А. В. Котов

ОПИСАНИЕ НЕВОЗМОЖНЫХ РАЗНОСТЕЙ БЛОЧНОГО ШИФРА ZODIAC

Введение

Данная работа основана на материале, изложенном в [1]. В статье [1] приведено несколько невозможных разностей, но не упомянут алгоритм их поиска или построения.

В настоящей работе формализованы некоторые понятия, введенные в [1], приведены два алгоритма перечисления разностей заданной длины и выписаны наиболее эффективные для атаки невозможные разности.

1. Разности

V_n — линейное пространство размерности n, $Vn = E_2^{(n)}$, $E_2 = \{0,1\}$

$c^{(i)}$ — шифртекст после i-ых раундов ($i = \overline{0,16}$), $c^{(i)} = (c_1^{(i)}, c_2^{(i)})$, где

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

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

Определение 2.1. Пусть $c^{(0)}$ и $\tilde{c}^{(0)}$ — произвольная пара открытых текстов. Тогда $\alpha^{(i)} = (\alpha_1^{(i)}, \alpha_2^{(i)}) = (c_1^{(i-1)} \oplus \tilde{c}_1^{(i-1)},\ c_2^{(i-1)} \oplus \tilde{c}_2^{(i-1)})$ — входная разность i-го раунда для пары открытых текстов $c^{(0)}$ и $\tilde{c}^{(0)}$. $\beta^{(i)} = (\alpha_1^{(i+1)})$ — выходная разность i-го раунда. Входной разностью будем называть входную разность первого раунда.

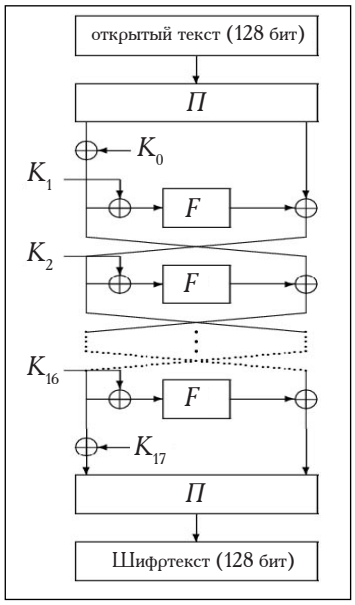

Рис. 1. Структура алгоритма Zodiac

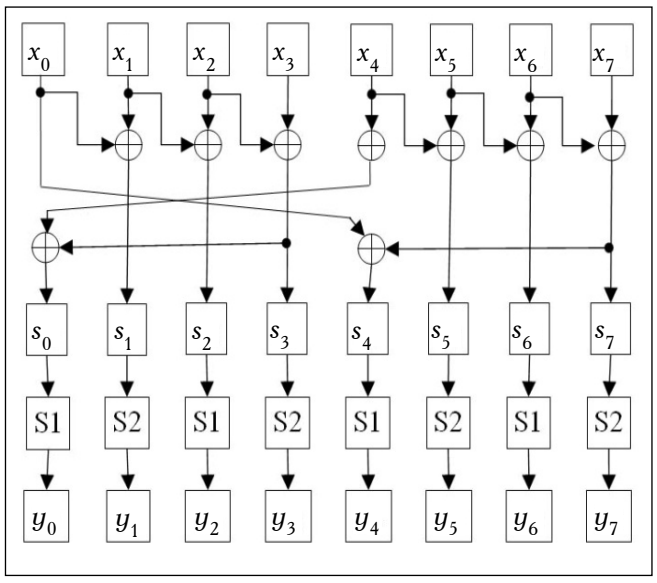

Рис. 2. Цикловая функция F

На рис. 1 изображена схема алгоритма Zodiac. Принцип работы функции f показан на рис. 2, где $x_j, s_j, y_j \in V_8$, $j = \overline{0,7}$. s-Блоки $s1$ и $s2$ — некоторые нелинейные подстановки на V_8.

Определение 2.2. Пусть $\alpha^{(1)}$ — фиксированная входная разность. Распишем $\alpha^{(i)}$ следующим образом:

$$\alpha^{(i)} = (\alpha_1^{(i)}, \alpha_2^{(i)}),\ \alpha_1^{(i)} = (x_{t,0}^{(i)}, x_{t,1}^{(i)}, ..., x_{t,7}^{(i)}),\ x_{t,j}^{(i)} \in V_8,\ t = \overline{1,2},\ j = \overline{0,7},\ i = \overline{1,16}.$$

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

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

В противном случае, если

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

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

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

Определение 2.3. Пусть α — ненулевая разность, содержащая хотя бы один определенный элемент. Длиной разности α будем называть такое число $l(\alpha) \in \mathbf{N}$, что при $\alpha^{(0)} = \alpha$ разность $\alpha^{(l(\alpha))}$ содержит хотя бы один определенный элемент, а в $\alpha^{(l(\alpha)+1)}$ все элементы являются неопределенными.

Покажем корректность определения. Если в $\alpha^{(i)}, i = 1,2,...$ все элементы являются неопределенными, то и в $\alpha^{(i+1)}$ все элементы также являются неопределенными, т. е. длина разности определена однозначно. Также длина ненулевой разности всегда конечна, что было проверено полным перебором всех различных разностей.

Приведем два алгоритма перечисления разностей. Для удобства будем считать, что каждый элемент входной разности может быть нулевым и определенным ненулевым. Ситуация, когда некоторый элемент входной разности не определен, разбивается на случаи, когда этот элемент нулевой или определенный ненулевой.

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	$a_{25}\ a_{26}\ a_{27}\ a_{28}\ a_{29}\ a_{30}\ a_{31}\ a_{32}$	$a_{18}\ a_{19}\ a_{20}\ a_{21}\ a_{22}\ a_{23}\ a_{24}\ a_9^*$

Рис. 3. Пример разности длины 8

Алгоритм 1. (Перечисление всех разностей и нахождение их длин)

1. $A = \{1, 2, ..., 16\}$;

{m — число определенных ненулевых элементов}

2. для $m = 1, 2, ..., 16$

3. для всех $B \subseteq A$, таких что $|B| = m$ do

4. для всех B' — разбиение множества B

5. В разности $\alpha^{(1)}$ на места из B записываем определенные ненулевые элементы, причем два элемента равны $\Leftrightarrow$ их номера принадлежат одному блоку в B'. На остальные места записываем нули.

6: Выводим пару $(\alpha^{(1)}, l(\alpha^{(1)}))$.

Общее число построенных разностей в таком случае равно $b_{17} - 1 = 82864869803$, где b_m — число Белла, $m \in \mathbf{N}_0$.

Алгоритм 2. (Перечисление разностей длины n, $n = 1, 2, \ldots$)

Находим разности длины n, у которых все ненулевые элементы равны. В дальнейшем для каждой найденной разности α действуем по следующему алгоритму.

1. $B = \{i:$ На i-м месте α содержит ненулевой элемент$\}$

2. для всех B' — разбиение множества B

3. В разности $\alpha^{(1)}$ на места из B записываем определенные ненулевые элементы, причем два элемента равны $\Leftrightarrow$ их номера принадлежат одному блоку в B'. На остальные места записываем нули.

4. if $l(\alpha^{(1)}) = n$ then

5. Выводим $\alpha^{(1)}$.

Для того чтобы, к примеру, перечислить все разности длины 7, действуя по алгоритму 2, потребовалось перебрать всего 168553 разностей.

Утверждение 2.1. *Алгоритм Zodiac не имеет разностей, у которых длина больше* 8.

Доказательство. Проведено полным перебором с использованием алгоритма 2.

В общей сложности было найдено 6 разностей длины 8, 114 разностей длины 7, 6350 — длины 6 и 303119 — длины 5.

2. Невозможные разности

Определение 3.1. Невозможной разностью γ длины m будем называть такую упорядоченную пару разностей $(\alpha^{(1)}, \beta^{(m)})$, что для любой пары открытых текстов $(c^{(0)}, \tilde{c}^{(0)})$, такой, что $c^{(0)} \oplus \tilde{c}^{(0)} = \alpha^{(1)}$, выполняется $c^{(m)} \oplus \tilde{c}^{(m)} \neq \beta^{(m)}$.

Утверждение 3.1. *Пусть* α — *разность длины* m_1, $\tilde{\alpha}$ — *разность длины* m_2. *Тогда на этих разностях нельзя построить невозможную разность длины, большей или равной* $(m_1 + m_2)$.

Доказательство. Положим $\alpha^{(1)} = \alpha, \tilde{\alpha}^{(1)} = \tilde{\alpha}$. Все элементы в $\alpha^{(m_1+1)}$ являются неопределенными (в противном случае длина α была бы больше, чем m_1). Все элементы в $\tilde{\alpha}^{(m_1+1)}$ также не определены. Тогда из метода построения невозможных разностных характеристик (см. [1]) следует ч.т.д.

Следствие. *Алгоритм шифрования Zodiac не имеет невозможных разностей длины, большей, чем 15.*

В общей сложности было найдено 8 невозможных разностей длины 15 и 352 — длины 14. В таблице на рис. 4 приведены наиболее эффективные для атаки невозможные разности 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
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

Рис. 4. Эффективные невозможные разности длины 14

Вывод

При атаке с известным открытым текстом полученные невозможные разности могут быть использованы в совокупности друг с другом. При атаке с выбранным открытым текстом знание всех невозможных разностей позволит выбрать самую эффективную.

СПИСОК ЛИТЕРАТУРЫ:

1. *Hong D., Sung J., Moriai S., Lee S., Lim J.* Impossible Differential Cryptanalysis of Zodiac. FSE 2001.
2. *Lee Ch. H., Jun K. H., Jung M. S., Park S. B., Kim J. D.* 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.