УДК 681.142

ОБОБЩЁННЫЕ МУЛЬТИКАНАЛЬНЫЙ АЛГОРИТМ И ПОЗИЦИОННАЯ СИСТЕМА СЧИСЛЕНИЯ

А.Н. Лаврёнов
Институт современных знаний имени А.М. Широкова, Минск
E-mail: lanin99@mail.ru

Система счисления – система счёта или совокупность правил по упорядочиванию (перечислению) объектов, а также способов их представления с помощью некоторого конечного множества символов. История человечества показала возможность существование символической, непозиционной и позиционной систем счисления. Однако в практической деятельности только последняя доказала свою наибольшую результативность и получила широкое распространение. Само название позиционной системы счисления (ПСС) указывает на то, что значение (значимость) каждого разряда, представленного неким символом, зависит от его положения.

Пусть исходное множество объектов A разделено на n подмножеств A_n, т. е. на языке множеств это выразим так

$$A = \sum_n A_n .$$

В каждом A_n его элементы упорядочены с помощью алфавита α_n, и их общее количество или мощность алфавита α_n есть $P(\alpha_n) = p_n$. Следовательно, любой набор X элементов множества A можно записать следующим образом:

$$\{X\} = \sum_{m=1}^{m=n} \alpha_m A_m \equiv \alpha_n \alpha_{n-1} \dots \alpha_m \dots \alpha_2 \alpha_1 .$$

Назовём такую конструкцию обобщённой позиционной системой счисления (ОПСС). Если в качестве A_m рассматривать соответственно b^m, $m!$, $F_k(m)$ или C_{n-1}^m, то получим степенную с основанием b, факториальную, k-фибоначчиевую и биномиальную ПСС. В качестве своего примера ОПСС предложим в роли основания деформированные k- обобщенные матрицы Фибоначчи $Q_k = \begin{bmatrix} \vec{c} & c_k \\ I_{k-1} & 0 \end{bmatrix}$, где $\vec{c} = diag(c_1, c_2, \dots c_{k-1})$ и c_k - параметры деформации.

Из вышеприведенного построения ОПСС ясно, что мощность P_A множества A равна сумме мощностей P_{A_n} подмножеств A_n, т. е. $P_A \equiv \sum_{m=1}^{m=n} P_{A_m}$. Данный факт разложения P_A на слагаемые P_{A_n} можно использовать для классификации ОПСС.

Также, если установить изоморфизм между элементами n- разрядной ОПСС и элементами l-разрядных ОПСС ($1 \le l \le n$), то можно ввести обобщенный мультиканальный алгоритм. В виду того, что в общем случае $P_{A_i} \ne P_{A_j}$, то имеются запрещенные комбинации и (или) множественное представление числа. Последнее улучшает диффузионные характеристики обобщенного мультиканального алгоритма и служит дополнительным барьером по защите информации от несанкционированного доступа.