УДК 621.391.251

И.А. Кулик, А.А. Борисенко, С.В. Костель

Сумской государственный университет, Сумы

ЗАЩИТА ИНФОРМАЦИИ НА ОСНОВЕ БИНОМИАЛЬНЫХ ЧИСЕЛ

Введение

На сегодняшний день существует множество методов защиты информации. Каждый из методов характеризуется своими особенностями и, следовательно, своей сферой применения. Среди этих методов существует особый класс методов, основой которых является защита информации на основе сжатия.

Любое сжатие информации представляет в определенной мере и защиту от несанкционированного доступа. При сжатии реализуется функция преобразования F: X→Y, где X представляет исходное множество сообщений, а Y – множество, в которое они преобразуются под воздействием алгоритма преобразования, представляющего собой алгоритм их сжатия. В процессе сжатия устраняется избыточность, связанная с неравномерным распределением вероятностей элементов исходной информации. Эта особенность затрудняет взлом зашифрованных данных и в большинстве случаев единственным способом дешифровки будет последовательный перебор всех возможных состояний [1].

Особый интерес для данного класса методов защиты на основе сжатия представляют методы нумерационного кодирования [2]. В частности предлагается использовать сжатие при помощи биномиальных чисел. Основой метода сжатия является биномиальная система счисления.

Биномиальная система счисления

Биномиальными системами счисления называются позиционные системы счисления с биномиальными коэффициентами в качестве оснований [3]. В предлагаемом методе защиты на основе сжатия используется линейная биномиальная система счисления с двоичным алфавитом.

Числовая функция и системы кодообразующих ограничений имеют следующий вид

$$F = x_{r-1}C_{n-1}^{k-q_{r-1}} + \ldots + x_i C_{n-r+i}^{k-q_i} + \ldots + x_1 C_{n-r-1}^{k-q_1} + x_0 C_{n-r}^{k-q_0};$$

$$\begin{cases} k \le r \le n-1; \\ q = k; \\ x_0 = 1 \end{cases} \quad \text{и} \quad \begin{cases} n-k = r-q; \\ 0 \le q \le k-1; \\ x_0 = 0, \end{cases}$$

где r – количество разрядов биномиального числа (длина), $r \in 1, 2, \ldots$; k – максимальное количество единиц q_{max} в биномиальном числе; i – порядковый номер разряда, $i = 0, 1, \ldots, r-1$; x_i – биномиальная двоичная цифра – 0 или 1; n – целочисленный параметр системы счисления; q – число единиц в биномиальном числе; q_i – сумма единичных значений цифр x_i от (r – 1)-го разряда до (i + 1)-го включительно:

$$q_i = \sum_{j=i+1}^{r} x_j, \qquad i = 0, 1, \ldots, r-1; \; x_r = 0.$$

Множество всех двоичных чисел длины n можно представить в виде суммы биномиальных коэффициентов

$$2^n = \sum_{i=0}^{n} C_n^i .$$

Важным свойством биномиальных систем счисления является то, что они могут каждое двоичное число преобразовать в биномиальное и далее в соответствующий ему двоичный номер.

Алгоритм работы метода защиты

Алгоритм защиты на основе сжатия с использованием линейных биномиальных чисел с двоичным алфавитом состоит из следующих операций:

1. Считывание двоичной последовательности определенной длинны n из массива исходных данных.
2. Подсчет количества единиц k двоичной последовательности.
3. Преобразование двоичной кодовой комбинации в биномиальный код. Эта операция состоит в отбрасывании в двоичной комбинации единиц справа до первого появления нуля или отбрасывании нулей справа до первой единицы.
4. Переход от биномиального числа к его порядковому номеру в биномиальной системе счисления с параметрами n и k. Чтоб осуществить переход к порядковому номеру необходимо произвести расчет кодообразующей функции. Суть расчета состоит в нахождении значений биномиальных коэффициентов с определенными индексами и их последующем сложении.

При кодировании множества двоичных последовательностей параметр n (количество бит обрабатываемых за один цикл работы алгоритма) устанавливается либо как постоянная величина, заложенная внутри кодирующего и декодирующего устройства, либо подбирается для каждого шифруемого пакета информации.

Выводы

В результате выполнения алгоритма защиты на основе сжатия с использованием биномиальных чисел обычный вероятностный источник информации преобразуется в два взаимозависимых источника информации – вероятностный источник ключей и комбинаторный источник равновероятных номеров сообщений. Последний несет в себе зашифрованную информацию о передаваемых сообщениях, а первый – о ключах к каждому из этих сообщений [4].

Так как комбинаторный источник генерирует номера с равной вероятностью, то в нем отсутствует избыточная информация и для дешифрации может быть использован простой перебор. При больших значениях n дешифрация при помощи перебора становится затруднительной.

Вся избыточность исходных сообщений в данном случае находится в вероятностном источнике ключей. Для его защиты может быть использован любой существующий метод шифровки данных. Однако при этом количество шифруемых данных будет значительно меньше, чем в случае кодирования обычных двоичных сообщений. Поэтому и защита их будет более эффективной.

При этом следует учесть, что при кодировании происходит сжатие информации, а значит, необходимо меньше памяти для её хранения и уменьшается время передачи зашифрованной информации по каналу связи. Кроме того, шифруется только малая часть передаваемой информации (источник ключей), следовательно, процесс шифрования будет проходить быстрей, чем при шифровании всей исходной информации.

Все эти достоинства позволяют говорить о высокой потенциальной эффективности метода защиты информации на основе сжатия с использованием биномиальных чисел.

Список литературы

1. Борисенко А.А. Защита информации на основе сжатия / А.А. Борисенко // Вестник СумГУ. – 2006. – № 4. – С. 53-55.

2. Амелькин В.А. Методы нумерационного кодирования / В.А. Амелькин. – Новосибирск: Наука, 1986. – 155 с.

3. Борисенко А.А. Биномиальный счет. Теория и практика: монография / А.А. Борисенко. – Сумы: Университетская книга, 2004. – 170 с.

4. Борисенко А.А. О разложении бернуллиевских источников информации / А.А. Борисенко // Вестник СумГУ. – 1995. – № 3. – С. 57-59.