УДК 681.325.5

О СВОЙСТВАХ ДВОИЧНЫХ МАТРИЦ, ИСПОЛЬЗУЕМЫХ В АЛГОРИТМАХ КОДИРОВАНИЯ ИНФОРМАЦИИ БУЛЕВЫМИ ПРЕОБРАЗОВАНИЯМИ

А. Б. Бубликов,
аспирант
Санкт-Петербургский государственный университет аэрокосмического приборостроения

Формулируются требования к свойствам двоичных матриц, используемых для кодирования потоковой информации на основе булевых преобразований.

Requirements to properties of the binary matrixes used for coding of stream information with boolean transformations are formulated.

Введение

Основные положения использования двоичных матриц для защиты информации или ее передачи со скрытым смыслом рассмотрены в работе [1]. Дальнейшим развитием идеи кодирования информации на основе булевых преобразований является модификация, ориентированная на использование двоичных матриц с ненулевым определителем в поле Галуа GF(2).

В данной работе анализируются некоторые особенности двоичных матриц, полученных с помощью метода, описанного в работе [2]. Метод генерации ключевых двоичных квадратных матриц с заданными свойствами дает две матрицы – ключевую (обозначим ее через K) и матрицу K^{-1}, такую, что $KK^{-1} = E$, где E – единичная матрица. Одновременно с указанными матрицами вычисляется порядок некоммутативной группы, порождаемой матрицей K.

Особенности алгоритма кодирования

Предложенный в работе [1] алгоритм кодирования информации на основе булевых преобразований не является симметричным в общем смысле этого слова – повторное кодирование полученной информации с тем же ключом не приведет к ее декодированию. В рассматриваемой реализации кодирование осуществляется посредством матрицы K^{-1}, а декодирование – с использованием матрицы K. Однако следует отметить, что алгоритм симметричен относительно ключевой матрицы. Это значит, что абсолютно не важно, какая из матриц будет участвовать в процессе кодирования информации, поскольку процесс декодирования будет производиться с помощью второй матрицы. Эта особенность алгоритма приводит к тому, что выдвигаемые требования к качеству ключевой матрицы K должны быть справедливыми и для матрицы K^{-1}.

Рассмотрим некоторые особенности алгоритма. В общем случае в алгоритме, производящем операции над блоками информации, представляющими собой двумерный массив элементов кодируемой информации, слово может иметь длину m бит. Основная операция алгоритма – перемножение двух матриц: матрицы K^{-1} (K при декодировании) и очередного блока информации. Все операции производятся в поле Галуа GF(2). Размерность блока информации должна соответствовать размерности n ключевой матрицы. Для упрощения анализа ограничимся длиной слова, равной 8 битам, и, соответственно, размерностью матриц (8×8).

Проведем анализ матриц K и K^{-1}, полученных предложенным в работе [2] методом, и результатов их использования при кодировании.

$$K = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \end{bmatrix};$$

$$K^{-1} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

Порядок некоммутативной группы, порождаемой матрицей K, равен 41, что является неплохим результатом для выбранной размерности матрицы и длины блока информации.

В обеих матрицах K и K^{-1} имеется по две строки, содержащие всего по одной единице.

Результат кодирования информации с использованием полученных матриц приведен ниже.

Исходная информации	Кодированная информация
Введите пароль:	пароль: №_Ccr~~iПи(
vikivikivikivikivikivikivikiviki	§
Номер матрицы: 1	§
1 1	Я
0 1	1 1 мамсяъм'бк<
Размер матрицы: 2×2	Чматрицы:М¤Ьс"уНЙнЦьЗ_Лкаца:
	1 1

Из приведенного примера видно, что именно наличие в матрице строк с одной единицей не позволяет кодировать все символы исходного текста.

Указанные особенности алгоритма и полученные результаты преобразования позволяют сформулировать некоторые очевидные требования к ключевой матрице и размеру блоков информации.

1. Ключевая матрица K и матрица K^{-1} должны содержать в своем составе равное количество единиц и нулей (достаточное условие) и не должны содержать строк и столбцов, в которых имеется только одна единица (необходимое условие). Преобладание в каждой строке ключевой матрицы единиц или наличие в строке только одной единицы приводят к тому, что при кодировании элементарное слово из состава очередного блока информации останется неизменным, поскольку операция перемножения матриц выполняется по модулю 2.

2. Размер блока информации L в байтах, вычисляемый как $L = m \times n^2 / 8$, зависит от длины (в битах) элементарного блока информации m, значение которого желательно иметь не кратным восьми, и размерности ключевой матрицы n, которую для улучшения качества кодирования рекомендуется выбирать как можно большей. Однако, поскольку алгоритм оперирует только полным блоком информации, это часто требует увеличения размера исходной информации до значения, кратного размеру блока L за счет дополнительной «незначащей информации».

3. Порядок некоммутативной группы, порождаемой ключевой матрицей K, должен быть по возможности большим, поскольку этот параметр отвечает за стойкость алгоритма к атакам типа «перебор». На этапе получения ключевой матрицы методом, предложенным в работе [2], это возможно заданием конкретного значения указанного параметра.

Выводы

Исходя из описанных выше требований и ограничений, налагаемых на ключевую матрицу и сам алгоритм, можно сделать выводы о целесообразности его применения для кодирования разных типов информации.

По типу информация, поступающая на кодирование, делится на потоковую и не потоковую. Применение алгоритма к потоковой информации позволит избежать недостатка, заключающегося в необходимости расширения последнего кодируемого блока до необходимого размера, за счет подбора необходимого сочетания параметров n и m для точного соответствия значению L.

Исходя из особенностей алгоритма, не рекомендуется применять алгоритм к информационному потоку, имеющему регулярную структуру и повторяющиеся фрагменты, при условии, что длина фрагмента меньше размерности ключевой матрицы. Несоответствие этому требованию приведет к тому, что все элементы одного или нескольких блоков информации будут одинаковы и, следовательно, не будут закодированы.

Таким образом, алгоритм наиболее подходит для кодирования двоичной аудио- и видеоинформации, особенно в потоковой реализации, и не применим для кодирования текстовой информации, имеющей много пробелов и регулярных структур.

Литература

1. **Ерош И. Л.** Разграничение доступа к ресурсам в системах коллективного пользования // Информационно-управляющие системы. – 2003. – № 2–3. – С. 63–66.
2. **Бубликов А. Б.** Методы получения двоичных матриц с заданными свойствами для использования в алгоритмах защиты информации на основе булевых преобразований / Седьмая научная сессия аспирантов ГУАП: Сб. докл.: В 2 ч. – Ч. I. Технические науки. – СПбГУАП, 2004. – С. 253–254.