Ежегодная международная научно-практическая конференция
«РусКрипто’2020»

Построение атаки на основе инвариантных подпространств для XSL-алгоритмов блочного шифрования на основе 3D подхода

Коновалов Никита,
студент 2-го курса магистратуры НИЯУ «МИФИ»

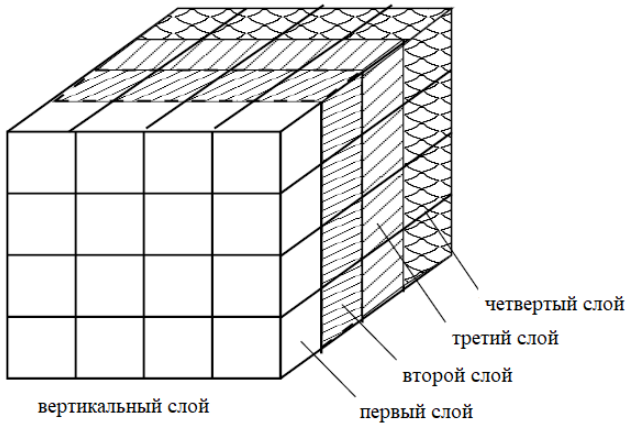
Квазиинволютивный XSL-алгоритм блочного шифрования «CUBE»

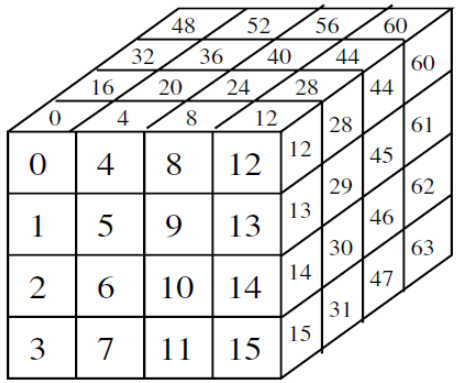
Трехмерное представление информационного блока:

$$a = (a_0, \dots, a_{64}), a_i \in GF(2), i \in \overline{0,63}$$

$$a^{(j)} = \{b_j \mid b \in GF(2^{16})\}, j \in (0,1,2,3)$$

$$\left(\begin{array}{cccc|cccc|cccc|cccc} a_0 & a_4 & a_8 & a_{12} & a_{16} & a_{20} & a_{24} & a_{28} & a_{32} & a_{36} & a_{40} & a_{44} & a_{48} & a_{52} & a_{56} & a_{60} \\ a_1 & a_5 & a_9 & a_{13} & a_{17} & a_{21} & a_{25} & a_{29} & a_{33} & a_{37} & a_{41} & a_{45} & a_{49} & a_{53} & a_{57} & a_{61} \\ a_2 & a_6 & a_{10} & a_{14} & a_{18} & a_{22} & a_{26} & a_{30} & a_{34} & a_{38} & a_{42} & a_{46} & a_{50} & a_{54} & a_{58} & a_{62} \\ a_3 & a_7 & a_{11} & a_{15} & a_{19} & a_{23} & a_{27} & a_{31} & a_{35} & a_{39} & a_{43} & a_{47} & a_{51} & a_{55} & a_{59} & a_{63} \end{array}\right)$$





Квазиинволютивный XSL-алгоритм блочного шифрования «CUBE»

Раундовая функция алгоритма шифрования CUBE

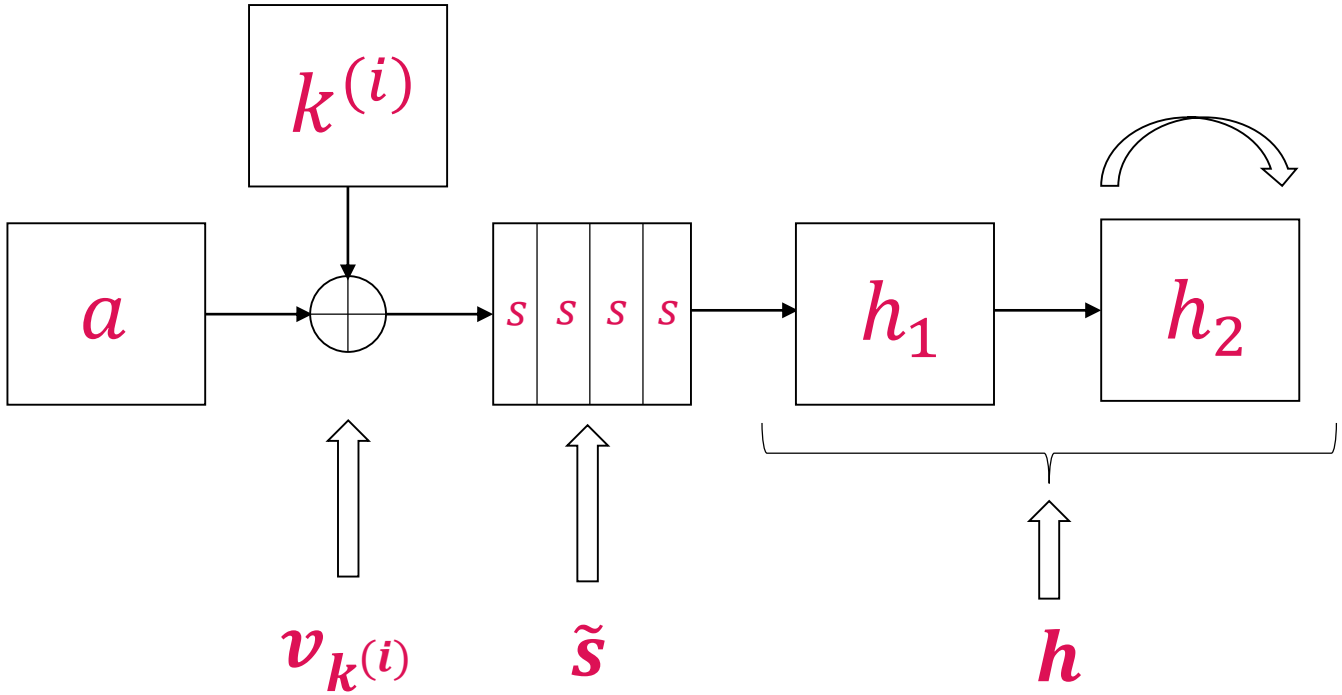
- Пусть V_n – n-мерное векторное пространство над полем $GF(2)$.
- Для преобразования $b: V_n \to V_n$ положим $a^b = b(a)$ для каждого $a \in V_n$.

$$g_{k^{(i)}}: a \mapsto (a \oplus k^{(i)})^{\tilde{s}h}$$

где $k^{(i)}$ – 64-битный раундовый ключ i-го раунда, $i \in \mathbb{N}$.

- Функция шифрования для r раундов:

$$g_{k^{(0)},k^{(1)},\dots,k^{(r-1)}} = v_{k^{(0)}} \tilde{s} h \dots v_{k^{(r-1)}}$$



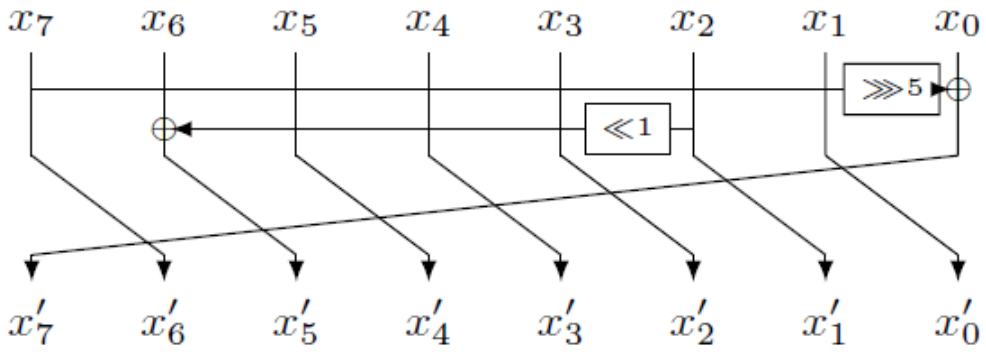
Квазиинволютивный XSL-алгоритм блочного шифрования «CUBE»

Алгоритм развертывания раундовых ключей

$$\boldsymbol{K = k^{(1)} \,||\, k^{(0)}},$$
$$\boldsymbol{k^{(i+2)} = \left(k^{(i+1)} * A\right) \oplus k^{(i)} \oplus (i+2)},$$

где $A = B^3$, $i \in \overline{0,15}$.

$$B = \begin{pmatrix} 0 & I & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & I & 0 & 0 \\ 0 & 0 & \ll 1 & 0 & 0 & 0 & I & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & I \\ I & 0 & 0 & 0 & 0 & 0 & 0 & \gg 5 \end{pmatrix}$$



- Умножение вектора на матрицу ($k^{(i)} * A$) аналогично трем итерациям работы схемы, $k^{(i)} = \{(x_0, \dots, x_7) \mid x_j \in GF(2^8)\}$.

Квазиинволютивный XSL-алгоритм блочного шифрования «CUBE»

Нелинейное преобразование $\tilde{s}$

- Нелинейное преобразование $\tilde{s}$ инволютивно $(\tilde{s}^2 = e)$, реализовано путем применения к координатам вектора a подстановки $s \in S(GF(2^4))$:

$$\tilde{s}: (a_0, \dots, a_{15}) \mapsto (a_0^s, \dots, a_{15}^s),$$

где $a = (a_0, \dots, a_{15}), a_i \in GF(2^4)$.

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	7	A	2	C	4	8	F	0	5	9	1	E	3	D	B	6

Квазиинволютивный XSL-алгоритм блочного шифрования «CUBE»

Линейное преобразование h_1

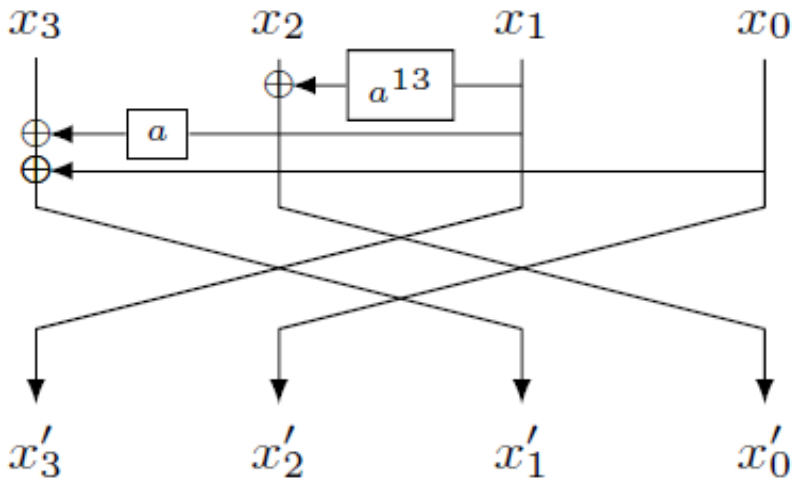
- Линейное преобразование h_1 базируется на применении максимально рассеивающих матриц (MDS) M_a и $M_{a^{13}}$ и реализовано в виде четырех итераций схемы (справа):

$$h_1 : a_i \mapsto a_i^{h_1},$$

где $a = (a_0, \dots, a_3), a_i \in GF(2^{16}), a_i = \{(x_0, \dots, x_3) \mid x_j \in GF(2^4)\}$.

- Блоки $[a]$ и $[a^{13}]$ обозначают умножение вектора x_j на матрицы M_a и $M_{a^{13}}$ соответственно.

$$M_{a^{13}} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \qquad M_a = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

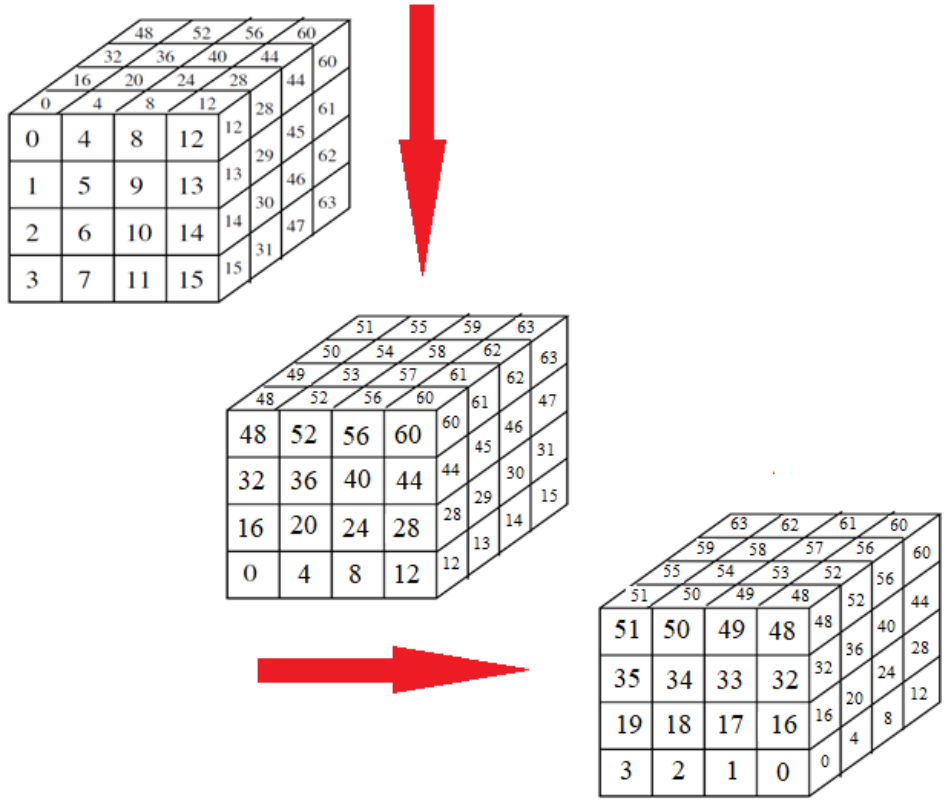


Квазиинволютивный XSL-алгоритм блочного шифрования «CUBE»

Линейное преобразование h_2

- Линейное преобразование h_2 реализовано перестановкой над вектором a, визуализировано в виде вращения куба «на себя» и «вправо»:

$$h_2 : a \mapsto a^{h_2}.$$



Построение атаки на основе инвариантных подпространств на редуцированный алгоритм «CUBE»

Множество собственных значений преобразования h_2

- Преобразование h_2 в виде подстановки u над множеством элементов вектора a:

$$u = \begin{pmatrix} a_0 \dots a_{63} \\ a_{15} \dots a_{48} \end{pmatrix}.$$

- Циклическое строение u: $(a_0, a_{15}, a_{51})(a_1, a_{11}, a_{35})(a_2, a_7, a_{19})(a_4, a_{31}, a_{50}) \dots (a_3)(a_{22})(a_{41})(a_{60})$,

20 циклов по 3 элемента и 4 цикла по 1 элементу.

$2^{(20+4)} = 2^{24}$ векторов для множества собственных значений относительно линейного преобразования h_2.

Построение атаки на основе инвариантных подпространств на редуцированный алгоритм «CUBE»

Инвариантное подпространство линейного преобразования $\mathbf{h_2}$

- Множество W, $W \subset V_n$, назовём инвариантным относительно линейного преобразования h_2, если $W^{h_2} = W$.

  Тогда существует 7-мерное инвариантное подпространство для преобразования h_2:

$$\boldsymbol{W = \{(abc)(abc)(abc) \dots (d)(e)(f)(g) \mid a, b, c, d, e, f, g \in GF(2)\},}$$

$$\boldsymbol{W = \{aaadaaabaaabaaabcccc \dots gbbb \mid a, b, c, d, e, f, g \in GF(2)\}.}$$

$$\boldsymbol{W = \begin{pmatrix} a\,a\,a\,a & c\,a\,a\,a & c\,c\,a\,a & c\,c\,c\,g \\ a\,a\,a\,a & c\,a\,a\,a & c\,c\,f\,b & c\,c\,c\,b \\ a\,a\,a\,a & c\,e\,b\,b & c\,c\,b\,b & c\,c\,b\,b \\ d\,b\,b\,b & c\,b\,b\,b & c\,b\,b\,b & c\,b\,b\,b \end{pmatrix}}$$

Построение атаки на основе инвариантных подпространств на редуцированный алгоритм «CUBE»

- Композиция $\tilde{s}h_1$ переводит W в смежный класс $W \oplus \theta$, $W^{h_2} = W$. Если $k^{(i)} \epsilon\, W \oplus \theta$, то справедливо:

$$(\boldsymbol{W})^{\boldsymbol{v}_{k^{(i)}}\tilde{\boldsymbol{s}}\boldsymbol{h}} = \boldsymbol{W}.$$

- **Утверждение 1.** *Существуют* $k^{(0)}$ *и* $k^{(1)}$ *такие, что* $k^{(0)}, k^{(1)} \epsilon\, W \oplus \theta$ *и справедливо равенство:*

$$(\boldsymbol{W})^{\boldsymbol{v}_{k^{(0)}}\tilde{\boldsymbol{s}}\boldsymbol{h}\boldsymbol{v}_{k^{(1)}}\tilde{\boldsymbol{s}}\boldsymbol{h}} = \boldsymbol{W}.$$

- Тогда трехраундовая версия алгоритма подвержена атаке [3] по инвариантным подпространствам, а класс ключей $K = k^{(1)}||k^{(0)}$ будет «потенциально слабым».
- Все блоки открытого текста, принадлежащие W через 2 раунда переходят только в блоки из множества W, а после 3 раунда (отбеливание) переходят в $\theta \oplus (\boldsymbol{W} \oplus \theta) * \boldsymbol{A} \oplus \mathrm{c}_2$:

$$(\boldsymbol{W})^{\boldsymbol{v}_{k^{(0)}}\tilde{\boldsymbol{s}}\boldsymbol{h}\boldsymbol{v}_{k^{(1)}}\tilde{\boldsymbol{s}}\boldsymbol{h}\boldsymbol{v}_{k^{(2)}}} = \theta \oplus (\boldsymbol{W} \oplus \theta) * \boldsymbol{A} \oplus \mathrm{c}_2.$$

Построение атаки на основе инвариантных подпространств на редуцированный алгоритм «CUBE»

- Из алгоритма развертывания раундовых ключей следует существование $|W|^2$ возможных значений $k^{(0)}$ и $k^{(1)}$ таких, что $k^{(1)}, k^{(2)} \epsilon\ W \oplus \Theta$.
- Так как $\boldsymbol{k^{(2)} = k^{(1)} * A \oplus k^{(0)} \oplus c_2}$, $k^{(1)}, k^{(2)} \epsilon\ W \oplus \Theta$, то $\boldsymbol{k^{(0)} \epsilon\ \Theta \oplus (W \oplus \Theta) * A \oplus c_2}$, а $\boldsymbol{k^{(3)} \epsilon\ W \oplus \Theta \oplus (W \oplus \Theta) * A \oplus c_3}$, где c - константа.
- Отсюда следует, что все блоки открытого текста из класса $\boldsymbol{W \oplus (W \oplus \Theta) * A \oplus c_2}$ через 3 раунда переходят только в блоки из множества W, а после 4 раунда (отбеливание) переходят в $\boldsymbol{\Theta \oplus (W \oplus \Theta) * A \oplus c_3}$:

- $\boldsymbol{(W \oplus (W \oplus \Theta) * A \oplus c_2)^{v_{k^{(0)}} \tilde{s} h} = W}$;
- $\boldsymbol{(W)^{v_{k^{(1)}} \tilde{s} h v_{k^{(2)}} \tilde{s} h} = W}$;
- $\boldsymbol{(W)^{v_{k^{(3)}}} = \Theta \oplus (W \oplus \Theta) * A \oplus c_3}$.

$$\boldsymbol{(W \oplus (W \oplus \Theta) * A \oplus c_2)^{v_{k^{(0)}} \tilde{s} h v_{k^{(1)}} \tilde{s} h v_{k^{(2)}} \tilde{s} h v_{k^{(3)}}} = \Theta \oplus (W \oplus \Theta) * A \oplus c_3}$$

Построение атаки на основе инвариантных подпространств на редуцированный алгоритм «CUBE»

- В ходе исследования был предложен алгоритм идентификации слабых ключей на редуцированный алгоритм «CUBE» в 4 раунда:

Вход: *Множество* $\boldsymbol{B} = \left(\boldsymbol{a}^{\boldsymbol{g}_{k^{(0)},\dots,k^{(3)}}} \mid \boldsymbol{a} \boldsymbol{\epsilon} \boldsymbol{W} \oplus (\boldsymbol{W} \oplus \Theta) * \boldsymbol{A} \oplus \mathrm{c}_{\boldsymbol{2}}\right)$.

Выход: *информация о принадлежности ключа* K *к классу слабых ключей.*

- *Для фиксированного* b_i *опробовать* $(\boldsymbol{b_i} \oplus \boldsymbol{k^{(3)}})$, $k^{(3)} \epsilon\, \Theta \oplus (W \oplus \Theta) * A \oplus \mathrm{c}_3$.
- *Для опробуемого* $(\boldsymbol{b_i} \oplus \boldsymbol{k^{(3)}})$ *проверить:*

$$(\boldsymbol{b_i} \oplus \boldsymbol{k^{(3)}}) \boldsymbol{\epsilon} \boldsymbol{W}.$$

- *Если* $(\boldsymbol{b_i} \oplus \boldsymbol{k^{(3)}})$ *не принадлежит множеству* W, *то ключ К не является слабым.*

- Таким образом, трудоемкость алгоритма можно оценить как $|W|^2$ операций сложения по модулю 2, число слабых ключей $|W|^2$.

Построение атаки на основе инвариантных подпространств на редуцированный алгоритм «CUBE»

Практическая реализация атаки

```
efff0dff01ff013f
efff0dff01ff0137
efff0dff01bf013f
efff0dff01bf0137
effffdffffffffff
effffdffffffffff7
effffdffffbfffff
effffdffffbffff7
effffffffffffff
effffffffffffff7
effffffffbfffff
effffffffbffff7
efff0fff01ff013f
efff0fff01ff0137
efff0fff01bf013f
efff0fff01bf0137
0000f000fe40fec8
0000f000fe40fec0
0000f000fe00fec8
0000f000fe00fec0
0000000000400008
0000000000400000
0000000000000008
0000000000000000
0000f200fe40fec8
0000f200fe40fec0
0000f200fe00fec8
0000f200fe00fec0
0000020000400008
0000020000400000
0000020000000008
0000020000000000
```

```
ffff0dff01ff0137
ffff0dff01bf013f
ffff0dff01bf0137
ffffffffffffffff
ffffffffffffffff7
ffffffffffbfffff
ffffffffffbffff7
ffffffffffffffff
ffffffffffffffff7
fffffffffbfffff
fffffffffbffff7
ffff0fff01ff013f
ffff0fff01ff0137
ffff0fff01bf013f
ffff0fff01bf0137
1111f133ff77ffff
1111f133ff77fff7
1111f133ff37ffff
1111f133ff37fff7
111103330177013f
1111033301770137
111103330137013f
1111033301370137
111101330177013f
1111013301770137
111101330137013f
1111013301370137
1111f333ff77ffff
1111f333ff77fff7
1111f333ff37ffff
1111f333ff37fff7
```

```
ubuntu@ubuntunikita:~/Загрузки$ ./cube
Открытый текст: ecc5d15635c0a123
K0: aa0ee3092a3c9ac0
1-й раунд: 0111f133ff77ffff

K1: f41af5f5d5c56230
2-й раунд: eeeefcccfec8fec8

K2: 6f6cd3fd30c96f17
3-й раунд: 0000f200fe40fec8

K3: 3d75e29ab9169f03
```

После каждого из трех раундов информационный блок принадлежи множеству W.

```
eeee0ecc00c80008
eeee0ecc00c80000
eeee0ecc00880008
eeee0ecc00880000
eeeefcccfec8fec8
eeeefcccfec8fec0
eeeefcccfe88fec8
eeeefcccfe88fec0
eeeefeccfec8fec8
eeeefeccfec8fec0
eeeefeccfe88fec8
eeeefeccfe88fec0
eeee0ccc00c80008
eeee0ccc00c80000
eeee0ccc00880008
eeee0ccc00880000
1000f000fe40fec8
1000f000fe40fec0
1000f000fe00fec8
1000f000fe00fec0
1000000000400008
1000000000400000
1000000000000008
1000000000000000
1000f200fe40fec8
1000f200fe40fec0
1000f200fe00fec8
1000f200fe00fec0
1000020000400008
1000020000400000
1000020000000008
1000020000000000
```

```
0111f133ff77ffff
0111f133ff77fff7
0111f133ff37ffff
0111f133ff37fff7
011103330177013f
0111033301770137
011103330137013f
0111033301370137
011101330177013f
0111013301770137
011101330137013f
0111013301370137
0111f333ff77ffff
0111f333ff77fff7
0111f333ff37ffff
0111f333ff37fff7
feee0ecc00c80008
feee0ecc00c80000
feee0ecc00880008
feee0ecc00880000
feeefcccfec8fec8
feeefcccfec8fec0
feeefcccfe88fec8
feeefcccfe88fec0
feeefeccfec8fec8
feeefeccfec8fec0
feeefeccfe88fec8
feeefeccfe88fec0
feee0ccc00c80008
feee0ccc00c80000
feee0ccc00880008
feee0ccc00880000
```

Результаты работы

- Исследовано линейное преобразование алгоритма блочного шифрования на основе 3D подхода «CUBE» с 64-битным информационным блоком. Найдено инвариантное подпространство W, $|W| = 2^7$.

- На основе найденого инвариантного подпространства построена атака на 4-х раундовую версию алгоритма, обнаружен класс потенциально слабых ключей K, $|K| = |W|^2$.

- Предложен алгоритм идентификации слабых ключей для фиксированных пар открытый текст – шифртекст, трудоемкость алгоритма 2^{14} операций сложения по модулю 2. Алгоритм эффективнее опробования ключей из класса слабых.

- Программно реализован алгоритм шифрования «CUBE», а также его 4-х раундовая версия. На практике проверен алгоритм идентификации слабых ключей. Все промежуточные значения информационного блока принадлежат множеству W.

Спасибо за внимание!

Контактная информация

Электронная почта:

nikitakonovalov2013@yandex.ru

Телефон:

+7-987-555-14-97

1. Berger T.P., Francq J., Minier M. (2015) CUBE Cipher: A Family of Quasi-Involutive Block Ciphers Easy to Mask. In: El Hajji S., Nitaj A., Carlet C., Souidi E. (eds) Codes, Cryptology, and Information Security. C2SI 2015 Lecture Notes in Computer Science, vol 9084 Springer, Cham.
2. Nakahara Jr. J. 3D: a three-dimensional block cipher / Jr. J. Nakahara // CANS 2008 Lect. Notes Comp. Sei. - 2008 - V. 5339 - P. 252-267
3. D. A. Burov, B. A. Pogorelov, “An attack on 6 rounds of Khazad”, Матем. вопр. криптогр., 7:2 (2016), 35–46