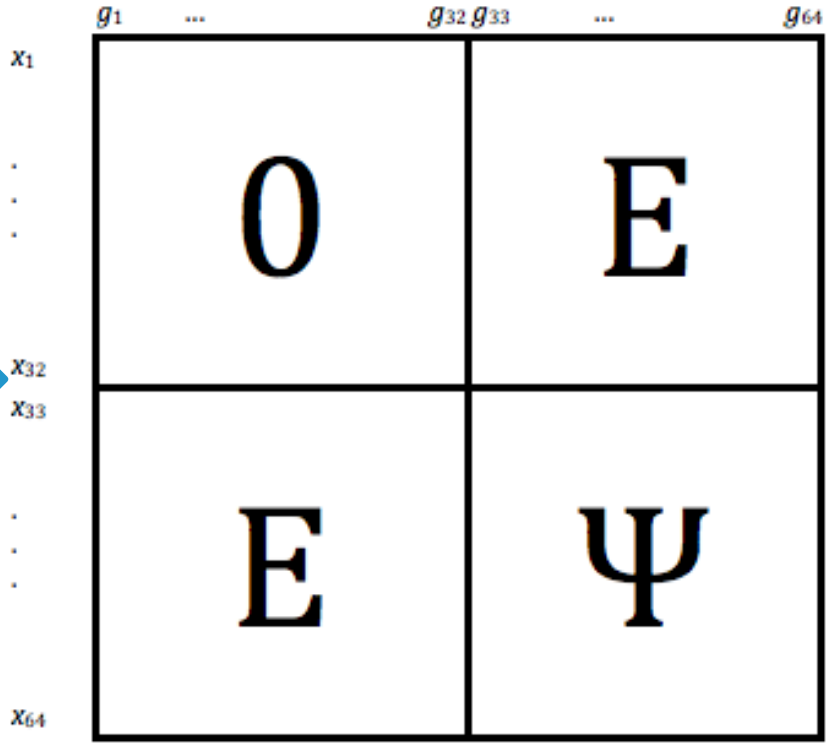
Пояснения к алгоритму оценки

1. $f(x)=h(g(x)) \Rightarrow$

$M_f \leq M_g * M_h$

2.





МСЗ раундовой подстановки СБШ

	$g_1 \dots g_{16}$	$g_{17} \dots g_{32}$	$g_{33} \dots g_{48}$	$g_{49} \dots g_{64}$
$x_1 \dots x_{16}$	0	0	0	E
$x_{17} \dots x_{32}$	E	0	0	Ψ_2
$x_{33} \dots x_{48}$	0	E	0	Ψ_3
$x_{49} \dots x_{64}$	0	0	E	Ψ_4

Подблоки, кодирующие СЗ (ψ2, ψ3, ψ4)

0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0
0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0
0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0
0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0
0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0
0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0
0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0
1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1
1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1
1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1
1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1
0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0
0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0
0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0
0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0

Минимальное число раундов шифрования

$n=4, r=16$

$h = 7$ (exp MC3)

Теоретические результаты работы

Для алгоритмов блочного шифрования, основанных на регистрах сдвига произвольной длины над множеством двоичных *r*-мерных векторов:

- построен критерий инволютивности.

Прикладные результаты работы

- построен пример блочного шифра на основе регистра сдвига длины 4, исследованы перемешивающие свойства его раундовой функции;

- на основе теоретико-графового подхода разработан алгоритм оценки наименьшего необходимого числа раундов шифрования для блочного шифра, использующего заданную раундовую подстановку.

Дальнейшее направление исследования

- Рассмотреть модельный пример алгоритма шифрования, основанного на регистре сдвига произвольной длины с обратной связью, представленной несколькими функциями;
- Исследовать криптографические свойства (инволютивность, биективность, перемешивающие свойства) таких моделей.

Спасибо за внимание!

e-mail: a.koreneva@pointlane.ru

Pointlane
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ