УДК 621.391

КРИПТОГРАФИЧЕСКОЕ ПРЕОБРАЗОВАНИЕ ИНФОРМАЦИИ НА ОСНОВЕ ТРЕХРАЗРЯДНЫХ ЛОГИЧЕСКИХ ФУНКЦИЙ

С.В. Рудницкий, аспирант
Черкасский государственный технологический университет, Черкассы (Украина)
Р.П. Мельник, адъюнкт
Академия пожарной безопасности имени Героев Чернобыля, Черкассы (Украина)
В.В. Веретельник, аспирант
Черкасский государственный технологический университет, Черкассы (Украина)

Ключевые слова: защита информации; логическая функция; криптографическое преобразование информации, матричное представление информации.

Аннотация: В данной работе на основе полученных выборочных экспериментальных данных и предложенного альтернативного способа записи основных элементарных функций проведен анализ базовых специализированных трехразрядных логических функций, который позволил выявить основную закономерность процесса построения моделей трехразрядных операций криптографического преобразования информации.

АКТУАЛЬНОСТЬ ПРОБЛЕМЫ

Вопрос эффективной защиты информации является приоритетным в деятельности силовых структур, банковских учреждений и авиационной службы. Утечка или изменение оперативной информации в данных ведомствах может привести к непоправимым действиям, нанести огромный вред и нести угрозу национальной безопасности страны в целом. Поэтому основной задачей является постоянное повышение качества систем защиты информации и оперативности ее обработки, прежде всего, криптостойкости и оперативности функционирования систем криптографической защиты. Одним из возможных решений проблемы безопасности является защита данных с помощью шифрования или кодирования. Предметом защиты является информация, которая хранится, обрабатывается и передается в компьютерных системах.

Вышеизложенное стало основой для проведения исследований по изучению специализированных логических функций, которые могут применяться для реализации криптографического преобразования данных.

АНАЛИЗ ПУБЛИКАЦИЙ

Систематизация логических функций, которые могут использоваться для криптографического преобразования и исследования функций декодирования информации в группе двухразрядных операций криптографического преобразования раскрыто в работах [1, 2], результаты исследования группы двухразрядных и трехразрядных криптографических операций приведены в [3, 4].

Однако в указанных исследованиях не рассматривался вопрос по изучению основных альтернативных способов записи специализированных логических функций. В будущем это позволит провести более детальный анализ и исследование свойств криптографических операций, построенных на основе специализированных логических функций.

ЦЕЛЬ РАБОТЫ

Провести исследование основных альтернативных способов записи специализированных логических функций для криптографического преобразования информации и синтез множества моделей специализированных трехразрядных логических функций, осуществить группирование моделей трехразрядных логических функций для криптографического преобразования по выбранным критериям.

ОСНОВНОЙ МАТЕРИАЛ

Определение множества трехразрядных элементарных операций базируется на том, что криптографические операции или элементарные функции синтезируются на основе выбранных основных элементарных функций и представляют собой композицию соответствующих функций преобразования: $F_{1,2,...,m} = (f_1^{(1)}, f_2^{(2)}, ..., f_m^N)$, где $f_1^{(1)}(x_1, x_2, ..., x_N)$, $f_2^{(2)}(x_1, x_2, ..., x_N)$, $f_m^{(N)}(x_1, x_2, ..., x_N)$ – функции преобразования первого, второго и N-го разряда информации соответственно, представляют собой дискретные логические функции.

На основе данных функций строятся операции криптографического кодирования и декодирования, например:

$$F^k_{30,57,106} = (f^{(1)}_{30}, f^{(2)}_{57}, f^{(3)}_{106}) \Rightarrow F^d_{45,54,106} = (f^{(1)}_{45}, f^{(2)}_{54}, f^{(3)}_{106});$$

$$F^k_{30,89,108} = (f^{(1)}_{30}, f^{(2)}_{89}, f^{(3)}_{108}) \Rightarrow F^d_{45,106,54} = (f^{(1)}_{45}, f^{(2)}_{106}, f^{(3)}_{54}),$$

где F^k, F^d – операция криптографического кодирования и декодирования соответственно; $f^{(1)}, f^{(2)}, f^{(3)}$ – основные элементарные операции над первым, вторым и третьим разрядом информации соответственно, а нижние индексы – обозначение номеров основных элементарных криптографических операций.

Для реализации исследования был проведен вычислительный эксперимент, в результате которого получено возможное множество моделей специализированных трехразрядных логических функций для криптографического преобразования информации. После чего проведена систематизация полученных экспериментальных данных, а именно осуществлено группирование моделей трехразрядных логических функций для криптографического преобразования по выбранным критериям и присвоенные им порядковые номера. В табл. 1приведены отдельные выборочные результаты вычислительного эксперимента.

Таблица 1. Выборочные данные результатов вычислительного эксперимента.

№ п/п	Номера криптографических функций кодирования	Номера криптографических функций декодирования	Принадлежность каждой из функций к группе (номер группы)	
			кодирование	декодирование
1.	**30 57 106**	**45 54 106**	**9 9 9**	**9 9 9**
2.	30 89 108	45 106 54	9 9 9	9 9 9
3.	30 106 57	75 86 108	9 9 9	9 9 9
4.	30 108 89	75 108 86	9 9 9	9 9 9
5.	**45 54 106**	**30 57 106**	**9 9 9**	**9 9 9**
6.	45 89 99	75 101 57	9 9 9	9 9 9
7.	**45 99 89**	**45 99 89**	**9 9 9**	**9 9 9**
8.	45 106 54	30 89 108	9 9 9	9 9 9
9.	54 45 106	54 45 106	9 9 9	9 9 9
10.	54 101 120	106 45 54	9 9 9	9 9 9
11.	54 106 45	86 75 108	9 9 9	9 9 9
12.	54 120 101	108 75 86	9 9 9	9 9 9
13.	57 30 106	57 30 106	9 9 9	9 9 9
14.	57 75 101	99 45 89	9 9 9	9 9 9
15.	57 101 75	101 75 57	9 9 9	9 9 9
16.	57 106 30	89 30 108	9 9 9	9 9 9
17.	**75 57 101**	**75 57 101**	**9 9 9**	**9 9 9**
18.	75 86 108	30 106 57	9 9 9	9 9 9
19.	75 101 57	45 89 99	9 9 9	9 9 9
20.	**75 108 86**	**30 108 89**	**9 9 9**	**9 9 9**
21.	86 75 108	54 106 45	9 9 9	9 9 9
22.	86 99 120	106 54 45	9 9 9	9 9 9
23.	86 108 75	86 108 75	9 9 9	9 9 9
24.	86 120 99	108 86 75	9 9 9	9 9 9
25.	89 30 108	57 106 30	9 9 9	9 9 9
26.	89 45 99	99 89 45	9 9 9	9 9 9
27.	89 99 45	101 57 75	9 9 9	9 9 9
28.	89 108 30	89 108 30	9 9 9	9 9 9
29.	99 45 89	57 75 101	9 9 9	9 9 9
30.	99 86 120	106 30 57	9 9 9	9 9 9
31.	99 89 45	89 45 99	9 9 9	9 9 9
32.	99 120 86	108 30 89	9 9 9	9 9 9
33.	101 54 120	106 57 30	9 9 9	9 9 9
34.	101 57 75	89 99 45	9 9 9	9 9 9
35.	101 75 57	57 101 75	9 9 9	9 9 9
36.	101 120 54	108 89 30	9 9 9	9 9 9
37.	106 30 57	99 86 120	9 9 9	9 9 9
38.	106 45 54	54 101 120	9 9 9	9 9 9
39.	106 54 45	86 99 120	9 9 9	9 9 9
40.	106 57 30	101 54 120	9 9 9	9 9 9
41.	108 30 89	99 120 86	9 9 9	9 9 9
42.	108 75 86	54 120 101	9 9 9	9 9 9
43.	108 86 75	86 120 99	9 9 9	9 9 9
44.	108 89 30	101 120 54	9 9 9	9 9 9
45.	**120 54 101**	**120 99 86**	**9 9 9**	**9 9 9**
46.	120 86 99	120 86 99	9 9 9	9 9 9
47.	**120 99 86**	**120 54 101**	**9 9 9**	**9 9 9**
48.	120 101 54	120 101 54	9 9 9	9 9 9

Данное исследование будет касаться только девятой группы специализированных логических функций криптографического преобразования. В ходе исследования девятой группы специализированных трехразрядных логических функций, которые могут применяться в качестве функций криптографического преобразования информации, найдены базовые функции (выделены жирным шрифтом в табл. 1). В таблице номера криптографических функций кодирования и декодирования могут быть представлены, как в табл. 2.

Анализ базовых функций в дальнейшей перспективе позволит понять процесс построения моделей трехразрядных операций криптографических преобразований на их основе.

Предыдущие исследования использовали запись трехразрядных логических функций по следующей модели:

$$\vec{F} = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus a_{13}x_3 \oplus b_1 \\ a_{21}x_1 \oplus a_{22}x_2 \oplus a_{23}x_3 \oplus b_2 \\ a_{31}x_1 \oplus a_{32}x_2 \oplus a_{33}x_3 \oplus b_3 \end{pmatrix},$$

где $a_{ij} \in [0,1]$, $b_i \in [0,1]$, $\oplus$ – операция сумма по mod 2.

Таблица 2. Описание криптографических функций

№ п/п	Двоичный код функции	Номер функции в десятичной системе счисления	Обозначение функции	Описание функции
1.	00011110	(30)	f_{30}	$x_1 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_2 \cdot x_3$
2.	00101101	(45)	f_{45}	$x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3$
3.	00110110	(54)	f_{54}	$\bar{x}_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3$

Например, если расписать каждую операцию, то получим расширенное дискретное представление криптографических операций:

$$F^k_{30,57,106} = \begin{bmatrix} x_1 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_2 \cdot x_3 \\ \bar{x}_1 \cdot x_2 \vee x_2 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3 \\ x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3 \end{bmatrix}; \quad F^d_{45,54,106} = \begin{bmatrix} x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3 \\ \bar{x}_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3 \\ x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3 \end{bmatrix};$$

$$F^k_{30,89,108} = \begin{bmatrix} x_1 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_2 \cdot x_3 \\ \bar{x}_1 \cdot x_3 \vee x_2 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3 \\ x_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3 \end{bmatrix}; \quad F^d_{45,106,54} = \begin{bmatrix} x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3 \\ x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3 \\ \bar{x}_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3 \end{bmatrix};$$

$$F^k_{30,106,57} = \begin{bmatrix} x_1 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_2 \cdot x_3 \\ x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3 \\ \bar{x}_1 \cdot x_2 \vee x_2 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3 \end{bmatrix}; \quad F^d_{75,86,108} = \begin{bmatrix} x_1 \cdot \bar{x}_3 \vee \cdot x_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3 \\ \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3 \\ x_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3 \end{bmatrix}.$$

Но, к сожалению, это не дало возможность выявить основные закономерности построения моделей функций криптографического преобразования. Поэтому было принято решение предложить другое альтернативное представление полученных специализированных трехразрядных логических функций для дальнейшего анализа и выявления закономерностей процесса построения.

Было предложено полиномиальное представление основных функций в базисе $\langle \wedge, \oplus, HE \rangle$, где стала заметна характерная закономерность замещения функций x_1, x_2, x_3.

$$F^k_{30,57,106} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3), \\ x_2 \oplus (x_1 \cdot \bar{x}_3), \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix}; \quad F^d_{45,54,106} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3), \\ x_2 \oplus (x_1 \cdot x_3), \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix};$$

$$F^k_{30,89,108} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \end{bmatrix}; \quad F^d_{45,106,54} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_2 \oplus (x_1 \cdot x_3) \end{bmatrix};$$

$$F^k_{30,106,57} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \end{bmatrix}; \quad F^d_{75,86,108} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_3 \oplus (x_1 \cdot x_2) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \end{bmatrix}.$$

Как видно из представления криптографических операций основная закономерность заключается в изменении положения инверсии в записи основных функций.

ВЫВОДЫ

В результате исследования девятой группы специализированных трехразрядных логических функций среди них были обнаружены базовые или основные функции криптографического преобразования. Исследовав обнаруженные функции в базисе $\langle \wedge, \oplus, HE \rangle$, была найдена закономерность замещения функций x_1, x_2, x_3 для построения криптографических операций на их основе.

Работа авторов частично поддержана Федеральной целевой программой «Научные и научно-педагогические кадры инновационной России» на 2009–2013 годы (соглашение № 14.B37.21.1934).

СПИСОК ЛИТЕРАТУРЫ

1. Рудницький В.М. Систематизація повної множини логічних функцій для криптографічного перетворення інформації / В.М. Рудницький, І.В. Миронець, В.Г. Бабенко // Зб. наук. пр. «Системи обробки інформації». – Харківський університет Повітряних Сил імені Івана Кожедуба. – 2011. – Випуск 8 (98). – С. 184–188.
2. Бабенко В.Г. Декодування інформації в групі двохрозрядних операцій криптографічного перетворення / В.Г. Бабенко, І.В. Миронець, С.В. Рудницький // Зб. наук. пр. «Системи управління, навігації та зв'язку». – ДП «Центральний науково-дослідний інститут навігації і управління». – 2011. – Випуск 4 (20). – С. 208–212.

3. Бабенко В.Г. Дослідження групи трьохрозрядних криптографічних операцій. В.Г. Бабенко, С.В. Рудницький Восьма наукова конференція Харківського університету Повітряних Сил імені Івана Кожедуба «Новітні технології – для захисту повітряного простору», 18-19 квітня 2012 року.
4. Бабенко В.Г. Дослідження двохрозрядних операцій криптографічного перетворення / В.Г. Бабенко, С.В. Рудницький // Всеукраїнська науково-технічна конференція «Інтегровані комп'ютерні технології в машинобудуванні ІКТМ-2011»: Тези доповідей. – Харків: Національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут», 2011. – Том 3. – С. 218.

CRYPTOGRAPHIC TRANSFORMATION OF INFORMATION ON THE BASIS THREE-DIGIT LOGIC FUNCTIONS

S.V. Rurdnitsky, postgraduate student
Cherkassy State Technological University, Cherkassy (Ukraine)
R.P. Melnik, postgraduate student
The Academy of Fire Safety named after Chernobyl Heroes, Cherkassy (Ukraine)
V.V. Veretelnik, postgraduate student
Cherkassy State Technological University, Cherkassy (Ukraine)

Keywords: protection of information; logic function; cryptographic transformation of information, matrix presentation of information.

Annotation: In this paper, on the basis of the sample of experimental data and the proposed alternative method of recording the basic elementary functions of analysis of basic three-digit specialized logic functions, which identified the principal pattern of process modeling three-digit operations cryptographic transformation of information.

УДК 628.316.12

УТИЛИЗАЦИЯ ВОДОЭМУЛЬСИОННЫХ СМАЗОЧНО-ОХЛАЖДАЮЩИХ ЖИДКОСТЕЙ НА ОСНОВЕ МЕМБРАННЫХ МЕТОДОВ

Д.Д. Фазуллин, младший научный сотрудник
Г.В. Маврин, кандидат химических наук, доцент, заведующий кафедрой «Химии и экологии»
Камская государственная инженерно-экономическая академия, Набережные Челны (Россия)
Р.Г. Мелконян, доктор технических наук, профессор
Московский государственный горный университет, Москва (Россия)

Ключевые слова: производительность; селективность; мембраны; ультрафильтрация; нанофильтрация; очистка; стоки; эмульсия.

Аннотация: Нефтесодержащие сточные воды представляют значительную токсикологическую опасность для водных экосистем и для человека. Общей проблемой современных технологий машиностроения является разработка экологически безопасных систем с максимально замкнутым технологическим циклом и минимальным количеством отходов. Мембранные методы разделения, позволяют значительно снизить затраты на обработку сточных вод и получать воду требуемого качества.