О невозможных дифференциалах алгоритма шифрования Zodiac

А. В. Котов

Руководитель: М. А. Пудовкина

Московский инженерно-физический институт

15 января 2009 г.

План доклада

Введение

Данная работа основана на материале, изложенном в статье "Impossible Differential Cryptanalysis of Zodiac"(1). В статье (1) приведено несколько невозможных дифференциалов, но не упомянут алгоритм поиска дифференциалов.
В настоящей работе формализованы некоторые понятия, введенные в (1), приведен быстрый алгоритм перечисления дифференциалов заданной длины и выписаны наиболее эффективные для атаки невозможные дифференциалы.

Основные обозначения

Обозначения

V_n — линейное пространство размерности n,

$$V_n = E_2^{(n)}, E_2 = \{0, 1\}.$$

Основные обозначения

Обозначения

V_n — линейное пространство размерности n,

$$V_n = E_2^{(n)}, E_2 = \{0, 1\}.$$

$c^{(i)}$ — шифртекст после i раундов $(i = \overline{0, 16})$,

$$c^{(i)} = (c_1^{(i)}, c_2^{(i)}), \text{ где } c_t^{(i)} = (c_{t,0}^{(i)}, c_{t,1}^{(i)}, \dots c_{t,7}^{(i)}),$$

$$c_{t,j}^{(i)} \in V_8, \ t = \overline{1, 2}, \ j = \overline{0, 7}.$$

$c_1^{(i)}$ и $c_2^{(i)}$ — левая и правая части текста соответственно.

Основные обозначения

Обозначения

V_n — линейное пространство размерности n,

$$V_n = E_2^{(n)}, E_2 = \{0, 1\}.$$

$c^{(i)}$ — шифртекст после i раундов $(i = \overline{0, 16})$,

$$c^{(i)} = (c_1^{(i)}, c_2^{(i)}), \text{ где } c_t^{(i)} = (c_{t,0}^{(i)}, c_{t,1}^{(i)}, \dots c_{t,7}^{(i)}),$$

$$c_{t,j}^{(i)} \in V_8, \ t = \overline{1, 2}, \ j = \overline{0, 7}.$$

$c_1^{(i)}$ и $c_2^{(i)}$ — левая и правая части текста соответственно.
Тогда $c^{(0)}$ — открытый текст, $c^{(16)}$ — шифртекст.

Понятие дифференциала

Определение

Пусть $(c_1^{(0)}, c_2^{(0)})$ и $(\widetilde{c}_1^{(0)}, \widetilde{c}_2^{(0)})$ — произвольная пара открытых текстов. Тогда

$$\alpha^{(i)} = (\alpha_1^{(i)}, \alpha_2^{(i)}) = (c_1^{(i-1)} \oplus \widetilde{c}_1^{(i-1)}, c_2^{(i-1)} \oplus \widetilde{c}_2^{(i-1)}) -$$

входной дифференциал i-го раунда для пары открытых текстов $c^{(0)}$ и $\widetilde{c}^{(0)}$.

Понятие дифференциала

Определение

Пусть $(c_1^{(0)}, c_2^{(0)})$ и $(\widetilde{c}_1^{(0)}, \widetilde{c}_2^{(0)})$ — произвольная пара открытых текстов. Тогда

$$\alpha^{(i)} = (\alpha_1^{(i)}, \alpha_2^{(i)}) = (c_1^{(i-1)} \oplus \widetilde{c}_1^{(i-1)}, c_2^{(i-1)} \oplus \widetilde{c}_2^{(i-1)}) -$$

входной дифференциал i-го раунда для пары открытых текстов $c^{(0)}$ и $\widetilde{c}^{(0)}$.

$$\beta^{(i)} = (\beta_1^{(i)}, \beta_2^{(i)}) = (c_1^{(i)} \oplus \widetilde{c}_1^{(i)}, c_2^{(i)} \oplus \widetilde{c}_2^{(i)}) = (\alpha_1^{(i+1)}, \alpha_2^{(i+1)}) -$$

выходной дифференциал i-го раунда для пары открытых текстов $c^{(0)}$ и $\widetilde{c}^{(0)}$.

Входным дифференциалом будем называть входной дифференциал 1-го раунда.

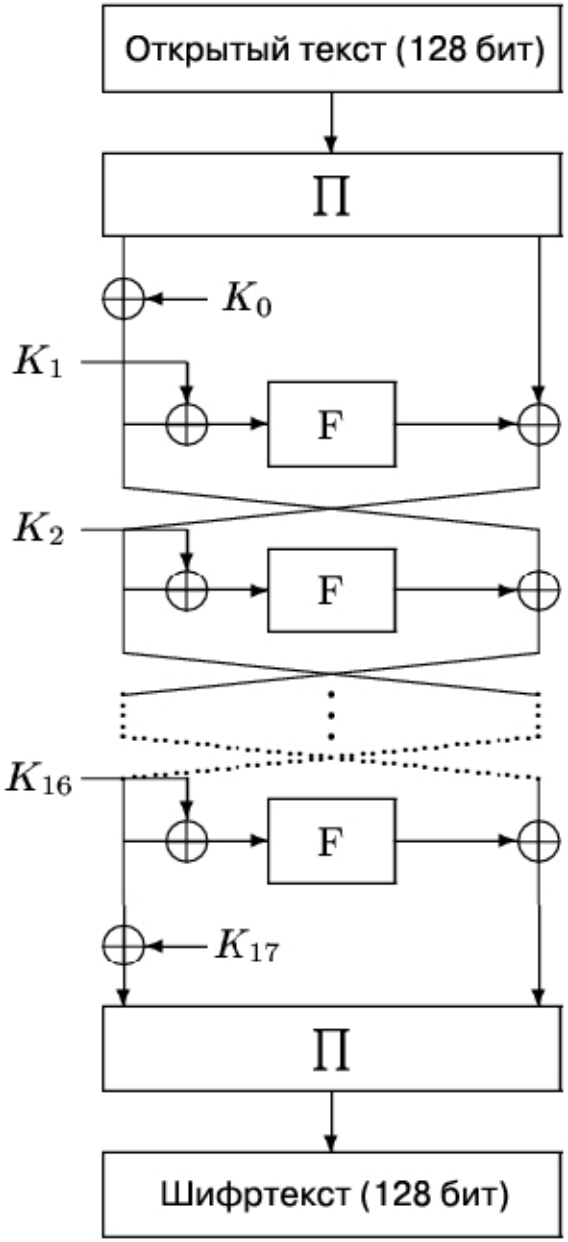


Рис.: Структура алгоритма Zodiac

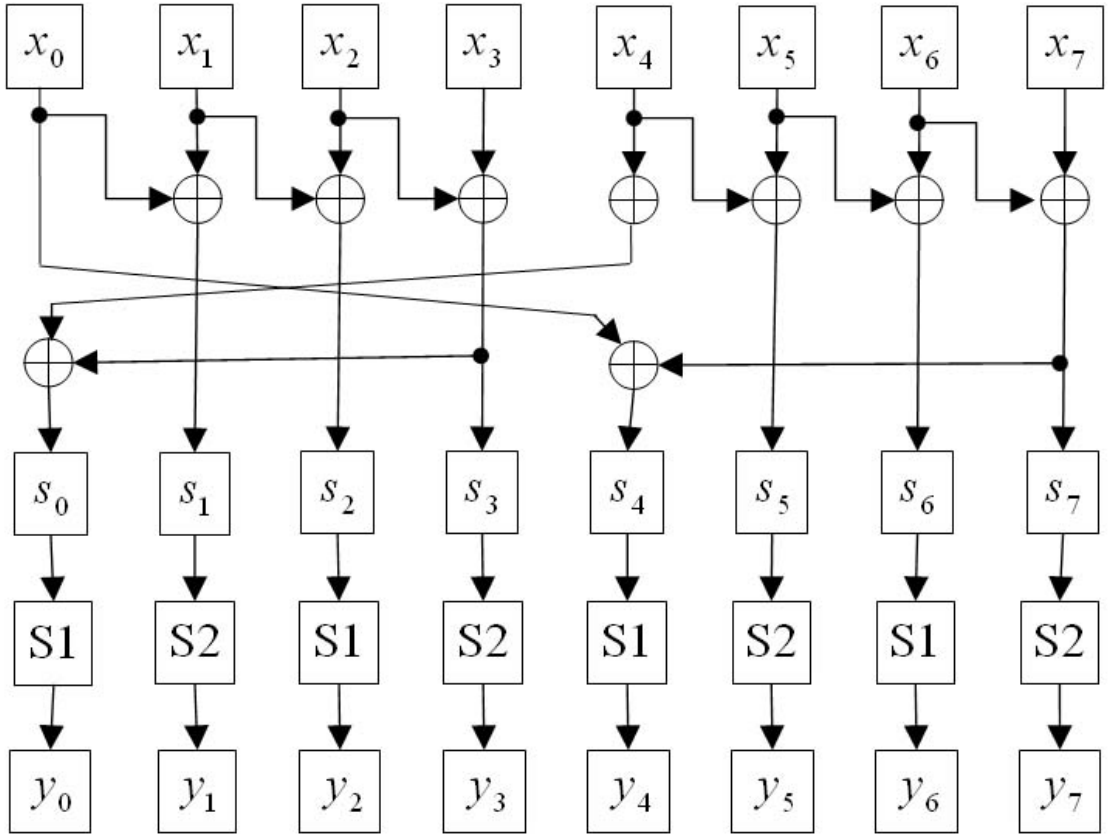


Рис.: Цикловая функция F

На схеме $x_j, s_j, y_j \in V_8$, $j = \overline{0,7}$. s-Блоки $s1$ и $s2$ — некоторые нелинейные подстановки на V_8.

Определение

Пусть $\alpha^{(1)} = (\alpha_1^{(1)}, \alpha_2^{(1)})$ — фиксированный входной дифференциал. Распишем $\alpha^{(i)}$ следующим образом:

$$\alpha^{(i)} = (\alpha_1^{(i)}, \alpha_2^{(i)}),\ \alpha_t^{(i)} = (x_{t,0}^{(i)}, x_{t,1}^{(i)}, \ldots, x_{t,7}^{(i)}),\ x_{t,j}^{(i)} \in V_8,$$

$$t = \overline{1,2},\ j = \overline{0,7},\ i = \overline{1,16}.$$

Определение

Пусть $\alpha^{(1)} = (\alpha_1^{(1)}, \alpha_2^{(1)})$ — фиксированный входной дифференциал. Распишем $\alpha^{(i)}$ следующим образом:

$$\alpha^{(i)} = (\alpha_1^{(i)}, \alpha_2^{(i)}),\ \alpha_t^{(i)} = (x_{t,0}^{(i)}, x_{t,1}^{(i)}, \ldots, x_{t,7}^{(i)}),\ x_{t,j}^{(i)} \in V_8,$$

$$t = \overline{1,2},\ j = \overline{0,7},\ i = \overline{1,16}.$$

Будем говорить, что элемент $x_{t,j}^{(i)}$ является определенным, если для случайно выбранной пары открытых текстов $c^{(0)}$ и $\widetilde{c}^{(0)}$, которой соответствует дифференциал $\alpha^{(1)}$, выполняется

$$\mathsf{P}\{x_{t,j}^{(i)} = 0\} = 1 \text{ или } \mathsf{P}\{x_{t,j}^{(i)} \in V_8^*\} = 1,\ V_8^* = V_8 \backslash \{0\}.$$

Определение

Пусть $\alpha^{(1)} = (\alpha_1^{(1)}, \alpha_2^{(1)})$ — фиксированный входной дифференциал. Распишем $\alpha^{(i)}$ следующим образом:

$$\alpha^{(i)} = (\alpha_1^{(i)}, \alpha_2^{(i)}),\ \alpha_t^{(i)} = (x_{t,0}^{(i)}, x_{t,1}^{(i)}, \ldots, x_{t,7}^{(i)}),\ x_{t,j}^{(i)} \in V_8,$$

$$t = \overline{1,2},\ j = \overline{0,7},\ i = \overline{1,16}.$$

Будем говорить, что элемент $x_{t,j}^{(i)}$ является определенным, если для случайно выбранной пары открытых текстов $c^{(0)}$ и $\widetilde{c}^{(0)}$, которой соответствует дифференциал $\alpha^{(1)}$, выполняется

$$\mathsf{P}\{x_{t,j}^{(i)} = 0\} = 1 \text{ или } \mathsf{P}\{x_{t,j}^{(i)} \in V_8^*\} = 1,\ V_8^* = V_8 \backslash \{0\}.$$

В противном случае, если

$$\mathsf{P}\{x_{t,j}^{(i)} = 0\} < 1 \text{ и } \mathsf{P}\{x_{t,j}^{(i)} \in V_8^*\} < 1,$$

то будем говорить, что элемент $x_{t,j}^{(i)}$ является неопределенным.

Обозначения

$a^*_m \in V^*_8$ — определенный ненулевой элемент, $m = 1, 2, \ldots$

$a_p \in V_8$ — неопределенный элемент, $p = 1, 2, \ldots$

Вместо определенного нулевого элемента будем писать 0.

Обозначения

$a^*_m \in V^*_8$ — определенный ненулевой элемент, $m = 1, 2, \ldots$
$a_p \in V_8$ — неопределенный элемент, $p = 1, 2, \ldots$
Вместо определенного нулевого элемента будем писать 0.

Преобразования элементов

Пусть s — подстановка на V_8. Зафиксируем некоторое множество $B \subseteq V_8$. Найдем минимальное $B' \subseteq V_8$, такое что для случайно выбранного $b \in B$ и случайно выбранного элемента текста $c \in V_8$

$$\mathrm{P}\{s(b \oplus c) \oplus s(c) \in B'\} = 1.$$

Обозначения

$a^*_m \in V_8^*$ — определенный ненулевой элемент, $m = 1, 2, \ldots$
$a_p \in V_8$ — неопределенный элемент, $p = 1, 2, \ldots$
Вместо определенного нулевого элемента будем писать 0.

Преобразования элементов

Пусть s — подстановка на V_8. Зафиксируем некоторое множество $B \subseteq V_8$. Найдем минимальное $B' \subseteq V_8$, такое что для случайно выбранного $b \in B$ и случайно выбранного элемента текста $c \in V_8$

$$\mathrm{P}\{s(b \oplus c) \oplus s(c) \in B'\} = 1.$$

Будем писать $b \xrightarrow{s} b'$, $b' \in B'$

Обозначения

$a^*_m \in V^*_8$ — определенный ненулевой элемент, $m = 1, 2, \ldots$
$a_p \in V_8$ — неопределенный элемент, $p = 1, 2, \ldots$
Вместо определенного нулевого элемента будем писать 0.

Преобразования элементов

Пусть s — подстановка на V_8. Зафиксируем некоторое множество $B \subseteq V_8$. Найдем минимальное $B' \subseteq V_8$, такое что для случайно выбранного $b \in B$ и случайно выбранного элемента текста $c \in V_8$

$$\mathrm{P}\{s(b \oplus c) \oplus s(c) \in B'\} = 1.$$

Будем писать $b \xrightarrow{s} b'$, $b' \in B'$
Пусть $a \in V_8$, $a^* \in V^*_8$. Тогда

$$0 \xrightarrow{s1} 0,\ a^* \xrightarrow{s1} \widetilde{a}^*,\ a \xrightarrow{s1} \widetilde{a},\ \text{где } \widetilde{a}^* \in V^*_8,\ \widetilde{a} \in V_8$$

$$0 \xrightarrow{s2} 0,\ a^* \xrightarrow{s2} \widehat{a}^*,\ a \xrightarrow{s2} \widehat{a},\ \text{где } \widehat{a}^* \in V^*_8,\ \widehat{a} \in V_8$$

Пример дифференциала

i	$\alpha_1^{(i)}$								$\alpha_2^{(i)}$							
1	0	a_1^*	a_2^*	0	0	0	0	0	0	a_3^*	0	0	0	0	0	0
2	a_4^*	a_1	a_2	a_5^*	0	0	0	0	0	a_1^*	a_2^*	0	0	0	0	0
3	a_3	a_4	a_5	a_6	a_6^*	0	0	0	a_4^*	a_1	a_2	a_5^*	0	0	0	0
4	a_7	a_8	a_9	a_{10}	a_{11}	a_7^*	0	0	a_3	a_4	a_5	a_6	a_6^*	0	0	0
5	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}	a_{17}	a_8^*	0	a_7	a_8	a_9	a_{10}	a_{11}	a_7^*	0	0
6	a_{18}	a_{19}	a_{20}	a_{21}	a_{22}	a_{23}	a_{24}	a_9^*	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}	a_{17}	a_8^*	0
7	a_{25}	a_{26}	a_{27}	a_{28}	a_{29}	a_{30}	a_{31}	a_{32}	a_{18}	a_{19}	a_{20}	a_{21}	a_{22}	a_{23}	a_{24}	a_9^*
8	a_{33}	a_{34}	a_{35}	a_{36}	a_{37}	a_{38}	a_{39}	a_{40}	a_{25}	a_{26}	a_{27}	a_{28}	a_{29}	a_{30}	a_{31}	a_{32}
...	...								...							

Два элемента в таблице обозначены различными символами тогда и только тогда, когда вероятность того, что значения этих элементов совпадают, меньше 1.

Длина дифференциала

Определение

Пусть α' — ненулевой дифференциал, содержащий хотя бы один определенный элемент. Длиной дифференциала α' будем называть число $m \in \mathbb{N}$, такое что при $\alpha^{(0)} = \alpha'$ дифференциал $\alpha^{(m)}$ содержит хотя бы один определенный элемент, а в $\alpha^{(m+1)}$ все элементы являются неопределенными.

Наивный алгоритм перечисления дифференциалов

Алгоритм 1. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

Наивный алгоритм перечисления дифференциалов

Алгоритм 1. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.

Наивный алгоритм перечисления дифференциалов

Алгоритм 1. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.
2. Для каждого разбиения из п. 1 перечислить разбиения множества определенных ненулевых элементов на блоки, так что элементы находятся в одном блоке $\Leftrightarrow$ их значения равны.

Наивный алгоритм перечисления дифференциалов

Алгоритм 1. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.
2. Для каждого разбиения из п. 1 перечислить разбиения множества определенных ненулевых элементов на блоки, так что элементы находятся в одном блоке $\Leftrightarrow$ их значения равны.
3. Для каждого дифференциала из п. 2. Вернуть дифференциал, если его длина равна k.

Наивный алгоритм перечисления дифференциалов

Алгоритм 1. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.
2. Для каждого разбиения из п. 1 перечислить разбиения множества определенных ненулевых элементов на блоки, так что элементы находятся в одном блоке $\Leftrightarrow$ их значения равны.
3. Для каждого дифференциала из п. 2. Вернуть дифференциал, если его длина равна k.

Временная сложность

Пусть n — число элементов во входном дифференциале. Тогда общее число построенных дифференциалов равно $B_{n+1} - 1 = O(B_{n+1})$, где B_t — число Белла, $t \in \mathbb{N}_0$.

Наивный алгоритм перечисления дифференциалов

Алгоритм 1. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.
2. Для каждого разбиения из п. 1 перечислить разбиения множества определенных ненулевых элементов на блоки, так что элементы находятся в одном блоке $\Leftrightarrow$ их значения равны.
3. Для каждого дифференциала из п. 2. Вернуть дифференциал, если его длина равна k.

Временная сложность

Пусть n — число элементов во входном дифференциале. Тогда общее число построенных дифференциалов равно $B_{n+1} - 1 = O(B_{n+1})$, где B_t — число Белла, $t \in \mathbb{N}_0$. Для алгоритма Zodiac ($n = 16$) необходимо перебрать $82\,864\,869\,803$ дифференциалов.

Быстрый алгоритм перечисления дифференциалов

Алгоритм 2. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

Быстрый алгоритм перечисления дифференциалов

Алгоритм 2. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.

Быстрый алгоритм перечисления дифференциалов

Алгоритм 2. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.
2. Для каждого разбиения из п. 1 положить все определенные ненулевые элементы равными. Если длина данного дифференциала $\geq k$, то перейти к п. 3.

Быстрый алгоритм перечисления дифференциалов

Алгоритм 2. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

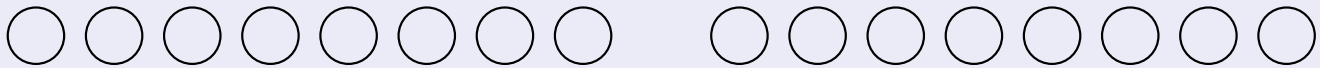
1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.
2. Для каждого разбиения из п. 1 положить все определенные ненулевые элементы равными. Если длина данного дифференциала $\geq k$, то перейти к п. 3.
3. Для дифференциала из п. 2 выполнить пп. 2–3 алгоритма 1.

Быстрый алгоритм перечисления дифференциалов

Алгоритм 2. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.
2. Для каждого разбиения из п. 1 положить все определенные ненулевые элементы равными. Если длина данного дифференциала $\geq k$, то перейти к п. 3.
3. Для дифференциала из п. 2 выполнить пп. 2–3 алгоритма 1.

Иллюстрация работы. Поиск дифференциалов длины $k = 8$



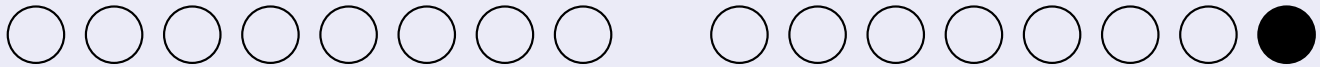
Выделяем ненулевые элементы.

Быстрый алгоритм перечисления дифференциалов

Алгоритм 2. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.
2. Для каждого разбиения из п. 1 положить все определенные ненулевые элементы равными. Если длина данного дифференциала $\geq k$, то перейти к п. 3.
3. Для дифференциала из п. 2 выполнить пп. 2–3 алгоритма 1.

Иллюстрация работы. Поиск дифференциалов длины $k = 8$



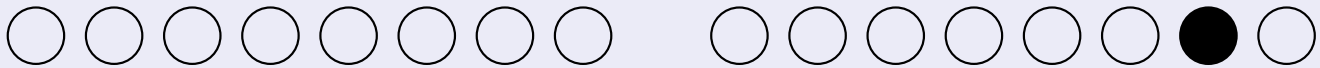
Выделяем ненулевые элементы.

Быстрый алгоритм перечисления дифференциалов

Алгоритм 2. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.
2. Для каждого разбиения из п. 1 положить все определенные ненулевые элементы равными. Если длина данного дифференциала $\geq k$, то перейти к п. 3.
3. Для дифференциала из п. 2 выполнить пп. 2–3 алгоритма 1.

Иллюстрация работы. Поиск дифференциалов длины $k = 8$



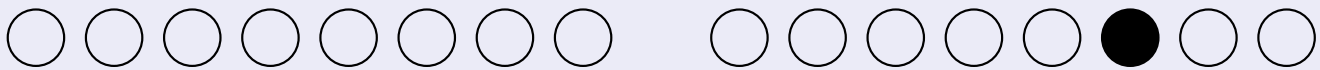
Выделяем ненулевые элементы.

Быстрый алгоритм перечисления дифференциалов

Алгоритм 2. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.
2. Для каждого разбиения из п. 1 положить все определенные ненулевые элементы равными. Если длина данного дифференциала $\geq k$, то перейти к п. 3.
3. Для дифференциала из п. 2 выполнить пп. 2–3 алгоритма 1.

Иллюстрация работы. Поиск дифференциалов длины $k = 8$



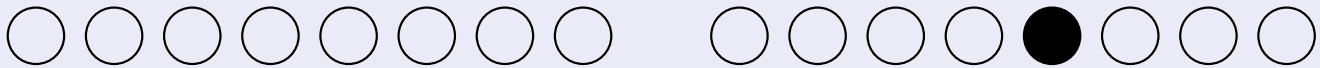
Выделяем ненулевые элементы.

Быстрый алгоритм перечисления дифференциалов

Алгоритм 2. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.
2. Для каждого разбиения из п. 1 положить все определенные ненулевые элементы равными. Если длина данного дифференциала $\geq k$, то перейти к п. 3.
3. Для дифференциала из п. 2 выполнить пп. 2–3 алгоритма 1.

Иллюстрация работы. Поиск дифференциалов длины $k = 8$



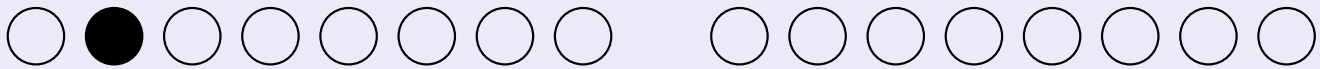
И так далее.

Быстрый алгоритм перечисления дифференциалов

Алгоритм 2. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.
2. Для каждого разбиения из п. 1 положить все определенные ненулевые элементы равными. Если длина данного дифференциала $\geq k$, то перейти к п. 3.
3. Для дифференциала из п. 2 выполнить пп. 2–3 алгоритма 1.

Иллюстрация работы. Поиск дифференциалов длины $k = 8$

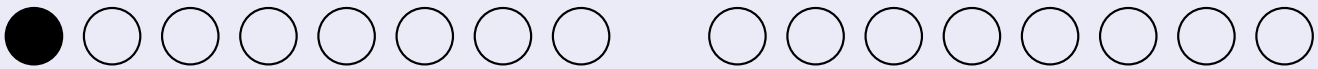


Быстрый алгоритм перечисления дифференциалов

Алгоритм 2. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.
2. Для каждого разбиения из п. 1 положить все определенные ненулевые элементы равными. Если длина данного дифференциала $\geq k$, то перейти к п. 3.
3. Для дифференциала из п. 2 выполнить пп. 2–3 алгоритма 1.

Иллюстрация работы. Поиск дифференциалов длины $k = 8$

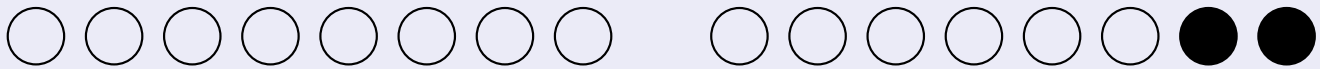


Быстрый алгоритм перечисления дифференциалов

Алгоритм 2. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.
2. Для каждого разбиения из п. 1 положить все определенные ненулевые элементы равными. Если длина данного дифференциала $\geq k$, то перейти к п. 3.
3. Для дифференциала из п. 2 выполнить пп. 2–3 алгоритма 1.

Иллюстрация работы. Поиск дифференциалов длины $k = 8$

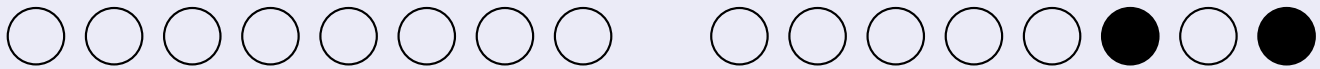


Быстрый алгоритм перечисления дифференциалов

Алгоритм 2. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.
2. Для каждого разбиения из п. 1 положить все определенные ненулевые элементы равными. Если длина данного дифференциала $\geq k$, то перейти к п. 3.
3. Для дифференциала из п. 2 выполнить пп. 2–3 алгоритма 1.

Иллюстрация работы. Поиск дифференциалов длины $k = 8$

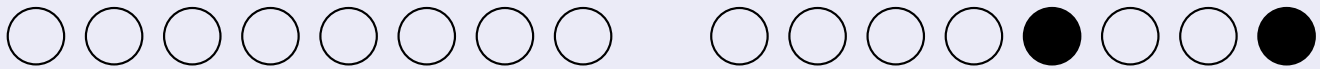


Быстрый алгоритм перечисления дифференциалов

Алгоритм 2. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.
2. Для каждого разбиения из п. 1 положить все определенные ненулевые элементы равными. Если длина данного дифференциала $\geq k$, то перейти к п. 3.
3. Для дифференциала из п. 2 выполнить пп. 2–3 алгоритма 1.

Иллюстрация работы. Поиск дифференциалов длины $k = 8$

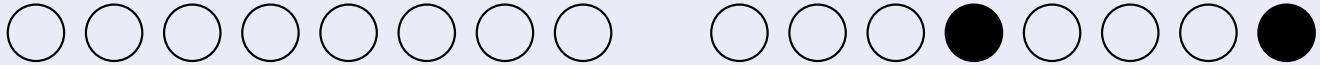


Быстрый алгоритм перечисления дифференциалов

Алгоритм 2. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.
2. Для каждого разбиения из п. 1 положить все определенные ненулевые элементы равными. Если длина данного дифференциала $\geq k$, то перейти к п. 3.
3. Для дифференциала из п. 2 выполнить пп. 2–3 алгоритма 1.

Иллюстрация работы. Поиск дифференциалов длины $k = 8$



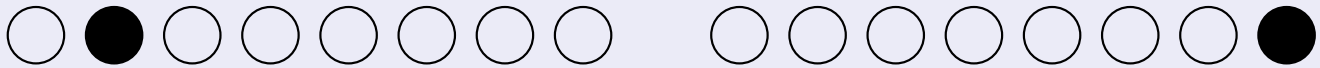
И так далее.

Быстрый алгоритм перечисления дифференциалов

Алгоритм 2. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.
2. Для каждого разбиения из п. 1 положить все определенные ненулевые элементы равными. Если длина данного дифференциала $\geq k$, то перейти к п. 3.
3. Для дифференциала из п. 2 выполнить пп. 2–3 алгоритма 1.

Иллюстрация работы. Поиск дифференциалов длины $k = 8$

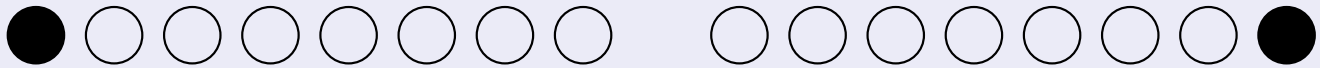


Быстрый алгоритм перечисления дифференциалов

Алгоритм 2. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.
2. Для каждого разбиения из п. 1 положить все определенные ненулевые элементы равными. Если длина данного дифференциала $\geq k$, то перейти к п. 3.
3. Для дифференциала из п. 2 выполнить пп. 2–3 алгоритма 1.

Иллюстрация работы. Поиск дифференциалов длины $k = 8$

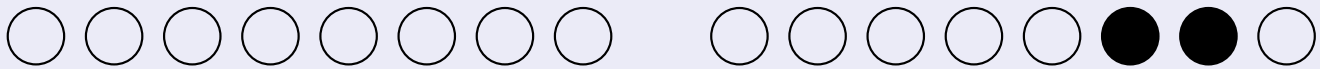


Быстрый алгоритм перечисления дифференциалов

Алгоритм 2. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.
2. Для каждого разбиения из п. 1 положить все определенные ненулевые элементы равными. Если длина данного дифференциала $\geq k$, то перейти к п. 3.
3. Для дифференциала из п. 2 выполнить пп. 2–3 алгоритма 1.

Иллюстрация работы. Поиск дифференциалов длины $k = 8$

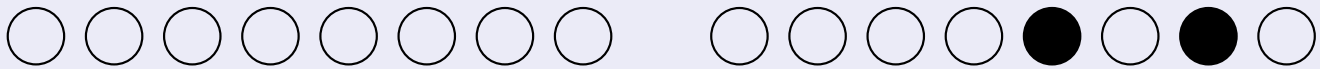


Быстрый алгоритм перечисления дифференциалов

Алгоритм 2. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.
2. Для каждого разбиения из п. 1 положить все определенные ненулевые элементы равными. Если длина данного дифференциала $\geq k$, то перейти к п. 3.
3. Для дифференциала из п. 2 выполнить пп. 2–3 алгоритма 1.

Иллюстрация работы. Поиск дифференциалов длины $k = 8$

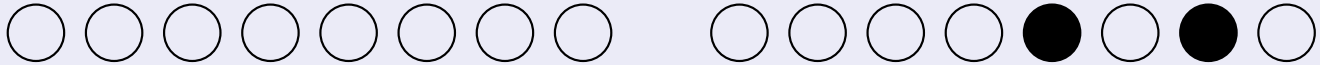


Быстрый алгоритм перечисления дифференциалов

Алгоритм 2. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.
2. Для каждого разбиения из п. 1 положить все определенные ненулевые элементы равными. Если длина данного дифференциала $\geq k$, то перейти к п. 3.
3. Для дифференциала из п. 2 выполнить пп. 2–3 алгоритма 1.

Иллюстрация работы. Поиск дифференциалов длины $k = 8$



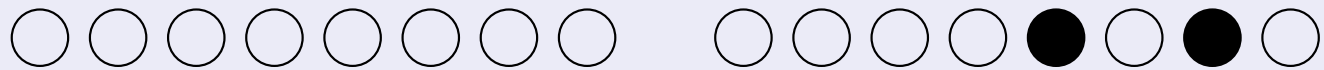
И так далее.

Быстрый алгоритм перечисления дифференциалов

Алгоритм 2. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.
2. Для каждого разбиения из п. 1 положить все определенные ненулевые элементы равными. Если длина данного дифференциала $\geq k$, то перейти к п. 3.
3. Для дифференциала из п. 2 выполнить пп. 2–3 алгоритма 1.

Иллюстрация работы. Поиск дифференциалов длины $k = 8$



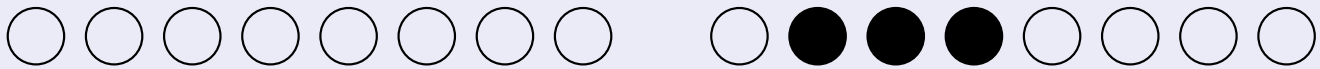
Пусть на некотором шаге найден дифференциал длины 8.

Быстрый алгоритм перечисления дифференциалов

Алгоритм 2. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.
2. Для каждого разбиения из п. 1 положить все определенные ненулевые элементы равными. Если длина данного дифференциала $\geq k$, то перейти к п. 3.
3. Для дифференциала из п. 2 выполнить пп. 2–3 алгоритма 1.

Иллюстрация работы. Поиск дифференциалов длины $k = 8$

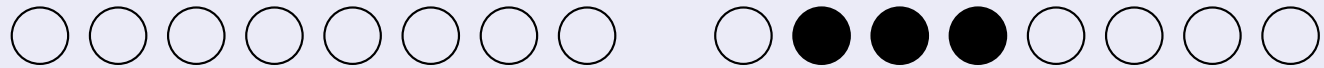


Быстрый алгоритм перечисления дифференциалов

Алгоритм 2. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.
2. Для каждого разбиения из п. 1 положить все определенные ненулевые элементы равными. Если длина данного дифференциала $\geq k$, то перейти к п. 3.
3. Для дифференциала из п. 2 выполнить пп. 2–3 алгоритма 1.

Иллюстрация работы. Поиск дифференциалов длины $k = 8$



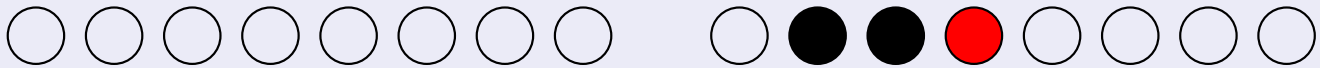
Необходимо проверить все дифференциалы данного вида.

Быстрый алгоритм перечисления дифференциалов

Алгоритм 2. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.
2. Для каждого разбиения из п. 1 положить все определенные ненулевые элементы равными. Если длина данного дифференциала $\geq k$, то перейти к п. 3.
3. Для дифференциала из п. 2 выполнить пп. 2–3 алгоритма 1.

Иллюстрация работы. Поиск дифференциалов длины $k = 8$



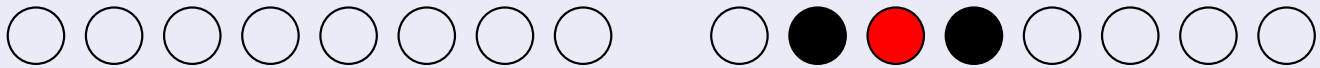
Необходимо проверить все дифференциалы данного вида.

Быстрый алгоритм перечисления дифференциалов

Алгоритм 2. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.
2. Для каждого разбиения из п. 1 положить все определенные ненулевые элементы равными. Если длина данного дифференциала $\geq k$, то перейти к п. 3.
3. Для дифференциала из п. 2 выполнить пп. 2–3 алгоритма 1.

Иллюстрация работы. Поиск дифференциалов длины $k = 8$



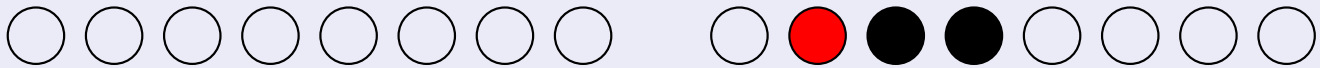
Необходимо проверить все дифференциалы данного вида.

Быстрый алгоритм перечисления дифференциалов

Алгоритм 2. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.
2. Для каждого разбиения из п. 1 положить все определенные ненулевые элементы равными. Если длина данного дифференциала $\geq k$, то перейти к п. 3.
3. Для дифференциала из п. 2 выполнить пп. 2–3 алгоритма 1.

Иллюстрация работы. Поиск дифференциалов длины $k = 8$



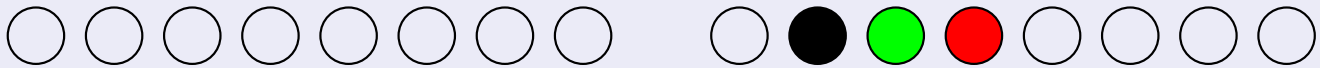
Необходимо проверить все дифференциалы данного вида.

Быстрый алгоритм перечисления дифференциалов

Алгоритм 2. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.
2. Для каждого разбиения из п. 1 положить все определенные ненулевые элементы равными. Если длина данного дифференциала $\geq k$, то перейти к п. 3.
3. Для дифференциала из п. 2 выполнить пп. 2–3 алгоритма 1.

Иллюстрация работы. Поиск дифференциалов длины $k = 8$



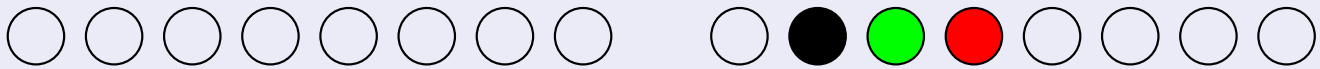
Необходимо проверить все дифференциалы данного вида.

Быстрый алгоритм перечисления дифференциалов

Алгоритм 2. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.
2. Для каждого разбиения из п. 1 положить все определенные ненулевые элементы равными. Если длина данного дифференциала $\geq k$, то перейти к п. 3.
3. Для дифференциала из п. 2 выполнить пп. 2–3 алгоритма 1.

Иллюстрация работы. Поиск дифференциалов длины $k = 8$



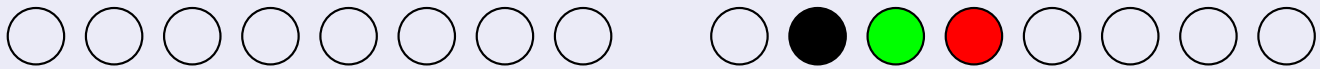
Временная сложность

Быстрый алгоритм перечисления дифференциалов

Алгоритм 2. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.
2. Для каждого разбиения из п. 1 положить все определенные ненулевые элементы равными. Если длина данного дифференциала $\geq k$, то перейти к п. 3.
3. Для дифференциала из п. 2 выполнить пп. 2–3 алгоритма 1.

Иллюстрация работы. Поиск дифференциалов длины $k = 8$



Временная сложность

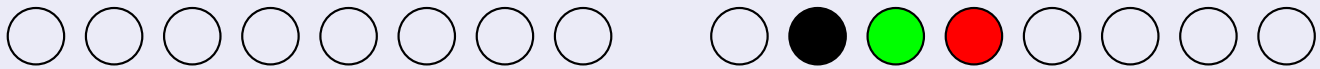
1. $O(B_{n+1})$, если $k << n/2$;

Быстрый алгоритм перечисления дифференциалов

Алгоритм 2. Перечисление дифференциалов длины k, $k \in \mathbb{N}$

1. Перечислить разбиения множества из $n = 16$ элементов на нулевые и определенные ненулевые элементы.
2. Для каждого разбиения из п. 1 положить все определенные ненулевые элементы равными. Если длина данного дифференциала $\geq k$, то перейти к п. 3.
3. Для дифференциала из п. 2 выполнить пп. 2–3 алгоритма 1.

Иллюстрация работы. Поиск дифференциалов длины $k = 8$



Временная сложность

1. $O(B_{n+1})$, если $k << n/2$;
2. $O(2^n)$, если $k \approx n/2$.

Замечание

Алгоритм 2 можно модифицировать, чтобы он мог выполняться рекурсивно. В таком случае на каждом шаге число различных ненулевых элементов должно увеличиваться на 1.

Замечание

Алгоритм 2 можно модифицировать, чтобы он мог выполняться рекурсивно. В таком случае на каждом шаге число различных ненулевых элементов должно увеличиваться на 1.

Утверждение

Алгоритм Zodiac не имеет дифференциалов, у которых длина больше 8.

Доказательство

Проверено полным перебором с использованием алгоритма 2.

Полученные результаты

Длина дифференциала	Количество дифференциалов
< 5	82 864 560 214
5	303 119
6	6 350
7	114
8	6
> 8	0
Всего	$B_{17} - 1$

Дифференциал длины 8

i	$\alpha_1^{(i)}$								$\alpha_2^{(i)}$							
1	0	0	0	0	0	0	0	0	0	a_1^*	0	0	0	0	0	0
2	0	a_1^*	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	a_2^*	a_3^*	0	0	0	0	0	0	a_1^*	0	0	0	0	0	0
4	a_4^*	a_1	a_2	a_5^*	0	0	0	0	0	a_2^*	a_3^*	0	0	0	0	0
5	a_3	a_4	a_5	a_6	a_6^*	0	0	0	a_4^*	a_1	a_2	a_5^*	0	0	0	0
6	a_7	a_8	a_9	a_{10}	a_{11}	a_7^*	0	0	a_3	a_4	a_5	a_6	a_6^*	0	0	0
7	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}	a_{17}	a_8^*	0	a_7	a_8	a_9	a_{10}	a_{11}	a_7^*	0	0
8	a_{18}	a_{19}	a_{20}	a_{21}	a_{22}	a_{23}	a_{24}	a_9^*	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}	a_{17}	a_8^*	0
9	a_{25}	a_{26}	a_{27}	a_{28}	a_{29}	a_{30}	a_{31}	a_{32}	a_{18}	a_{19}	a_{20}	a_{21}	a_{22}	a_{23}	a_{24}	a_9^*

Таблица: Один из дифференциалов длины 8

Дифференциал длины 8

i	$\alpha_1^{(i)}$								$\alpha_2^{(i)}$							
1	0	0	0	0	0	0	0	0	0	0	a_1^*	a_1^*	0	0	0	0
2	0	0	a_1^*	a_1^*	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	a_2^*	0	0	0	0	0	0	0	a_1^*	a_1^*	0	0	0	0
4	a_3^*	0	a_1	a_2	0	0	0	0	0	0	a_2^*	0	0	0	0	0
5	a_3	a_4^*	a_4	a_5	a_5^*	0	0	0	a_3^*	0	a_1	a_2	0	0	0	0
6	a_6	a_7	a_8	a_9	a_{10}	a_6^*	0	0	a_3	a_4^*	a_4	a_5	a_5^*	0	0	0
7	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}	a_7^*	0	a_6	a_7	a_8	a_9	a_{10}	a_6^*	0	0
8	a_{17}	a_{18}	a_{19}	a_{20}	a_{21}	a_{22}	a_{23}	a_8^*	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}	a_7^*	0
9	a_{24}	a_{25}	a_{26}	a_{27}	a_{28}	a_{29}	a_{30}	a_{31}	a_{17}	a_{18}	a_{19}	a_{20}	a_{21}	a_{22}	a_{23}	a_8^*

Таблица: Один из дифференциалов длины 8

Невозможные дифференциалы

Определение

Невозможным дифференциалом γ длины m будем называть такую упорядоченную пару дифференциалов $(\alpha^{(1)}, \beta^{(m)})$, что для любой пары открытых текстов $(c^{(0)}, \widetilde{c}^{(0)})$, такой что $c^{(0)} \oplus \widetilde{c}^{(0)} = \alpha^{(1)}$, выполняется $c^{(m)} \oplus \widetilde{c}^{(m)} \neq \beta^{(m)}$.

i	$\alpha_1^{(i)}$								$\alpha_2^{(i)}$							
1	0	0	0	0	0	0	0	0	0	a_1^*	0	0	0	0	0	0
2	0	a_1^*	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	a_2^*	a_3^*	0	0	0	0	0	0	a_1^*	0	0	0	0	0	0
4	a_4^*	a_1	a_2	a_5^*	0	0	0	0	0	a_2^*	a_3^*	0	0	0	0	0
5	a_3	a_4	a_5	a_6	a_6^*	0	0	0	a_4^*	a_1	a_2	a_5^*	0	0	0	0
6	a_7	a_8	a_9	a_{10}	a_{11}	a_7^*	0	0	a_3	a_4	a_5	a_6	a_6^*	0	0	0
7	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}	a_{17}	a_8^*	0	a_7	a_8	a_9	a_{10}	a_{11}	a_7^*	0	0
8	a_{18}	a_{19}	a_{20}	a_{21}	a_{22}	a_{23}	a_{24}	a_9^*	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}	a_{17}	a_8^*	0
9	a_{25}	a_{26}	a_{27}	a_{28}	a_{29}	a_{30}	a_{31}	a_{32}	a_{18}	a_{19}	a_{20}	a_{21}	a_{22}	a_{23}	a_{24}	a_9^*
9’	a_{30}	a_{31}	a_{32}	a_{33}	a_{34}	a_{13}^*	0	0	a_{35}	a_{36}	a_{37}	a_{38}	a_{39}	a_{40}	a_{14}^*	0
10’	a_{27}	a_{13}^*	a_{28}	a_{29}	a_{14}^*	0	0	0	a_{30}	a_{31}	a_{32}	a_{33}	a_{34}	a_{13}^*	0	0
11’	a_{12}^*	0	a_{25}	a_{26}	0	0	0	0	a_{27}	a_{13}^*	a_{28}	a_{29}	a_{14}^*	0	0	0
12’	0	0	a_{11}^*	0	0	0	0	0	a_{12}^*	0	a_{25}	a_{26}	0	0	0	0
13’	0	0	a_{10}^*	a_{10}^*	0	0	0	0	0	0	a_{11}^*	0	0	0	0	0
14’	0	0	0	0	0	0	0	0	0	0	a_{10}^*	a_{10}^*	0	0	0	0
15’	0	0	a_{10}^*	a_{10}^*	0	0	0	0	0	0	0	0	0	0	0	0

Эффективные невозможные дифф-лы длины 14

1	$\alpha^{(1)}$	0	a_1^*	a_1^*	a_1^*	0	0	0	0	0	a_2^*	a_3^*	a_3^*	0	0	0	0
	$\beta^{(14)}$	0	a_4^*	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	$\alpha^{(1)}$	0	a_1^*	a_1^*	a_1^*	0	0	0	0	0	a_2^*	a_3^*	0	a_3^*	a_3^*	a_3^*	a_3^*
	$\beta^{(14)}$	0	a_4^*	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	$\alpha^{(1)}$	0	a_1^*	a_1^*	a_1^*	0	0	0	0	0	a_2^*	0	a_3^*	a_3^*	a_3^*	a_3^*	a_3^*
	$\beta^{(14)}$	0	a_4^*	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	$\alpha^{(1)}$	0	a_1^*	a_1^*	a_1^*	0	0	0	0	0	a_2^*	a_3^*	a_3^*	0	0	0	0
	$\beta^{(14)}$	0	0	a_4^*	a_4^*	0	0	0	0	0	0	0	0	0	0	0	0

Эффективные невозможные дифф-лы длины 14

5	$\alpha^{(1)}$	0	a_1^*	a_1^*	a_1^*	0	0	0	0	0	a_2^*	a_3^*	0	a_3^*	a_3^*	a_3^*	a_3^*
	$\beta^{(14)}$	0	0	a_4^*	a_4^*	0	0	0	0	0	0	0	0	0	0	0	0
6	$\alpha^{(1)}$	0	a_1^*	a_1^*	a_1^*	0	0	0	0	0	a_2^*	0	a_3^*	a_3^*	a_3^*	a_3^*	a_3^*
	$\beta^{(14)}$	0	0	a_4^*	a_4^*	0	0	0	0	0	0	0	0	0	0	0	0
7	$\alpha^{(1)}$	0	a_1^*	a_1^*	a_1^*	0	0	0	0	0	a_2^*	a_3^*	0	0	0	0	0
	$\beta^{(14)}$	0	a_4^*	a_4^*	a_4^*	0	0	0	0	0	0	0	0	0	0	0	0
8	$\alpha^{(1)}$	0	a_1^*	a_1^*	a_1^*	0	0	0	0	0	a_2^*	0	a_3^*	0	0	0	0
	$\beta^{(14)}$	0	a_4^*	a_4^*	a_4^*	0	0	0	0	0	0	0	0	0	0	0	0

Утверждение

Пусть α — дифференциал длины m_1, $\widetilde{\alpha}$ — дифференциал длины m_2. Тогда на этих дифференциалах нельзя построить невозможный дифференциал длины $l \geq m_1 + m_2$.

Доказательство

Положим $\alpha^{(1)} = \alpha$, $\widetilde{\alpha}^{(1)} = \widetilde{\alpha}$. Все элементы в $\alpha_1^{(m_1+1)}$ являются неопределенными (в противном случае длина α была бы больше, чем m_1). В $\widetilde{\alpha}_1^{(m_2+1)}$ все элементы также неопределены. Тогда из свойства последнего раунда дифференциала следует ч. т. д.

Утверждение

Пусть α — дифференциал длины m_1, $\widetilde{\alpha}$ — дифференциал длины m_2. Тогда на этих дифференциалах нельзя построить невозможный дифференциал длины $l \geq m_1 + m_2$.

Доказательство

Положим $\alpha^{(1)} = \alpha$, $\widetilde{\alpha}^{(1)} = \widetilde{\alpha}$. Все элементы в $\alpha_1^{(m_1+1)}$ являются неопределенными (в противном случае длина α была бы больше, чем m_1). В $\widetilde{\alpha}_1^{(m_2+1)}$ все элементы также неопределены. Тогда из свойства последнего раунда дифференциала следует ч. т. д.

Следствие

Алгоритм шифрования Zodiac не имеет невозможных дифференциалов длины, большей чем 15.

Полученные результаты

Длина невозм. дифф-ла	Количество невозм. дифф-лов
14	352
15	8
> 15	0

Полученные результаты

Длина невозм. дифф-ла	Количество невозм. дифф-лов
14	352
15	8
> 15	0

Вывод

При атаке с известным открытым текстом полученные невозможные дифференциалы могут быть использованы в совокупности. При атаке с выбранным открытым текстом знание всех невозможных дифференциалов позволит выбрать самый эффективный.

Список литературы


Deukjo Hong, Jaechul Sung, Shiho Moriai, SangjinLee and Jongin Lim, Impossible Differential Cryptanalysis of Zodiac, FSE 2001


ChangHyi Lee, KyungHwa Jun, MinSukJung, SangBae Park, and JongDeok Kim, Zodiac Version 1.0(revised) Architecture and Specification, Standardization Workshop on Information Security Technology 2000, Korean Contribution on MP18033, ISO/IEC JTC1/SC27 N2563, 2000.

Спасибо за внимание!