УДК 004.056.055

И.В. Миронец

Черкасский государственный технологический университет, Черкассы

ОПЕРАЦИИ КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ИНФОРМАЦИИ В ДВОИЧНО-ВОСЬМЕРИЧНОЙ СИСТЕМЕ СЧИСЛЕНИЯ

Статья посвящена повышению скорости и достоверности шифрования на основе представления информации в двоично-восьмеричной системе счисления. На основании разработанной двоично-восьмеричной системы счисления для исследуемых трехразрядных логических функций кодирования-декодирования в двоичной системе были получены соответствующие функции кодирования и декодирования информации. Предложенные математические модели операций кодирования и декодирования могут быть использованы для повышения достоверности передачи конфиденциальной информации по каналам связи.

Ключевые слова: *криптографическое перекодирования, системы счисления, устройство контроля информации.*

Введение

Постановка проблемы. С массовым внедрением компьютеров во все сферы деятельности человека объем информации, хранимой в электронном виде, вырос в тысячи раз. А с появлением компьютерных сетей даже отсутствие физического доступа к компьютеру перестала быть гарантией целостности информации. В современных условиях защита информации становится все более актуальной и одновременно все более сложной проблемой, ведь несанкционированное искажения, копирования, уничтожения информации в настоящее время касаются всех сфер деяьельности, в том числе в АСУ, используемых в войсках.

Использование современных информационных технологий обусловливает необходимость решения специфических задач, таких как обеспечение уверенности в гарантиях ответственности лиц, которые отдают распоряжения, ответственности исполнителей за своевременное выполнение распоряжений и т.д. [1, 2]. Для решения указанных задач необходимо наличие специфических алгоритмов. Поэтому большой интерес вызывает анализ методов синтеза кодов, корректирующих ошибки, и разработка методов синтеза арифметических кодов [3].

Анализ публикаций и исследований. Аналитический обзор распространенных криптографических систем, современных методов и средств развития новых тенденций показал, что проблема обеспечения эффективности обработки информации в криптографических системах очень важна и актуальна.

Одним из самых действенных средств защиты информационно-телекоммуникационных систем является использование методов и средств криптографии.

Основной задачей на современном этапе развития общества и его информатизации является выполнение требования постоянного повышения качества систем защиты информации и оперативности обработки информации и, прежде всего, криптостойкости и оперативности функционирования систем криптографической защиты информации.

Проблема обеспечения высокой надежности является одной из центральных, о чем свидетельствует значительная вводимая избыточность [4-7]. Однако вводимая избыточность вступает в противоречие с быстродействием и сложностью, что, в конечном счете, сказывается на самой надежности.

Органичным обобщением возникшей проблемы можно считать работы А.В. Ткаченко, посвященные теории синтеза структурных кодов [8-11]. Разработаны принципы и методы кодирования, декодирования и выполнения арифметических операций в структурных кодах. Однако полученные системы счисления не обладают гарантированным обнаружением ошибок.

Целью данной работы является повышение скорости и достоверности шифрования на основе представления информации в двоично-восьмеричной системе счисления.

Основной материал

Эффективность функционирования системы в значительной мере определяется ее качеством, под которым понимается совокупность свойств системы, обуславливающих ее пригодность для использования по назначению [12]. Для определения уровня качества используются показатели и критерии оценки качества. Показатели качества являются его количественной мерой, а критерии оценки формируют условия, которым должны удовлетворять значения показателей и определяют правила сравнения между собой различных вариантов построения системы.

Рассмотрим представление числа X в кодах с постоянным числом единиц для любого a (a - количество единичных символов в группе разрядов). Намного проще и быстрее получить данные коды на

основе позиционных систем счисления с основанием больше или равно 2 [13].

Любое число X в данных системах счисления может быть представлено в виде слов

$$X = \pm\left(x_{n-1}, x_{n-1}, ..., x_1, x_0\right),$$

где $$X = \pm\sum_{i=0}^{n-1} x_i r^i, \quad 0 \le x \le r-1. \qquad (1)$$

Представление данного числа в виде двоичных слов будем называть двоично-r-ичной позиционной системой счисления (2r).

Представив число x в виде унарного кода при a=1, получим код числа X при a=m, где n=r*m, а m – количество разрядов в группе.

Такие 2r коды с постоянным числом единиц являются весозначными и могут рассматриваться как 2r системы счисления. Так как r-ичная система счисления обеспечивает единое представления числа X [15, 16], то и двоичная система счисления с постоянным числом единиц обеспечит единственное представление числа. Взяв за основу коды с постоянным числом единиц при a=1, можно представить в явном виде весовые коэффициенты разрядов кода:

- двоичная система счисления с постоянным числом единиц:

$0*2^0$, $1*2^0$, $0*2^1$, $1*2^1$, $0*2^2$, $1*2^2$, … , $0*2^n$, $1*2^n$;

- двоично-троичная система счисления с постоянным числом единиц:

$0*3^0$, $1*3^0$, $2*3^0$, $0*3^1$, $1*3^1$, $2*3^1$, … , $0*3^n$, $1*3^n$, $2*3^n$;

- двоично-четверичная система счисления с постоянным числом единиц:

$0*4^0$, $1*4^0$, $2*4^0$, $3*4^0$, … , $0*4^n$, $1*4^n$, $2*4^n$, $3*4^n$.

- двоично-восьмеричная система счисления с постоянным числом единиц:

$0*8^0$, $1*8^0$, $2*8^0$, $3*8^0$, $4*8^0$, $5*8^0$, $6*8^0$, $7*8^0$… , $0*8^n$, $1*8^n$, $2*8^n$, $3*8^n$,$4*8^n$, $5*8^n$, $6*8^n$, $7*8^n$.

Любое целое число X может быть представлено 2r кодом в следующем виде:

$$X = \pm\sum_{j=0}^{n-1}\sum_{i=0}^{r-1} x_{i+j} i r^i, \quad x \in [0; r-1]. \qquad (2)$$

Данное выражение легко доказывается, исходя из того, что любое число может быть представлено системой счисления с основанием больше двух (1), и что любое число может быть представлено весозначным кодом с постоянным числом единиц при a=1.

Выражение (2) позволяет сделать вывод, что любой 2r код с постоянным числом единиц при a=1 является весозначным с одномерным весовым рядом. Следовательно, данные коды можно рассматривать как системы счисления.

Синтезированные системы счисления с постоянным числом единиц являются частным случаем кодов с постоянным числом единиц, поэтому они предназначены для обнаружения ошибок в каналах передачи, хранения и обнаружения информации.

Так как весовой ряд 2r системы счисления (2) можно условно разбить на блоки по r-разрядов в каждом блоке и представленное любое число может иметь только одну единицу в каждом блоке разрядов, следовательно, устройство обнаружения ошибок будет иметь общий вид [17-18]:

$$F = \overline{F_1} \vee \overline{F_2} \vee ... \vee \overline{F_k} \vee ... \vee \overline{F_n}, \quad k \in [1; n], \qquad (3)$$

где $\overline{F_k} = C_1\overline{C_2}\,\overline{C_3}...\overline{C_r} \vee \overline{C_1}C_2\overline{C_3}...\overline{C_r} \vee ... \vee \overline{C_1}\,\overline{C_2}$, причем C_i - i - й вход устройства контроля $i \in [1; r]$.

Рассмотрим систему счисления при r=8, так как она обеспечивает наибольшую вероятность безотказной работы аппаратных средств. Для повышения быстродействия и контроля трёхразрядных операций целесообразно использовать двоично-восьмеричную систему счисления. Любое целое число X может быть в ней представлено:

$$X = \pm\sum_{j=0}^{n-1}\sum_{i=0}^{7} x_{8i+j} \cdot i \cdot 8^i, \qquad x \in [0; 1]. \qquad (4)$$

На основании разработанной двоично-восьмеричной системы счисления, для исследуемых логических функций кодирования-декодирования в двоичной системе были получены соответствующие функции кодирования и декодирования. Как пример можно рассмотреть следующие функции:

$$\vec{F}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \vec{F}\begin{pmatrix} x_1x_2x_3 \\ x_1x_2\overline{x}_3 \\ x_1\overline{x}_2x_3 \\ x_1\overline{x}_2\overline{x}_3 \\ \overline{x}_1x_2x_3 \\ \overline{x}_1x_2\overline{x}_3 \\ \overline{x}_1\overline{x}_2x_3 \\ \overline{x}_1\overline{x}_2\overline{x}_3 \end{pmatrix} \to \vec{F}^{2/8} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{pmatrix};$$

$$\vec{F}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_3 \\ x_2 \end{pmatrix} = \vec{F}\begin{pmatrix} x_1x_2x_3 \\ x_1\overline{x}_2x_3 \\ x_1x_2\overline{x}_3 \\ x_1\overline{x}_2\overline{x}_3 \\ \overline{x}_1x_2x_3 \\ \overline{x}_1\overline{x}_2x_3 \\ \overline{x}_1x_2\overline{x}_3 \\ \overline{x}_1\overline{x}_2\overline{x}_3 \end{pmatrix} \to \vec{F}^{2/8} = \begin{pmatrix} x_1 \\ x_3 \\ x_2 \\ x_4 \\ x_5 \\ x_7 \\ x_6 \\ x_8 \end{pmatrix};$$

$$\vec{F}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1 \oplus x_3 \\ x_3 \\ x_2 \end{pmatrix} = \vec{F}\begin{pmatrix} x_1x_2x_3 \\ \overline{x}_1\overline{x}_2x_3 \\ x_1x_2\overline{x}_3 \\ \overline{x}_1\overline{x}_2\overline{x}_3 \\ \overline{x}_1x_2x_3 \\ x_1\overline{x}_2x_3 \\ \overline{x}_1x_2\overline{x}_3 \\ x_1\overline{x}_2\overline{x}_3 \end{pmatrix} \to \vec{F}^{2/8} = \begin{pmatrix} x_1 \\ x_7 \\ x_2 \\ x_8 \\ x_5 \\ x_3 \\ x_6 \\ x_4 \end{pmatrix};$$

$$\vec{F}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1 \oplus x_2 \\ x_1 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix} = \vec{F}\begin{pmatrix} x_1x_2x_3 \\ x_1\bar{x}_2\bar{x}_3 \\ \bar{x}_1x_2\bar{x}_3 \\ \bar{x}_1\bar{x}_2x_3 \\ \bar{x}_1\bar{x}_2\bar{x}_3 \\ \bar{x}_1x_2x_3 \\ x_1\bar{x}_2x_3 \\ x_1x_2\bar{x}_3 \end{pmatrix} \rightarrow$$

$$\vec{F}^{2/8} = \begin{pmatrix} x_1 \\ x_4 \\ x_6 \\ x_7 \\ x_8 \\ x_5 \\ x_3 \\ x_2 \end{pmatrix};$$

$$\vec{F}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \oplus x_3 \\ x_3 \end{pmatrix} = \vec{F}\begin{pmatrix} x_1x_2x_3 \\ \bar{x}_1\bar{x}_2\bar{x}_3 \\ \bar{x}_1\bar{x}_2x_3 \\ x_1x_2\bar{x}_3 \\ \bar{x}_1x_2x_3 \\ x_1\bar{x}_2\bar{x}_3 \\ x_1\bar{x}_2x_3 \\ \bar{x}_1x_2\bar{x}_3 \end{pmatrix} \rightarrow$$

$$\vec{F}^{2/8} = \begin{pmatrix} x_1 \\ x_8 \\ x_7 \\ x_2 \\ x_5 \\ x_4 \\ x_3 \\ x_6 \end{pmatrix}.$$

Анализируя полное множество полученных функций кодирования-декодирования в двоично-восьмеричной системе счисления, можем сделать вывод, что все кодирование сводится к перестановке разрядов.

Выводы

В процессе проведения вычислительного эксперимента были получены операции кодирования-декодирования в двоично-восьмеричной системе счисления для всех трёхразрядных операций криптографического преобразования информации.

Полученный результат подтверждает гипотезу о том, что предложенные математические модели операций кодирования и декодирования могут быть использованы для повышения достоверности передачи конфиденциальной информации по каналам связи. Причем, синтезированные аналоги операций кодирования-декодирования для двоично-восьмеричной системы счисления представляют собой алгебраическую группу G_8 - перестановок.

Список литературы

1. Согомонян Б.С. Самопроверяемые устройства и отказоустойчивые системы / Б.С. Согомонян, Е.В. Слабаков. – М.: Радио и связь, 1989. - 208 с.

2. Дадаев Ю.Г. Теория арифметических кодов / Ю.Г. Дадаев. - М.: Радио и связь, 1981. – 180 с.

3. Рудницкий В.Н. Исследование методов синтеза структурных кодов / В.Н. Рудницкий, Н.Н. Пантелеева // Электроника и связь. – 2003. - № 18. – С. 62–64.

4. Рудницкий В.Н. Повышение достоверности обработки информации на основе реконфигурации структурных кодов / / В.Н. Рудницкий, Н.Н. Пантелеева // Электроника и связь. – 2003. - № 20. – С. 116–120.

5. Элементы теории испытаний и контроля технических систем. Под ред. Р.Н. Юсупова. - Л.: Энергия, 1978. – 192 с.

Поступила в редколлегию 10.08.2015

Рецензент: д-р техн. наук, проф. И.В. Рубан, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

ОПЕРАЦІЇ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ В ДВІЙКОВО - ВІСІМКОВІЙ СИСТЕМІ ЧИСЛЕННЯ

І.В. Миронець

Дана стаття присвячена підвищенню швидкості та достовірності шифрування на основі подання інформації в двійково-вісімковій системі числення. На підставі розробленої двійково-вісімковій системи числення для досліджуваних трьохрозрядних логічних функцій кодування-декодування в двійковій системі були отримані відповідні функції кодування та декодування інформації. Запропоновані математичні моделі операцій кодування і декодування можуть бути використані для підвищення достовірності передачі конфіденційної інформації по каналам зв'язку.

Ключові слова: *криптографічне кодування і декодування, системи числення, пристрій контролю інформації.*

THE OPERATIONS OF CRYPTOGRAPHIC TRANSFORMATION OF INFORMATION AT BINARY-OCTAL NUMBER SYSTEM

I.V. Mironets

This article is dedicated to increasing the speed and reliability-based encryption of information in binary-octal system. On the basis of the developed binary-octal number system for the study of logic functions of three-digit code in the binary system have been obtained by the respective functions of encoding and decoding information. The proposed mathematical model of the encoding and decoding can be used to improve the reliability of the transmission of confidential information via communication channels.

Keywords: *cryptographic transcoding, number systems, the information control device.*