Захист інформації в інформаційно-телекомунікаційних системах

УДК 004.312.26

А.А. Борисенко, Т.А. Протасова, Е.А. Протасова

Сумский государственный университет, Сумы

СИНТЕЗ КОМПОЗИЦИЙ НА ОСНОВЕ МНОГОЗНАЧНЫХ БИНОМИАЛЬНЫХ ЧИСЕЛ

В работе предложен алгоритм построения композиций на основе биномиальных систем счисления с многозначным алфавитом, приведено доказательство функции перехода от биномиального числа к композиции, рассмотрен пример, предложены блок-схема алгоритма прямого преобразования и функциональная схема формирователя композиций. Предложенная структура, а также устройство на его основе обладают повышенной помехозащищенностью и универсальностью, а использование в данном формирователе в качестве промежуточной многозначной биномиальной системы счисления существенно повышает скорость преобразований.

Ключевые слова: *комбинаторные конфигурации, многозначные биномиальные коды, криптография, сочетания, перестановки, композиции, биномиальная система счисления*

Введение

При решении задач обработки, хранения и передачи информации, в криптографии и криптоанализе широко применяются комбинаторные методы решения и, как следствие, комбинаторные конфигурации. Наиболее часто используются сочетания, перестановки, композиции. Существующие алгоритмы формирования комбинаторных конфигураций, а также устройства на их основе достаточно сложны и не являются универсальными.

Более эффективно задачу генерирования комбинаторных конфигураций можно решать с помощью многозначной биномиальной системы счисления [1], которая используется в качестве промежуточной. При таком подходе сначала формируются числа биномиальной системы счисления, а затем их преобразовывают в комбинаторные конфигурации.

В настоящее время уже предложен ряд устройств, формирующих комбинаторные конфигурации на основе многозначных биномиальных кодов, например, многозначные биномиальные счетчики для перебора сочетаний и композиций [2,3]. В работе [4] доказано свойство изоморфности многозначных биномиальных чисел и комбинаторных конфигураций типа сочетания, которое делает правомочными алгоритмы переходов от биномиальных кодов к сочетаниям, а в работе [5] предложены алгоритмы построения и структура такого устройства.

Далее рассмотрим алгоритмы формирования комбинаторной конфигурации типа композиция и докажем их правомочность.

Результаты исследований

Композицией является последовательность из *m* целых положительных чисел (цифр), сумма которых равна p. Максимальная цифра в композиции $q = p - m + 1$.

Утверждение 1. Если $\alpha_1\alpha_2\ldots\alpha_i\ldots\alpha_k$ есть многозначное число, то, если к каждой, кроме последней, α_i -й цифре этого числа прибавить единицу, т.е.

$$\beta_i = \alpha_i + 1, \qquad (1)$$

вычислить последнюю цифру β_{k+1}, равную разности параметра P и суммы $\sum_{i-1}^{k}\beta_i$ всех ранее вычисленных элементов, $\beta_{k+1} = P - \sum_{i-1}^{k}\beta_i$, полученные цифры являются элементами последовательности, которая образует композицию P из $m = k + 1$ частей $\beta_1\beta_2\ldots\beta_i\ldots\beta_{k+1}$.

Доказательство. Так как мощность множеств многозначных чисел вида $a = \alpha_1\ldots\alpha_k$ и композиций $b = \beta_1\ldots\beta_k\beta_{k+1}$ одинакова [6] то достаточно показать, что отображение f, заданное формулой (1), инъективно. Другими словами, разным многозначным числам a_1 и a_2 ставятся в соответствие различные композиции $b_1 = f(a_1) = \beta_1\ldots\beta_k\beta_{k+1}$ и $b_2 = f(a_2) = \beta_1'\ldots\beta_k'\beta_{k+1}'$. В самом деле, пусть $a_1 = \alpha_1\alpha_2\ldots\alpha_k$ и $a_2 = \alpha_1'\alpha_2'\ldots\alpha_k'$ – два различных многозначных числа, т.е. $a_1 \neq a_2$. Пусть, далее, $\ell \geq 1$ – первый слева разряд, в котором a_1 отличается от a_2, т.е.

$$\alpha_i = \alpha_\ell,\ i = 1,\ldots,\ell-1 \qquad (2)$$

$$\alpha_\ell \neq \alpha'_\ell \qquad (3)$$

Покажем, что тогда аналогичные соотношения имеют место для b_1 и b_2.

Действительно, из правила (1) и соотношений $(2)-(3)$ вытекают цепочки $\beta_i = \alpha_i + 1 = \alpha'_i + 1 = \beta'_i$, $i = 1,\ldots,\ell-1$, $\beta_i = \alpha_i + 1 \neq \alpha'_i + 1$, которые и означают, что $b_1 = f(a_1) \neq b_2 = f(a_2)$. Утверждение доказано.

Алгоритм перехода от многозначного биномиального числа к композиции, использующей утверждение 1, имеет следующий вид:

1. Прибавить к каждой цифре многозначного биномиального числа единицу. Этим формируются все разряды композиции, кроме последнего.

2. Вычислить сумму S всех полученных в пункте 1 разрядов композиции.

3. Вычислить параметр P = q + m = q + k + 1

4. Вычислить Z = P – S, где Z равно значению искомой цифры последнего k + 1-го разряда композиции

Пример 1. Биномиальное число 1123 преобразовать в композицию с параметром P = 15.

Определяем значения разрядов композиции с первого по *n*-тый.

$\beta_1 = \alpha_1 + 1 = 1 + 1 = 2$; $\beta_2 = \alpha_2 + 1 = 1 + 1 = 2$;

$\beta_3 = \alpha_3 + 1 = 2 + 1 = 3$; $\beta_4 = \alpha_4 + 1 = 3 + 1 = 4$;

Подсчитаем сумму значений разрядов композиции: $\sum_{i=1}^{n} \beta_i$:

$\beta_1 + \beta_2 + \beta_3 + \beta_4 = 2 + 2 + 3 + 4 = 11$.

Вычисляем последнюю цифру композиции: $\beta_5 = P - \sum_{i=1}^{4} \beta_i = 15 - 11 = 4$.

В результате получена композиция – 22344.

Процедуру формирования композиций иллюстрирует функциональная схема, представленная на рис. 1. Согласно алгоритму преобразования, блок-схема которого представлена на рис. 2, для получения разрядов композиций к каждому разряду биномиального числа необходимо прибавить единицу. Эту операцию можно проводить параллельно, как представлено на рис. 2.

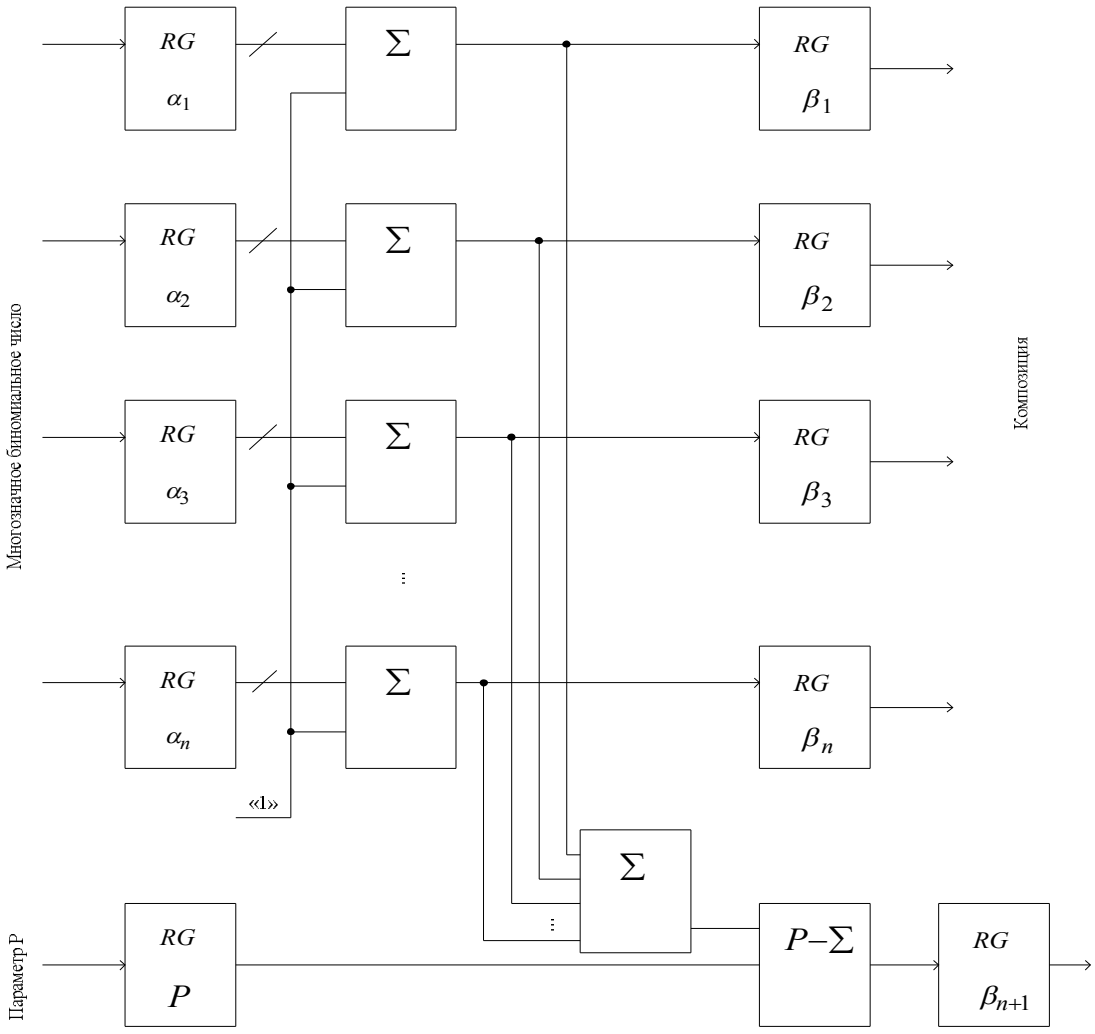

Рис. 1. Функциональная схема преобразования биномиального числа в композицию

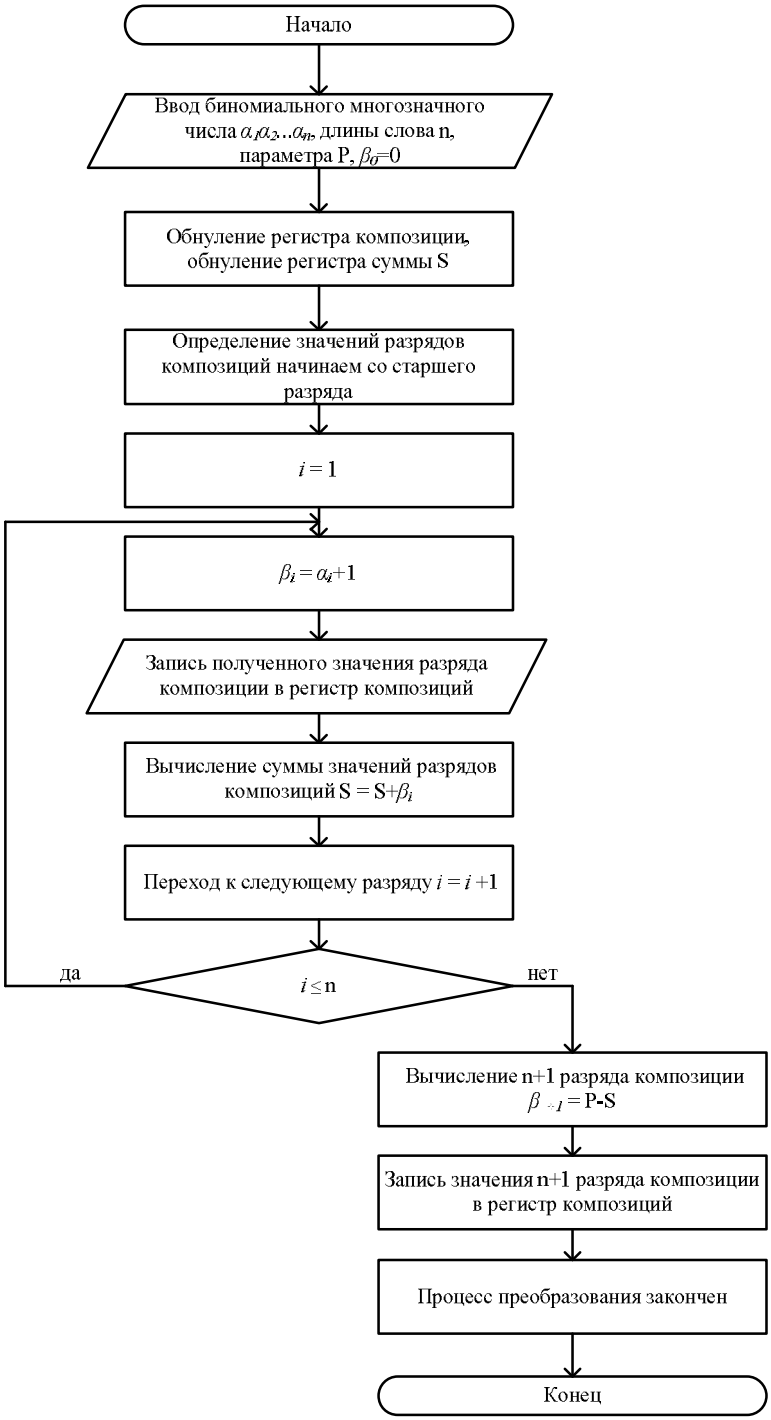

Рис. 2. Блок-схема алгоритма формирования композиций

Схема содержит:

- регистры исходного биномиального числа, в которые записаны значения разрядов биномиального числа;
- первую группу сумматоров, в которых производится суммирование разряда биномиального числа с единицей,
- отдельный сумматор, предназначенный для суммирования полученных значений разрядов композиции,
- вычитатель, предназначенный для получения последнего разряда композиции вычитанием от значения параметра суммы значений разрядов композиции,
- выходные регистры, предназначенные для хранения полученных значений разрядов композиции.

Выводы

Таким образом, в данной работе рассмотрен принцип построения комбинаторных конфигураций на основе биномиальных систем счисления с многозначным алфавитом, предложены блок-схема алгоритма прямого преобразования и структурная схема формирователя композиций. Предложенная струк-

тура, а также устройство на его основе обладают повышенной помехозащищенностью и универсальностью, а использование в данном формирователе в качестве промежуточной многозначной биномиальной системы счисления существенно повышает скорость преобразования.

Список литературы

1. Борисенко А.А. Системы счисления с биномиальным основанием / А.А. Борисенко, Е.Л. Онанченко, А.Н. Кобяков // Вестник СумГУ. – 1994. – № 1. – С. 96 – 101.

2. А.с. СССР, №1187262. Борисенко А.А., Володченко Г.С., Кузнецов В.Н., Онанченко Е.Л. Счетчик импульсов, 1984.

3. А.с. СССР, №1398090. Борисенко А.А., Онанченко Е.Л., Плескач А.И., Худогов Г.И. Счетчик импульсов, 1986.

4. Протасова Т.А. Синтез комбинаторных конфигураций на основе многозначних биномиальных кодов / Т.А. Протасова, Е.Л. Онанченко, О.А. Калигаева, В.В. Калашников, В.Д. Бугай // Вісник Сумського державного університету. — 1997. — № 2 (8). — С. 103 – 109.

5. Протасова Т.А. Формирователь сочетаний на основе многозначительных биномиальных чисел / Т.А. Протасова // Вісник Сумського державного університету. Серія Технічні науки. – 2005. – № 9 (81). — С. 32 – 38.

6. Кузнецов О.П. Дискретная математика для инженера / О.П. Кузнецов, Г.М. Адельсон–Вельский. – М.: Энергоатомиздат, 1988. – 480 с.

Надійшла до редколегії 27.03.2012

Рецензент: д-р ф.-м. наук, проф. Г.С. Воробьев, Сумский государственный университет, Сумы.

СИНТЕЗ КОМПОЗИЦІЙ НА ОСНОВІ БАГАТОЗНАЧНИХ БІНОМІАЛЬНИХ ЧИСЕЛ

О.А. Борисенко, Т.О. Протасова, К.О. Протасова

У роботі запропоновано алгоритм побудови композицій на основі біноміальних систем числення з багатозначним алфавітом, приведено доказ функції переходу від біноміального числа до композиції, розглянуто приклад, запропоновані блок-схема алгоритму прямого перетворення і функціональна схема формувача композицій. Запропонована структура, а також пристрій на його основі мають підвищену перешкодозахищеність і універсальність, а використання в даному формувачі в якості проміжної багатозначною біноміальної системи числення істотно підвищує швидкість перетворень.

Ключові слова: *комбінаторні конфігурації, багатозначні біноміальні коди, криптографія, сполучення, перестановки, комбінації, композиції, біноміальна система числення.*

SYNTHESIS OF COMPOSITIONS BASED ON BINOMIAL VALUED NUMBER

A.A. Borisenko, T.A. Protasova, E.A. Protasova

In this paper we propose an algorithm for constructing compositions based on the binomial number system with a multi-valued alphabet, a proof of the binomial transition function of a composition, consider an example block diagram of the proposed algorithm and the direct conversion of the functional diagram of the shaper compositions. The proposed structure, as well as a device based on it have a high noise immunity and flexibility, and use this as a shaper of the intermediate multi-valued binomial number system greatly increases the speed of change.

Keywords: *combinatorial configurations, valued binomial codes, cryptography, combinations, permutation, composition, binomial number system.*