А. М. Коренева

ПРИМЕНЕНИЕ ТЕОРЕТИКО-ГРАФОВОГО ПОДХОДА ДЛЯ ОПРЕДЕЛЕНИЯ ЗНАЧЕНИЯ ЭКСПОНЕНТА МАТРИЦЫ СУЩЕСТВЕННОЙ ЗАВИСИМОСТИ

Объектом исследования в статье является класс перемешивающих графов и соответствующих матриц, иначе говоря, матриц и графов существенной зависимости. При помощи таких моделей изучают перемешивающие свойства преобразований [1].

Важной характеристикой перемешивающих свойств системы преобразований является экспонент системы соответствующих графов преобразований.

Экспонент квадратной неотрицательной матрицы M (обозначим $\exp M$) — это наименьшее натуральное t (если такое t существует), при котором матрица M^t положительна:

$$\exp M = \min\{t: M^t > 0\}.$$

Экспонентом класса примитивных матриц называется минимальная степень, такая, что все матрицы класса в этой степени имеют только положительные элементы [2].

В работе предложен алгоритм, согласно которому можно получить значение экспонента матрицы существенной зависимости (МСЗ). Также приведено значение экспонента, полученное в ходе проведения тестирования алгоритма на примере итеративного СБШ *DES*.

Для рассматриваемого алгоритма шифрования процесс оценки значения экспонента МСЗ состоит из нескольких этапов.

На первом этапе необходимо выделить множество «элементарных» преобразований, которые составляют основу циклового преобразования. Под «элементарным» преобразованием данной работе понимается преобразование, реализуемое базовыми элементами криптографической схемы.

Затем для каждого из «элементарных» преобразований проводится анализ множества существенных переменных. На основании полученного множества существенных переменных для каждого преобразования осуществляется построение МСЗ.

Если преобразования перемножаются, т. е. выполняются последовательно друг за другом, то результирующая матрица является произведением двух матриц перемножаемых преобразований. Т. е. если преобразование $f(x) = h(g(x))$, то МСЗ M_f преобразования f вычисляется по формуле $M_f = M_g * M_h$, где матрицы M_g и M_h являются МСЗ для преобразований g и h соответственно.

В случае если преобразования выполняются параллельно, то необходимо совершать компоновку общей матрицы (нечто вроде присоединения матриц подходящего размера) по правилам построения соответствующей цикловой функции.

Далее, получив МСЗ для одного цикла преобразования, необходимо вычислить экспонент полученной матрицы. Матрица возводится в степень до тех пор, пока она не станет положительна. Значение степени, при которой МСЗ стала положительной, является значением экспонента для данной матрицы.

Блок-схема разработанного алгоритма представлена на рис. 1.

Цикловое преобразование, как правило, не является совершенным, но многократное его применение (подразумевается произведение цикловых преобразований) обеспечивает полное перемешивание — существенную зависимость каждой координатной функции выходного вектора от всех переменных. Значение экспонента МСЗ циклового преобразования покажет минимально допустимое число циклов шифрования, при осуществлении которых общее преобразование зашифрования становится совершенным и, следовательно, исключает возможность применения к нему атаки, основанной на методе последовательного опробования элементов ключа.

В соответствии с предложенным алгоритмом, построим МСЗ для преобразования шифрования *DES* в режиме простой замены.

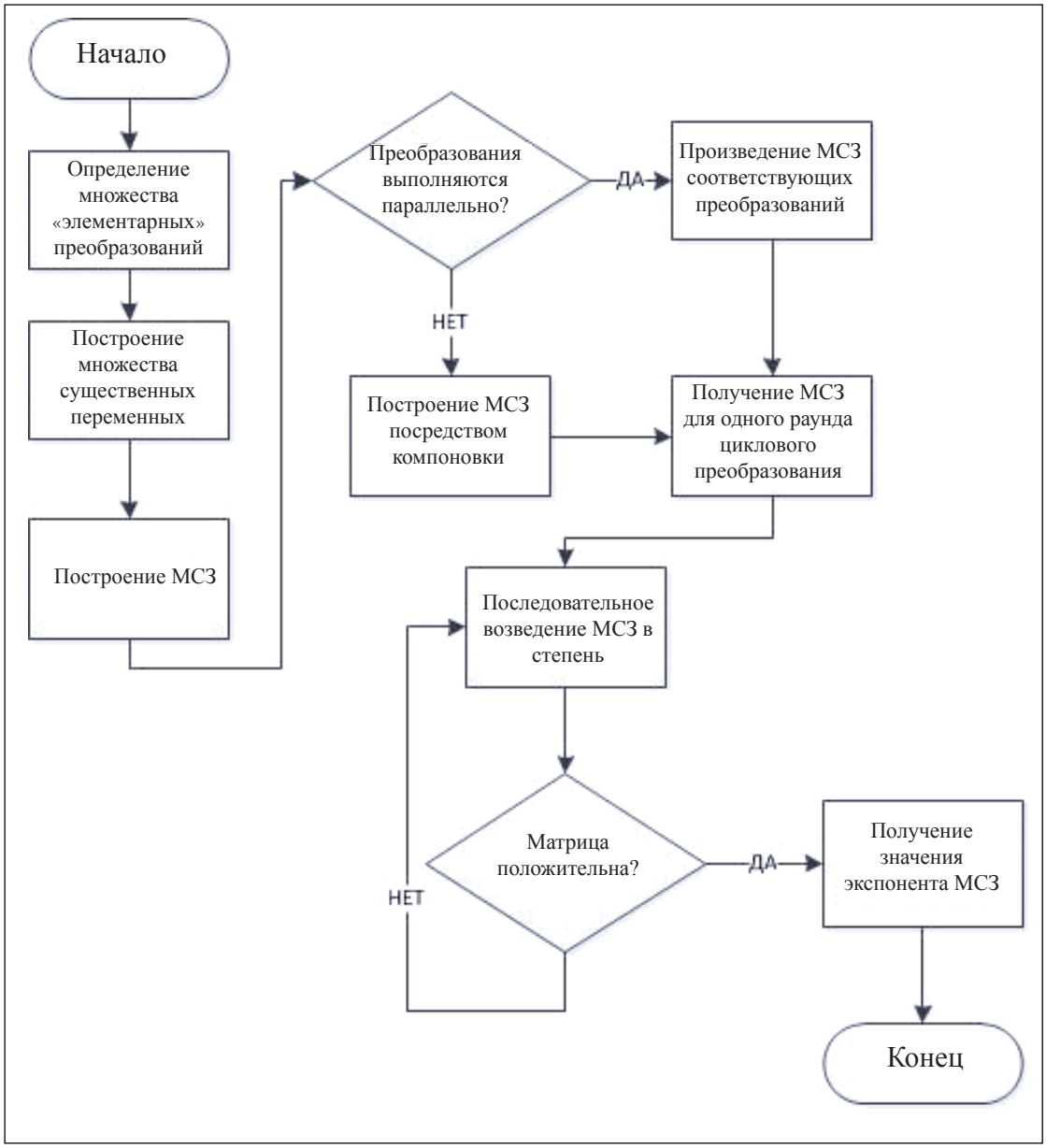

Рис. 1. Блок-схема разработанного алгоритма

На первом этапе необходимо выделить преобразования, которые являются «элементарными». Для каждого из выделенных преобразований построить перемешивающие матрицы. Сформировать МСЗ в соответствии с правилами построения цикловой функции для *DES*.

Первый цикл зашифрования реализуется над блоком открытого текста размером 64 бита. Открытый текст делится на 2 части по 32 бита каждая (обозначим X_1 и X_2), над которыми осуществляются преобразования зашифрования.

Среди преобразований алгоритма шифрования *DES* наибольший интерес с точки зрения исследования существенной зависимости представляют преобразования функции усложнения. При построении МСЗ рассматривались следующие преобразования:

- расширение 32-битового вектора X_2 до 48-битового вектора;
- подмешивание 48-битового циклового ключа q путем XOR-суммирования;
- нелинейная замена с помощью s-боксов 48-битового вектора на 32-битовый вектор;
- перемешивание координат 32-битового вектора с помощью перестановки P.

Для каждого из рассмотренных преобразований, посредством исследования существенной зависимости каждой координатной функции от переменных, были построены МСЗ.

В соответствии с правилами построения цикловой функции, была получена результирующая МСЗ *DES* (размер 64x64). По главной диагонали матрицы расположены блок из нулевых элементов (32x32) и МСЗ функции усложнения (32x32). По побочной диагонали расположены блоки, представляющие собой единичные матрицы размером 32x32.

В результате тестирования было получено значение экспонента МСЗ *DES*, равное 5. Следовательно, композиция 5 цикловых преобразований *DES* обеспечивает полное перемешивание — существенную зависимость каждой выходной координатной функции от всех переменных, т. е. реализует совершенное преобразование.

Данное значение согласовано с известными результатами для алгоритма *DES* [3], что увеличивает глубину обоснованности полученного результата.

СПИСОК ЛИТЕРАТУРЫ:

1. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. — 424 с.
2. *Сачков В. Н., Ошкин И. Б.* Экспоненты классов неотрицательных матриц // Дискретная математика. 1993. № 2 (5). С. 150–159.
3. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Пер. с англ. М.: Издательство ТРИУМФ, 2003. — 816 с.