УДК 004.056.55

Моделирование алгебраической структуры шифра AES с использованием цепных дробей

Ю. И. Горбенко, А. А. Кузнецов, С. В. Костенко
Харьковский национальный университет имени В.Н. Каразина, Украина

В данной работе с использованием математического аппарата цепных дробей исследуется алгебраическая структура шифра AES. Приводится краткое описание шифра AES (FIPS-197), рассматриваются основные преобразования, используемые в этом крипто алгоритме, и его алгебраическая структура. С использованием полиномиального описания вводится алгебраическая форма нелинейного узла замен шифра, позволяющая существенно упростить систему уравнений, связывающих значения открытого текста, секретного ключа и полученного шифр-текста.

Ключевые слова: *цепные дроби, алгебраическая структура, шифр-текст.*

В даній роботі з використанням математичного апарату ланцюгових дробів досліджується алгебраїчна структура шифру AES. Приводиться короткий опис шифру AES (FIPS-197), розглядаються основні перетворення, які використовуються в цьому крипто алгоритмі, та його алгебраїчна структура. З використанням поліноміального опису вводиться алгебраїчна форма нелінійного вузла замін шифру, яка дозволяє суттєво спростити систему рівнянь, які зв'язують значення відкритого тексту, таємного ключа та отриманого шифр-текста.

Ключові слова: *ланцюгові дроби, алгебраїчна структура, шифр-текст.*

In the paper, the algebraic structure of cipher AES is studied using the mathematical apparatus of continued fractions. Provided here brief description of the cipher AES (FIPS-197) covers the basic transformations used in this cryptographic algorithm and its algebraic structure. Polynomial description of the Algebraic form of nonlinear input node substitutions cipher greatly simplifies the system of equations connecting the values of the plaintext, the secret key and the resulting cipher text.

Key words:*continued fraction, algebraic structure, cipher text.*

1. Введение

В качестве стандарта шифрования по результатам открытого конкурса AES, проведенного Национальным институтом стандартов и технологий США в 1997-2001 г.г. был принят Advanced Encryption Standard (AES) - симметричный алгоритм блочного шифрования (размер блока 128 бит, размер ключа 128/192/256 бит) [1 - 3]. Целью данной работы является анализ алгебраической структуры шифра AES, т.е. вывод алгебраических уравнений, связывающих значения открытого текста, секретного ключа и полученного шифр-текста. При этом предлагается использовать математический аппарат цепных дробей.

2. Краткое описание алгоритма шифрования

Конкурс AES проводился Национальным институтом стандартов и технологий США в 1997-2001 г.г. и победителем объявлен алгоритм Rijndael (Рэндал) [1 - 3]. Фактически шифр AES, стандартизированный в FIPS-197, представляет собой один из вариантов алгоритма Rijndael.

Различные преобразования в алгоритме Rijndael (AES) оперируют с промежуточным результатом, называемым *Состояние* (State). Состояние может быть изображено как прямоугольный массив байтов. Этот массив имеет 4 строки, количество столбцов обозначается через *Nb* и равно длине блока, деленной на 32 (для AES используется *Nb* = 4). Ключ шифра также изображается как прямоугольный массив с 4 строками. Количество столбцов Ключа шифра обозначается через *Nk* и равно длине ключа, деленной на 32 (для AES используется *Nk* = 4, 6 или 8).

Вход и выход, используемые в Rijndael в его внешнем интерфейсе, являются одноразмерными массивами 8-битных байтов, пронумерованных в восходящем порядке от 0 до $4 \cdot Nb - 1$. Эти блоки поэтому имеют длины 16, 14 и 32 байт и индексы массивов в пределах 0..15, 0..23, 0..31.

Ключ шифра рассматривается как одноразмерные массивы 8-битных байтов, пронумерованные в восходящем порядке от 0 до $4 \cdot Nk - 1$. Эти блоки поэтому имеют длины 16, 24 и 32 байт и индексы массивов в пределах 0..15, 0..23, 0..31.

Входные байты шифра («открытый текст», если используется режим зашифровывания ECB) отображаются в байты состояния в порядке $a_{0,0}, a_{1,0}, a_{2,0}, a_{3,0}, a_{0,1}, a_{1,1}, a_{2,1}, a_{3,1}, a_{4,1} \ldots$, и байты ключа шифра отображаются в массив в порядке $k_{0,0}, k_{1,0}, k_{2,0}, k_{3,0}, k_{0,1}, k_{1,1}, k_{2,1}, k_{3,1}, k_{4,1} \ldots$ В конце оперирования шифра его выход извлекается из состояния выбором байтов состояния в таком же порядке.

Следовательно, если одноразмерным индексом байта в блоке является n, и двуразмерным индексом является (i,j), мы имеем:

$$i = n \bmod 4; \quad j = \lfloor n/4 \rfloor; \qquad n = i + 4 * j .$$

Далее, индекс i есть также номером байта в 4-байтном векторе или слове и j есть индекс вектора или слова в отдельно взятом блоке.

Количество раундов обозначено через *Nr* и зависит от значений *Nb* и *Nk*. Для шифра AES используются следующие параметры: *Nr* = 10 (при *Nk* = 4), *Nr* = 12 (при *Nk* = 6), *Nr* = 14 (при *Nk* = 8).

Раундовое преобразование состоит из четырех различных преобразований: *ByteSub(State); ShiftRow(State); MixColumn(State); AddRoundKey(State, RoundKey).* Последний раунд с удаленным шагом *MixColumn(State).* В этих обозначениях «функции» (Round, ByteSub, ShiftRow, …) оперируют с массивами, на которые указывают указатели (State, RoundKey).

Преобразование ByteSub есть нелинейной заменой байтов, которое оперирует с каждым байтом Состояния независимо. Таблица замена (или S-блок) инвертируема и создана композицией двух преобразований:

1. Вычисляется мультипликативно обратный элемент в поле $GF(2^8)$ (в полиномиальном представлении элементов поля операции производятся по модулю неприводимого бинарного многочлена $m(x) = x^8 + x^4 + x^3 + x + 1$), при этом элемент ‘00’ отображается в себя;

2. Применяется аффинное преобразование (над двоичным полем GF(2)), которое определено как:

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \quad (1)$$

Применение описанного S-блока ко всем байтам состояния обозначается как ByteSub(State). Обратным к ByteSub является замена байтов с применением инвертированной таблицы. Это достигается обращением аффинного отображения, за которым следует взятие мультипликативно обратного в поле $GF(2^8)$.

В ***преобразовании ShiftRow*** строки Состояния сдвигаются на различное количество позиций. Строка 0 не смещается, строка 1 смещается на C1 байт, строка 2 – на C2 байт и строка 3 – на C3 байт. Для шифра AES: C1 = 1, C2 = 2, C3 = 3. Операция сдвига строк Состояния на определенную величину обозначается через ShiftRow(State). Обратным к ShiftRow есть циклический сдвиг 3 нижних строк на *Nb* – C1, *Nb* – C2, *Nb* – C3, байт соответственно так, что байт на позиции *j* в строке *i* двигается на позицию (*j* + *Nb* – Ci) mod *Nb*.

В MixColumn столбцы Состояния рассматриваются как многочлены над полем $GF(2^8)$ и умножаются по модулю x^4+1 с фиксированным многочленом $c(x)$, заданным как $c(x) = '03'x^3 + '01'x^2 + '01'x + '02'$.

Этот многочлен является взаимно-простым с x^4+1 и поэтому инвертируемым. Это может быть записано как матричное умножение. Пусть $b(x) = c(x) \otimes a(x)$,

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

Применение этой операции ко всем столбцам Состояния обозначается через MixColumn(State). Инверсия преобразования MixColumn сходна к MixColumn. Каждый столбец преобразуется умножением его на особый многочлен *d(x)*, определенный через $\left('03'x^3 + '01'x^2 + '01'x + '02'\right) \otimes d(x) = '01'$.

Он задан таким образом:

$$d(x) = '0B'x^3 + '0D'x^2 + '09'x + '0E'.$$

Сложение с раундовым ключом. В этой операции к Состоянию применяется RoundKey простым побитным сложением по модулю 2. Раундовый ключ

производится из ключа шифра посредством процедуры формирования ключей. Длина раундового ключа равна длине блока *Nb*. Преобразование, которое состоит из побитового сложения Состояния и раундового ключа обозначается через AddRoundKey(State,RoundKey) оно является своей собственной инверсией.

Процедура формирования ключей. Раундовые ключи производятся из ключа шифра посредством процедуры формирования ключей. Она включает в себя два компонента: Расширение ключа и Выбор раундового ключа. Основной принцип заключается в следующем:

- общее количество бит раундового ключа равно длине блока, умноженной на количество раундов плюс 1 (т.е. для блока длины 128 бит и 10 раундов необходимо 1408 раундовых ключей);
- Ключ шифра расширяется в Расширенный ключ;
- раундовые ключи берутся из Расширенного ключа следующим образом: первый раундовый ключ состоит из первых *Nb* слов, второй – из следующих *Nb* слов, и так далее.

Расширенный ключ есть линейный массив 4-байтных слов и обозначается как *W[Nb*(Nr+1)]*. Первые *Nk* слов содержат Ключ шифра. Все другие слова определяются рекурсивно по величинам слов с меньшими индексами. Функция Расширения ключа зависит от величины *Nk*: есть версия для *Nk* меньше или равно 6, и есть версия для *Nk* больше 6.

Для $Nk \le 6$ расширенный ключ формируется по следующему правилу:

*W[i] = (Key[4*i],Key[4*i+1], Key[4*i+2],Key[4*i+3]), i = 0, …, Nk – 1;*

*W[i] = W[i - Nk] ^ temp, i = Nk, …, Nb * (Nr + 1) – 1,*

при этом если *(i)mod(Nk)=0*:

temp = SubByte(RotByte(temp)) ^ Rcon[i / Nk],

если *(i)mod(Nk)≠0*:

temp = W[i - 1].

В этом представлении *SubByte(W)* есть функция, которая возвращает 4-байтовое слово, в котором каждый байт есть результат применения S-блока к байту на соответствующей позиции во входном слове. Функция *RotByte(W)* возвращает слово, в котором байты являются циклической перестановкой байтов на входе таким образом, что входное слово (a, b, c, d) продуцируется в выходное слово (b, c, d, a).

Таким образом, первые *Nk* слов заполнены Ключом шифра. Каждое следующее слово *W[i]* равно сумме по модулю 2 с предыдущим словом *W[i–1]* и словом, расположенным на *Nk* позиций ранее *W[i–Nk]*. Для слов с позициями, кратными *Nk*, перед сложением по модулю 2 к слову *W[i–1]* применяется преобразование и прибавляется по модулю 2 раундовая константа. Это преобразование состоит из циклического сдвига байт с слове (*RotByte*), за которым следует применение табличного поиска ко всем 4 байтам слова (*SubByte*).

Отличием при формировании расширенного ключа $Nk > 6$ есть то, что для *i*–4, кратного *Nk*, перед сложением по модулю 2 к W[i–1] применяется SubByte.

Раундовые константы не зависят от *Nk* и определены как:

$$\mathrm{Rcon}[i] = \left(\mathrm{RC}[i], '00', '00', '00'\right),$$

где RC[i] представляют собой элемент поля GF(2^8) со значением $x^{(i-1)}$, такой, что

$$\mathrm{RC}[1] = 1 \ \ (\text{i.e.}\,'01')$$
$$\mathrm{RC}[i] = \mathrm{x} \ \ (\text{i.e.}\,'02') \bullet \left(\mathrm{RC}[i-1]\right) = x^{(i-1)}.$$

Выбор раундового ключа. Раундовый ключ i задан буфером слов раундового ключа от *W[Nb*i]* до *W[Nb*(i+1)]*.

Шифр Rijndael состоит из:

- Начального добавления раундового ключа
- $Nr - 1$ раундов
- Окончательного раунда.

Аспекты реализации. Шифр Rijndael приспособлен для эффективной реализации на широком спектре процессоров и специализированном аппаратном обеспечении. В частности, для 32-х битной платформы различные шаги раундового преобразования могут быть скомбинированы в единственный набор (множество) выборочных таблиц, приводящих к быстрой реализации на процессорах с длиной слова 32 или выше.

Выразим один столбец выхода раунда e в величинах байт входа раунда a (значением $a_{i,j}$ обозначим байт в строке i и столбце j, значением a_j обозначим столбец j Состояния a). Для прибавления ключей и для преобразования MixColumn получим:

$$\begin{bmatrix} e_{0,j} \\ e_{1,j} \\ e_{2,j} \\ e_{3,j} \end{bmatrix} = \begin{bmatrix} d_{0,j} \\ d_{1,j} \\ d_{2,j} \\ d_{3,j} \end{bmatrix} \oplus \begin{bmatrix} k_{0,j} \\ k_{1,j} \\ k_{2,j} \\ k_{3,j} \end{bmatrix} \ and \ \begin{bmatrix} d_{0,j} \\ d_{1,j} \\ d_{2,j} \\ d_{3,j} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} c_{0,j} \\ c_{1,j} \\ c_{2,j} \\ c_{3,j} \end{bmatrix}.$$

Для преобразований ShiftRow и ByteSub имеем:

$$\begin{bmatrix} c_{0,j} \\ c_{1,j} \\ c_{2,j} \\ c_{3,j} \end{bmatrix} = \begin{bmatrix} b_{0,j} \\ b_{1,j+C1} \\ b_{2,j+C2} \\ b_{3,j+C3} \end{bmatrix} \ and \ b_{i,j} = \mathrm{S}\left[a_{i,j}\right].$$

В последнем выражении индексы столбцов должны быть взяты по модулю Nb. Сгруппировав выражения, приведенные выше, получим:

$$\begin{bmatrix} e_{0,j} \\ e_{1,j} \\ e_{2,j} \\ e_{3,j} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} \mathrm{S}\left[a_{0,j}\right] \\ \mathrm{S}\left[a_{1,j+C1}\right] \\ \mathrm{S}\left[a_{2,j+C2}\right] \\ \mathrm{S}\left[a_{3,j+C3}\right] \end{bmatrix} \oplus \begin{bmatrix} k_{0,j} \\ k_{1,j} \\ k_{2,j} \\ k_{3,j} \end{bmatrix}.$$

Матричное умножение выразим как линейную комбинацию векторов:

$$\begin{bmatrix} e_{0,j} \\ e_{1,j} \\ e_{2,j} \\ e_{3,j} \end{bmatrix} = \mathrm{S}\left[a_{0,j}\right]\begin{bmatrix} 02 \\ 01 \\ 01 \\ 03 \end{bmatrix} \oplus \mathrm{S}\left[a_{1,j+C1}\right]\begin{bmatrix} 03 \\ 02 \\ 01 \\ 01 \end{bmatrix} \oplus \mathrm{S}\left[a_{2,j+C2}\right]\begin{bmatrix} 01 \\ 03 \\ 02 \\ 01 \end{bmatrix} \oplus \mathrm{S}\left[a_{3,j+C3}\right]\begin{bmatrix} 01 \\ 01 \\ 03 \\ 02 \end{bmatrix} \oplus \begin{bmatrix} k_{0,j} \\ k_{1,j} \\ k_{2,j} \\ k_{3,j} \end{bmatrix}$$

Множители $\mathrm{S}[a_{i,j}]$ четырех векторов получены составлением выборочной таблицы на входах байтах $a_{i,j}$ в таблице S-блока S[256].

Определим 4 таблицы с 256-ю вводами 4-байтовых слов от T_0 до T_3:

$$\mathrm{T}_0[a] = \begin{bmatrix} \mathrm{S}[a] \bullet 02 \\ \mathrm{S}[a] \\ \mathrm{S}[a] \\ \mathrm{S}[a] \bullet 03 \end{bmatrix} \quad \mathrm{T}_1[a] = \begin{bmatrix} \mathrm{S}[a] \bullet 03 \\ \mathrm{S}[a] \bullet 02 \\ \mathrm{S}[a] \\ \mathrm{S}[a] \end{bmatrix}$$

$$\mathrm{T}_2[a] = \begin{bmatrix} \mathrm{S}[a] \\ \mathrm{S}[a] \bullet 03 \\ \mathrm{S}[a] \bullet 02 \\ \mathrm{S}[a] \end{bmatrix} \quad \mathrm{T}_3[a] = \begin{bmatrix} \mathrm{S}[a] \\ \mathrm{S}[a] \\ \mathrm{S}[a] \bullet 03 \\ \mathrm{S}[a] \bullet 02 \end{bmatrix}.$$

Эти 4 таблицы занимают до 4 Кбайт памяти, с их использованием раундовое преобразование может быть выражено в виде:

$$e_j = \mathrm{T}_0\left[a_{0,j}\right] \oplus \mathrm{T}_1\left[a_{1,j+C1}\right] \oplus \mathrm{T}_2\left[a_{2,j+C2}\right] \oplus \mathrm{T}_3\left[a_{3,j+C3}\right] \oplus k_j . \qquad (2)$$

Следовательно, реализация выборочных таблиц с 4 Кбайтами памяти требует только 4 сложения по модулю 2 на столбец каждого раунда.

Можно заметить, что $\mathrm{T}_i[a]$ = RotByte($\mathrm{T}_{i-1}[a]$). Тогда заплатив тремя дополнительными ротациями на столбец в каждом раунде реализация шифра может быть выполнена с одной таблицей, общим размером в 1 Кбайт памяти:

$$e_j = k_j \oplus \mathrm{T}_0\left[b_{0,j}\right] \oplus$$
$$\oplus \texttt{Rotbyte}\left(\mathrm{T}_0\left[b_{1,j+C1}\right] \oplus \texttt{Rotbyte}\left(\mathrm{T}_0\left[b_{2,j+C2}\right] \oplus \texttt{Rotbyte}\left(\mathrm{T}_0\left[b_{3,j+C3}\right]\right)\right)\right)$$

Т.к. в последнем раунде нет операции MixColumn, взамен Т-таблиц должна быть использована S-таблица.

3. Алгебраическая структура шифра

Рассмотрим алгебраическую структуру шифра. При этом ограничимся исследованием шифра AES с $Nk = 4$, т.е. будем рассматривать Rijndael с длиной ключа и длиной блока в 128 бит, значения Состояния и Ключа шифра представляются в виде таблиц 4×4. Число раундов преобразования $Nr = 10$.

Целью проводимых исследований является анализ алгебраической структуры шифра, т.е. вывод алгебраических уравнений, связывающих значения открытого текста, секретного ключа и полученного шифр-текста. Для удобства дальнейших вычислений обозначим байты Состояния и Ключа шифра на выходе каждого *u* –го раунда (*u = 1, 2, ..., 10*) верхним индексом, т.е. в виде $a_{i,j}^{u}$ и $k_{i,j}^{u}$. Начальное значение Состояния (открытый текст до шифрования) обозначим в виде массива $a_{i,j}^{0}$. Значения $a_{i,j}^{10}$ Состояния на 10-м раунде будут соответствовать байтам полученного шифр-текста.

Байты секретного ключа, в соответствии с приведенным выше правилом формирования раундовых ключей, будут записаны в массив значений $k_{i,j}^{1}$ Ключа шифра (на первом раунде):

$k_{0,0}^{1}$	$k_{0,1}^{1}$	$k_{0,2}^{1}$	$k_{0,3}^{1}$
$k_{1,0}^{1}$	$k_{1,1}^{1}$	$k_{1,2}^{1}$	$k_{1,3}^{1}$
$k_{2,0}^{1}$	$k_{2,1}^{1}$	$k_{2,2}^{1}$	$k_{2,3}^{1}$
$k_{3,0}^{1}$	$k_{3,1}^{1}$	$k_{3,2}^{1}$	$k_{3,3}^{1}$

Выразим алгебраическую зависимость значений $a_{i,j}^{1}$ Состояния (после первого раунда шифрования) от значений $a_{i,j}^{0}$ Состояния (байт открытого текста) и значений $k_{i,j}^{1}$ Ключа шифра. Используя (2) для всех $j = 0, ..., 3$ имеем [4]:

$$a_{0,j}^{1} = '02' S[a_{0,j}^{0}] \oplus '03' S[a_{1,j+1}^{0}] \oplus S[a_{2,j+2}^{0}] \oplus S[a_{3,j+3}^{0}] \oplus k_{0,j}^{1};$$

$$a_{1,j}^{1} = S[a_{0,j}^{0}] \oplus '02' S[a_{1,j+1}^{0}] \oplus '03' S[a_{2,j+2}^{0}] \oplus S[a_{3,j+3}^{0}] \oplus k_{1,j}^{1};$$

$$a_{2,j}^{1} = S[a_{0,j}^{0}] \oplus S[a_{1,j+1}^{0}] \oplus '02' S[a_{2,j+2}^{0}] \oplus '03' S[a_{3,j+3}^{0}] \oplus k_{2,j}^{1};$$

$$a_{3,j}^{1} = '03' S[a_{0,j}^{0}] \oplus S[a_{1,j+1}^{0}] \oplus S[a_{2,j+2}^{0}] \oplus '02' S[a_{3,j+3}^{0}] \oplus k_{3,j}^{1},$$

где индексы приводятся по модулю 4.

Рассмотрим алгебраическую структуру S-блока шифра AES.

В работе [5] показано, что с помощью интерполяции можно получить следующую алгебраическую форму:

$$S[x] = '63' + '8F' x^{127} + 'B5' x^{191} + '01' x^{223} + 'F4' x^{239} + '25' x^{247} + \\ + 'F9' x^{251} + '09' x^{253} + '05' x^{254}, \quad (3)$$

которая, однако, сложна для вывода окончательных выражений, связывающих секретных ключ, открытый и закрытый текст.

В работе [6] используется следующая форма представления S-блока:

$$S[x] = w_8 + \sum_{d=0}^{7} w_d x^{255-2^d}, \quad (4)$$

для некоторых констант $w_0,...,w_8$, что также приводит к чрезвычайно громоздким окончательным выражениям.

Некоторое развитие представление (4) получило в статье [7].

В данной работе предлагается иная алгебраическая форма представления S-блока шифра AES, которая, как будет показано ниже, значительно упрощает вывод итоговых уравнений.

Рассмотрим выражение (1). Воспользуемся полиномиальным представлением элементов конечных полей для описания алгебраической структуры S-блока. Для этого вход представим в виде многочлена $a(x) \in GF(2^8)$, его мультипликативно обратный элемент (по модулю $m(x)$) в поэлементной записи формально запишем в виде:

$$\frac{1}{a(x)} = b(x) = b_0 + b_1 x + ... + b_7 x^7,$$

где коэффициенты $b_0,..., b_7$ определяют значения вектора-столбца в произведении (1), т.е.

$$\begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} = \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix}.$$

С помощью подстановки получим следующее выражение:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \end{bmatrix} = \begin{bmatrix} b_0 + b_4 + b_5 + b_6 + b_7 \\ b_0 + b_1 + b_5 + b_6 + b_7 \\ b_0 + b_1 + b_2 + b_6 + b_7 \\ b_0 + b_1 + b_2 + b_3 + b_7 \\ b_0 + b_1 + b_2 + b_3 + b_4 \\ b_1 + b_2 + b_3 + b_4 + b_5 \\ b_2 + b_3 + b_4 + b_5 + b_6 \\ b_3 + b_4 + b_5 + b_6 + b_7 \end{bmatrix} + \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \end{bmatrix} =$$

$$= \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} b_7 \\ b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \end{bmatrix} + \begin{bmatrix} b_6 \\ b_7 \\ b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \end{bmatrix} + \begin{bmatrix} b_5 \\ b_6 \\ b_7 \\ b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \end{bmatrix} + \begin{bmatrix} b_4 \\ b_5 \\ b_6 \\ b_7 \\ b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} + \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \end{bmatrix}.$$

Сумму пяти векторов-столбцов в правой части выражения запишем в полиномиальном виде (с операциями умножения по модулю $x^8 + 1$), получим:

$$S[a(x)] = b(x) + xb(x) + x^2 b(x) + x^3 b(x) + x^4 b(x) + c(x) =$$
$$= (1 + x + x^2 + x^3 + x^4)b(x) + c(x) = \frac{'1F'}{a(x)} + c(x). \quad (5)$$

Полученная алгебраическая форма (5) является наиболее простым из известных выражений, например, по сравнению с (3) и (4). Фактически, выражение (5) устанавливает наиболее простой (из известных автору) способ вычисления S-блока шифра AES – для каждого входного элемента достаточно вычислить мультипликативно обратный и умножить полученный результат на константу (по модулю $x^8 + 1$) и сложить с константой. Для удобства в дальнейших вычислениях будем использовать форму $S[a] = \frac{1}{a}$, подразумевая под этой записью вычисление мультиптикативно обратного в поле $GF(2^8)$ с умножением полученного результата на многочлен $1 + x + x^2 + x^3 + x^4$ (по модулю $x^8 + 1$) и сложения с константой.

Воспользуемся выражением (5) (в форме $S[a] = \frac{1}{a}$) для построения системы алгебраических уравнений, описывающих **первый раунд шифрования**:

$$a^1_{0,j} = A^0_{0,j} \oplus k^1_{0,j};\ a^1_{1,j} = A^0_{1,j} \oplus k^1_{1,j};\ a^1_{2,j} = A^0_{2,j} \oplus k^1_{2,j};\ a^1_{3,j} = A^0_{3,j} \oplus k^1_{3,j}, \quad (6)$$

где:

$$A^0_{0,j} = \frac{'02'}{a^0_{0,j}} \oplus \frac{'03'}{a^0_{1,j+1}} \oplus \frac{1}{a^0_{2,j+2}} \oplus \frac{1}{a^0_{3,j+3}},$$

$$A^0_{1,j} = \frac{1}{a^0_{0,j}} \oplus \frac{'02'}{a^0_{1,j+1}} \oplus \frac{'03'}{a^0_{2,j+2}} \oplus \frac{1}{a^0_{3,j+3}},$$

$$A^0_{2,j} = \frac{1}{a^0_{0,j}} \oplus \frac{1}{a^0_{1,j+1}} \oplus \frac{'02'}{a^0_{2,j+2}} \oplus \frac{'03'}{a^0_{3,j+3}},$$

$$A^0_{3,j} = \frac{'03'}{a^0_{0,j}} \oplus \frac{1}{a^0_{1,j+1}} \oplus \frac{1}{a^0_{2,j+2}} \oplus \frac{'02'}{a^0_{3,j+3}}.$$

Из этой линейной системы неизвестные байты секретного ключа $k^1_{0,j}$, $k^1_{1,j}$, $k^1_{2,j}$ и $k^1_{3,j}$ выражаются линейной комбинацией байт шифр-текста и инвертированных (в конечном поле) байт открытого текста. Для вычисления одного байта секретного ключа необходимо выполнить 4 инверсии, 2 умножения, 5 сложения в конечном поле $GF(2^8)$ и 4 умножения на многочлен $1 + x + x^2 + x^3 + x^4$ по модулю $x^8 + 1$.

Для второго раунда система уравнений будет иметь вид:

$$a^2_{0,j} = A^1_{0,j} \oplus k^2_{0,j};\ a^2_{1,j} = A^1_{1,j} \oplus k^2_{1,j};\ a^2_{2,j} = A^1_{2,j} \oplus k^2_{2,j};\ a^2_{3,j} = A^1_{3,j} \oplus k^2_{3,j}, \quad (7)$$

где:

$$A^1_{0,j} = \frac{'02'}{A^0_{0,j} \oplus k^1_{0,j}} \oplus \frac{'03'}{A^0_{1,j+1} \oplus k^1_{1,j+1}} \oplus \frac{1}{A^0_{2,j+2} \oplus k^1_{2,j+2}} \oplus \frac{1}{A^0_{3,j+3} \oplus k^1_{3,j+3}},$$

$$A^1_{1,j} = \frac{1}{A^0_{0,j} \oplus k^1_{0,j}} \oplus \frac{'02'}{A^0_{1,j+1} \oplus k^1_{1,j+1}} \oplus \frac{'03'}{A^0_{2,j+2} \oplus k^1_{2,j+2}} \oplus \frac{1}{A^0_{3,j+3} \oplus k^1_{3,j+3}},$$

$$A^1_{2,j} = \frac{1}{A^0_{0,j} \oplus k^1_{0,j}} \oplus \frac{1}{A^0_{1,j+1} \oplus k^1_{1,j+1}} \oplus \frac{'02'}{A^0_{2,j+2} \oplus k^1_{2,j+2}} \oplus \frac{'03'}{A^0_{3,j+3} \oplus k^1_{3,j+3}},$$

$$A^1_{3,j} = \frac{'03'}{A^0_{0,j} \oplus k^1_{0,j}} \oplus \frac{1}{A^0_{1,j+1} \oplus k^1_{1,j+1}} \oplus \frac{1}{A^0_{2,j+2} \oplus k^1_{2,j+2}} \oplus \frac{'02'}{A^0_{3,j+3} \oplus k^1_{3,j+3}}.$$

В системе (7) в качестве неизвестных переменных выступают байты секретного ключа $k^1_{0,j}$, $k^1_{1,j+1}$, $k^1_{2,j+2}$ и $k^1_{3,j+3}$, а также байты раундовых ключей $k^2_{0,j}$, $k^2_{1,j}$, $k^2_{2,j}$ и $k^2_{3,j}$. Выразим раундовые ключи (для второго раунда) в виде алгебраических уравнений от секретных ключей шифра (от ключей первого раунда):

$$k^2_{0,0} = k^1_{0,0} \oplus \mathrm{S}[k^1_{1,3}] \oplus '01' = k^1_{0,0} \oplus '01' \oplus \frac{1}{k^1_{1,3}};\ k^2_{1,0} = k^1_{1,0} \oplus \mathrm{S}[k^1_{2,3}] = k^1_{1,0} \oplus \frac{1}{k^1_{2,3}};$$

$$k^2_{2,0} = k^1_{2,0} \oplus \mathrm{S}[k^1_{3,3}] = k^1_{2,0} \oplus \frac{1}{k^1_{3,3}};\ k^2_{3,0} = k^1_{3,0} \oplus \mathrm{S}[k^1_{0,3}] = k^1_{3,0} \oplus \frac{1}{k^1_{0,3}};$$

$$k^2_{0,1} = k^1_{0,1} \oplus k^2_{0,0} = k^1_{0,1} \oplus k^1_{0,0} \oplus '01' \oplus \frac{1}{k^1_{1,3}};\ k^2_{1,1} = k^1_{1,1} \oplus k^2_{1,0} = k^1_{1,1} \oplus k^1_{1,0} \oplus \frac{1}{k^1_{2,3}};$$

$$k^2_{2,1} = k^1_{2,1} \oplus k^2_{2,0} = k^1_{2,1} \oplus k^1_{2,0} \oplus \frac{1}{k^1_{3,3}};\ k^2_{3,1} = k^1_{3,1} \oplus k^2_{3,0} = k^1_{3,1} \oplus k^1_{3,0} \frac{1}{k^1_{0,3}};$$

$$k^2_{0,2} = k^1_{0,2} \oplus k^2_{0,1} = k^1_{0,2} \oplus k^1_{0,1} \oplus k^1_{0,0} \oplus '01' \oplus \frac{1}{k^1_{1,3}};$$

$$k^2_{1,2} = k^1_{1,2} \oplus k^2_{1,1} = k^1_{1,2} \oplus k^1_{1,1} \oplus k^1_{1,0} \oplus \frac{1}{k^1_{3,2}};\ k^2_{2,2} = k^1_{2,2} \oplus k^2_{2,1} = k^1_{2,2} \oplus k^1_{2,1} \oplus k^1_{2,0} \oplus \frac{1}{k^1_{3,3}};$$

$$k^2_{3,2} = k^1_{3,2} \oplus k^2_{3,1} = k^1_{3,2} \oplus k^1_{3,1} \oplus k^1_{3,0} \oplus \frac{1}{k^1_{3,0}};$$

$$k^2_{0,3} = k^1_{0,3} \oplus k^2_{0,2} = k^1_{0,3} \oplus k^1_{0,2} \oplus k^1_{0,1} \oplus k^1_{0,0} \oplus '01' \oplus \frac{1}{k^1_{3,1}};$$

$$k^2_{1,3} = k^1_{1,3} \oplus k^2_{1,2} = k^1_{1,3} \oplus k^1_{1,2} \oplus k^1_{1,1} \oplus k^1_{1,0} \oplus \frac{1}{k^1_{2,3}};$$

$$k^2_{2,3} = k^1_{2,3} \oplus k^2_{2,2} = k^1_{2,3} \oplus k^1_{2,2} \oplus k^1_{2,1} \oplus k^1_{2,0} \oplus \frac{1}{k^1_{3,3}};$$

$$k^2_{3,3} = k^1_{3,3} \oplus k^2_{3,2} = k^1_{3,3} \oplus k^1_{3,2} \oplus k^1_{3,1} \oplus k^1_{3,0} \oplus \frac{1}{k^1_{0,3}};.$$

С учетом последних обозначений формулы (7) примут вид:

$$a^2_{0,j} = A^1_{0,j} \oplus \frac{1}{k^1_{1,3}} \oplus '01' \bigoplus_{w=0}^{j} k^1_{0,w};\ a^2_{1,j} = A^1_{1,j} \oplus \frac{1}{k^1_{2,3}} \bigoplus_{w=0}^{j} k^1_{1,w};$$

$$a^2_{2,j} = A^1_{2,j} \oplus \frac{1}{k^1_{3,3}} \bigoplus_{w=0}^{j} k^1_{2,w};\ a^2_{3,j} = A^1_{3,j} \oplus \frac{1}{k^1_{0,3}} \bigoplus_{w=0}^{j} k^1_{3,w}.$$

Таким образом, значения секретного ключа, открытого и закрытого текста после двух раундов шифрования связаны системой из 16 уравнений от 16 неизвестных. Каждое уравнение содержит от 4 до 8 неизвестных (в зависимости от значения индекса j).

На третьем раунде система уравнений будет иметь вид:

$$a^3_{0,j} = A^2_{0,j} \oplus k^3_{0,j};\ a^3_{1,j} = A^2_{1,j} \oplus k^3_{1,j};\ a^3_{2,j} = A^2_{2,j} \oplus k^3_{2,j};\ a^3_{3,j} = A^2_{3,j} \oplus k^3_{3,j},\ (8)$$

где:

$$A^2_{0,j} = \frac{'02'}{A^1_{0,j} \oplus k^2_{0,j}} \oplus \frac{'03'}{A^1_{1,j+1} \oplus k^2_{1,j+1}} \oplus \frac{1}{A^1_{2,j+2} \oplus k^2_{2,j+2}} \oplus \frac{1}{A^1_{3,j+3} \oplus k^2_{3,j+3}},$$

$$A^2_{1,j} = \frac{1}{A^1_{0,j} \oplus k^2_{0,j}} \oplus \frac{'02'}{A^1_{1,j+1} \oplus k^2_{1,j+1}} \oplus \frac{'03'}{A^1_{2,j+2} \oplus k^2_{2,j+2}} \oplus \frac{1}{A^1_{3,j+3} \oplus k^2_{3,j+3}},$$

$$A^2_{2,j} = \frac{1}{A^1_{0,j} \oplus k^2_{0,j}} \oplus \frac{1}{A^1_{1,j+1} \oplus k^2_{1,j+1}} \oplus \frac{'02'}{A^1_{2,j+2} \oplus k^2_{2,j+2}} \oplus \frac{'03'}{A^1_{3,j+3} \oplus k^2_{3,j+3}},$$

$$A^3_{3,j} = \frac{'03'}{A^1_{0,j} \oplus k^2_{0,j}} \oplus \frac{1}{A^1_{1,j+1} \oplus k^2_{1,j+1}} \oplus \frac{1}{A^1_{2,j+2} \oplus k^2_{2,j+2}} \oplus \frac{'02'}{A^1_{3,j+3} \oplus k^2_{3,j+3}}.$$

В системе (8) неизвестными являются байты раундовых ключей $k^2_{0,j}$, $k^2_{1,j+1}$, $k^2_{2,j+2}$, $k^2_{3,j+3}$, $k^3_{0,j}$, $k^3_{1,j}$, $k^3_{2,j}$ и $k^3_{3,j}$. Выше было показано, что $k^2_{0,j}$, $k^2_{1,j+1}$, $k^2_{2,j+2}$, $k^2_{3,j+3}$ выражаются в виде алгебраических уравнений от неизвестных байтов секретного ключа $k^1_{0,j}$, $k^1_{1,j+1}$, $k^1_{2,j+2}$ и $k^1_{3,j+3}$. Выразим по аналогии раундовые ключи третьего раунда $k^3_{0,j}$, $k^3_{1,j}$, $k^3_{2,j}$ и $k^3_{3,j}$:

$$k^3_{0,0} = k^2_{0,0} \oplus \mathrm{S}[k^2_{1,3}] \oplus '02' = k^1_{0,0} \oplus \frac{1}{k^1_{1,3}} \oplus \frac{1}{\bigoplus\limits_{w=0}^{3} k^1_{1,w} \oplus \frac{1}{k^1_{2,3}}} \oplus '03';$$

$$k^3_{1,0} = k^2_{1,0} \oplus \mathrm{S}[k^2_{2,3}] = k^1_{1,0} \oplus \frac{1}{k^1_{2,3}} \oplus \frac{1}{\bigoplus\limits_{w=0}^{3} k^1_{2,w} \oplus \frac{1}{k^1_{3,3}}};$$

$$k^3_{2,0} = k^2_{2,0} \oplus \mathrm{S}[k^2_{3,3}] = k^1_{2,0} \oplus \frac{1}{k^1_{3,3}} \oplus \frac{1}{\bigoplus\limits_{w=0}^{3} k^1_{3,w} \oplus \frac{1}{k^1_{0,3}}};$$

$$k^3_{3,0} = k^2_{3,0} \oplus \mathrm{S}[k^2_{0,3}] = k^1_{3,0} \oplus \frac{1}{k^1_{0,3}} \oplus \frac{1}{\bigoplus\limits_{w=0}^{3} k^1_{0,w} \oplus \frac{1}{k^1_{3,1}} \oplus '01'};$$

$$k^3_{0,1} = k^2_{0,1} \oplus k^3_{0,0} = k^1_{0,1} \oplus \frac{1}{\bigoplus\limits_{w=0}^{3} k^1_{1,w} \oplus \frac{1}{k^1_{2,3}}} \oplus '02';$$

$$k^3_{1,1} = k^2_{1,1} \oplus k^3_{1,0} = k^1_{1,1} \oplus \frac{1}{\bigoplus\limits_{w=0}^{3} k^1_{2,w} \oplus \frac{1}{k^1_{3,3}}};$$

$$k^3_{2,1} = k^2_{2,1} \oplus k^3_{2,0} = k^1_{2,1} \oplus \mathrm{S}[\bigoplus_{w=0}^{3} k^1_{3,w}] = k^1_{2,1} \oplus \frac{1}{\bigoplus\limits_{w=0}^{3} k^1_{3,w} \oplus \frac{1}{k^1_{0,3}}};$$

$$k_{3,1}^3 = k_{3,1}^2 \oplus k_{3,0}^3 = k_{3,1}^1 \oplus \frac{1}{\bigoplus\limits_{w=0}^{3} k_{0,w}^1 \oplus \frac{1}{k_{3,1}^1} \oplus '01'};$$

$$k_{0,2}^3 = k_{0,2}^2 \oplus k_{0,1}^3 = k_{0,2}^1 \oplus k_{0,0}^1 \oplus \frac{1}{k_{1,3}^1} \oplus \frac{1}{\bigoplus\limits_{w=0}^{3} k_{1,w}^1 \oplus \frac{1}{k_{2,3}^1}} \oplus '03';$$

$$k_{1,2}^3 = k_{1,2}^2 \oplus k_{1,1}^3 = k_{1,2}^1 \oplus k_{1,0}^1 \oplus \frac{1}{k_{3,2}^1} \oplus \frac{1}{\bigoplus\limits_{w=0}^{3} k_{2,w}^1 \oplus \frac{1}{k_{3,3}^1}};$$

$$k_{2,2}^3 = k_{2,2}^2 \oplus k_{2,1}^3 = k_{2,2}^1 \oplus k_{2,0}^1 \oplus \frac{1}{k_{3,3}^1} \oplus \frac{1}{\bigoplus\limits_{w=0}^{3} k_{3,w}^1 \oplus \frac{1}{k_{0,3}^1}};$$

$$k_{3,2}^3 = k_{3,2}^2 \oplus k_{3,1}^3 = k_{3,1}^1 \oplus k_{3,0}^1 \oplus \frac{1}{k_{3,0}^1} \oplus \frac{1}{\bigoplus\limits_{w=0}^{3} k_{0,w}^1 \oplus \frac{1}{k_{3,1}^1} \oplus '01'};$$

$$k_{0,3}^3 = k_{0,3}^2 \oplus k_{0,2}^3 = k_{0,3}^1 \oplus k_{0,1}^1 \oplus \frac{1}{k_{3,1}^1} \oplus \frac{1}{k_{1,3}^1} \oplus \frac{1}{\bigoplus\limits_{w=0}^{3} k_{1,w}^1 \oplus \frac{1}{k_{2,3}^1}} \oplus '02';$$

$$k_{1,3}^3 = k_{1,3}^2 \oplus k_{1,2}^3 = k_{1,3}^1 \oplus k_{1,1}^1 \oplus \frac{1}{k_{2,3}^1} \oplus \frac{1}{k_{3,2}^1} \oplus \frac{1}{\bigoplus\limits_{w=0}^{3} k_{2,w}^1 \oplus \frac{1}{k_{3,3}^1}};$$

$$k_{2,3}^3 = k_{2,3}^2 \oplus k_{2,2}^3 = k_{2,3}^1 \oplus k_{2,1}^1 \oplus \frac{1}{\bigoplus\limits_{w=0}^{3} k_{3,w}^1 \oplus \frac{1}{k_{0,3}^1}};$$

$$k_{3,3}^3 = k_{3,3}^2 \oplus k_{3,2}^3 = k_{3,3}^1 \oplus k_{3,1}^1 \oplus \frac{1}{k_{0,3}^1} \oplus \frac{1}{k_{3,0}^1} \oplus \frac{1}{\bigoplus\limits_{w=0}^{3} k_{0,w}^1 \oplus \frac{1}{k_{3,1}^1} \oplus '01'}.$$

Выражение (8) связывает значения секретного ключа, открытого и закрытого текста после трех раундов шифрования системой из 16 алгебраических уравнений от 16 неизвестных.

Обобщим полученные выражения на большее число раундов.

На *i*-ом раунде система уравнений, связывающих значения секретного ключа, открытого и закрытого текста, будет иметь вид:

$$a_{0,j}^i = A_{0,j}^{i-1} \oplus k_{0,j}^i;\ a_{1,j}^i = A_{1,j}^{i-1} \oplus k_{1,j}^i;\ a_{2,j}^i = A_{2,j}^{i-1} \oplus k_{2,j}^i;\ a_{3,j}^i = A_{3,j}^{i-1} \oplus k_{3,j}^i, \quad (9)$$

где:

$$A_{0,j}^i = \frac{'02'}{A_{0,j}^{i-1} \oplus k_{0,j}^i} \oplus \frac{'03'}{A_{1,j+1}^{i-1} \oplus k_{1,j+1}^i} \oplus \frac{1}{A_{2,j+2}^{i-1} \oplus k_{2,j+2}^i} \oplus \frac{1}{A_{3,j+3}^{i-1} \oplus k_{3,j+3}^i},$$

$$A^i_{1,j} = \frac{1}{A^{i-1}_{0,j} \oplus k^i_{0,j}} \oplus \frac{'02'}{A^{i-1}_{1,j+1} \oplus k^i_{1,j+1}} \oplus \frac{'03'}{A^{i-1}_{2,j+2} \oplus k^i_{2,j+2}} \oplus \frac{1}{A^{i-1}_{3,j+3} \oplus k^i_{3,j+3}},$$

$$A^i_{2,j} = \frac{1}{A^{i-1}_{0,j} \oplus k^i_{0,j}} \oplus \frac{1}{A^{i-1}_{1,j+1} \oplus k^i_{1,j+1}} \oplus \frac{'02'}{A^{i-1}_{2,j+2} \oplus k^i_{2,j+2}} \oplus \frac{'03'}{A^{i-1}_{3,j+3} \oplus k^i_{3,j+3}},$$

$$A^i_{3,j} = \frac{'03'}{A^{i-1}_{0,j} \oplus k^i_{0,j}} \oplus \frac{1}{A^{i-1}_{1,j+1} \oplus k^i_{1,j+1}} \oplus \frac{1}{A^{i-1}_{2,j+2} \oplus k^i_{2,j+2}} \oplus \frac{'02'}{A^{i-1}_{3,j+3} \oplus k^i_{3,j+3}}.$$

Значения раундовых ключей (на четвертом раунде) выражаются следующими уравнениями:

$$k^4_{0,0} = k^3_{0,0} \oplus \mathrm{S}[k^3_{1,3}] \oplus '04' =$$

$$= k^1_{0,0} \oplus \frac{1}{k^1_{1,3}} \oplus \frac{1}{\bigoplus\limits_{w=0}^{3} k^1_{1,w} \oplus \frac{1}{k^1_{2,3}}} \oplus \frac{1}{k^1_{1,3} \oplus k^1_{1,1} \oplus \frac{1}{k^1_{2,3}} \oplus \frac{1}{k^1_{3,2}} \oplus \frac{1}{\bigoplus\limits_{w=0}^{3} k^1_{2,w} \oplus \frac{1}{k^1_{3,3}}}} \oplus '07';$$

$$k^4_{1,0} = k^3_{1,0} \oplus \mathrm{S}[k^3_{2,3}] = k^1_{1,0} \oplus \frac{1}{k^1_{2,3}} \oplus \frac{1}{\bigoplus\limits_{w=0}^{3} k^1_{2,w} \oplus \frac{1}{k^1_{3,3}}} \oplus \frac{1}{k^1_{2,3} \oplus k^1_{2,1} \oplus \frac{1}{\bigoplus\limits_{w=0}^{3} k^1_{3,w} \oplus \frac{1}{k^1_{0,3}}}};$$

$$k^4_{2,0} = k^3_{2,0} \oplus \mathrm{S}[k^3_{3,3}] =$$

$$= k^1_{2,0} \oplus \frac{1}{k^1_{3,3}} \oplus \frac{1}{\bigoplus\limits_{w=0}^{3} k^1_{3,w} \oplus \frac{1}{k^1_{0,3}}} \oplus \frac{1}{k^1_{3,3} \oplus k^1_{3,1} \oplus \frac{1}{k^1_{0,3}} \oplus \frac{1}{k^1_{3,0}} \oplus \frac{1}{\bigoplus\limits_{w=0}^{3} k^1_{0,w} \oplus \frac{1}{k^1_{3,1}}} \oplus '01'};$$

$$k^4_{3,0} = k^3_{3,0} \oplus \mathrm{S}[k^3_{0,3}] =$$

$$= k^1_{3,0} \oplus \frac{1}{k^1_{0,3}} \oplus \frac{1}{\bigoplus\limits_{w=0}^{3} k^1_{0,w} \oplus \mathrm{S}[k^1_{3,1}] \oplus '01'} \oplus \frac{1}{k^1_{0,3} \oplus k^1_{0,1} \oplus \frac{1}{k^1_{3,1}} \oplus \frac{1}{k^1_{1,3}} \oplus \frac{1}{\bigoplus\limits_{w=0}^{3} k^1_{1,w} \oplus \frac{1}{k^1_{2,3}}} \oplus '02'};$$

$$k^4_{0,1} = k^3_{0,1} \oplus k^4_{0,0} = k^1_{0,1} \oplus k^1_{0,0} \oplus \frac{1}{k^1_{1,3}} \oplus \frac{1}{k^1_{1,3} \oplus k^1_{1,1} \oplus \frac{1}{k^1_{2,3}} \oplus \frac{1}{k^1_{3,2}} \oplus \frac{1}{\bigoplus\limits_{w=0}^{3} k^1_{2,w} \oplus \frac{1}{k^1_{3,3}}}} \oplus '05';$$

$$k^4_{1,1} = k^3_{1,1} \oplus k^4_{1,0} = k^1_{1,1} \oplus k^1_{1,0} \oplus \frac{1}{k^1_{2,3}} \oplus \frac{1}{k^1_{2,3} \oplus k^1_{2,1} \oplus \frac{1}{\bigoplus\limits_{w=0}^{3} k^1_{3,w} \oplus \frac{1}{k^1_{0,3}}}};$$

$$k_{2,1}^4 = k_{2,1}^3 \oplus k_{2,0}^4 = k_{2,1}^1 \oplus k_{2,0}^1 \oplus \frac{1}{k_{3,3}^1} \oplus \frac{1}{k_{3,3}^1 \oplus k_{3,1}^1 \oplus \frac{1}{k_{0,3}^1} \oplus \frac{1}{k_{3,0}^1} \oplus \frac{1}{\bigoplus_{w=0}^{3} k_{0,w}^1 \oplus \frac{1}{k_{3,1}^1} \oplus '01'}};$$

$$k_{3,1}^4 = k_{3,1}^3 \oplus k_{3,0}^4 = k_{3,1}^1 \oplus k_{3,0}^1 \oplus \frac{1}{k_{0,3}^1} \oplus \frac{1}{k_{0,3}^1 \oplus k_{0,1}^1 \oplus \frac{1}{k_{3,1}^1} \oplus \frac{1}{k_{1,3}^1} \oplus \frac{1}{\bigoplus_{w=0}^{3} k_{1,w}^1 \oplus \frac{1}{k_{2,3}^1}} \oplus '02'};$$

$$k_{0,2}^4 = k_{0,2}^3 \oplus k_{0,1}^4 =$$

$$= k_{0,2}^1 \oplus \frac{1}{\bigoplus_{w=0}^{3} k_{1,w}^1 \oplus \frac{1}{k_{2,3}^1}} \oplus k_{0,1}^1 \oplus \frac{1}{k_{1,3}^1 \oplus k_{1,1}^1 \oplus \frac{1}{k_{2,3}^1} \oplus \frac{1}{k_{3,2}^1} \oplus \frac{1}{\bigoplus_{w=0}^{3} k_{2,w}^1 \oplus \frac{1}{k_{3,3}^1}}} \oplus '06';$$

$$k_{1,2}^4 = k_{1,2}^3 \oplus k_{1,1}^4 = k_{1,2}^1 \oplus \frac{1}{\bigoplus_{w=0}^{3} k_{2,w}^1 \oplus \frac{1}{k_{3,3}^1}} \oplus k_{1,1}^1 \oplus \frac{1}{k_{2,3}^1 \oplus k_{2,1}^1 \oplus \frac{1}{\bigoplus_{w=0}^{3} k_{3,w}^1 \oplus \frac{1}{k_{0,3}^1}}};$$

$$k_{2,2}^4 = k_{2,2}^3 \oplus k_{2,1}^4 =$$

$$= k_{2,2}^1 \oplus \frac{1}{\bigoplus_{w=0}^{3} k_{3,w}^1 \oplus \frac{1}{k_{0,3}^1}} \oplus k_{2,1}^1 \oplus \frac{1}{k_{3,3}^1 \oplus k_{3,1}^1 \oplus \frac{1}{k_{0,3}^1} \oplus \frac{1}{k_{3,0}^1} \oplus \frac{1}{\bigoplus_{w=0}^{3} k_{0,w}^1 \oplus \frac{1}{k_{3,1}^1} \oplus '01'}};$$

$$k_{3,2}^4 = k_{3,2}^3 \oplus k_{3,1}^4 =$$

$$= \frac{1}{\bigoplus_{w=0}^{3} k_{0,w}^1 \oplus \frac{1}{k_{3,1}^1} \oplus '01'} \oplus \frac{1}{k_{0,3}^1 \oplus k_{0,1}^1 \oplus \frac{1}{k_{3,1}^1} \oplus \frac{1}{k_{1,3}^1} \oplus \frac{1}{\bigoplus_{w=0}^{3} k_{1,w}^1 \oplus \frac{1}{k_{2,3}^1}} \oplus '02'};$$

$$k_{0,3}^4 = k_{0,3}^3 \oplus k_{0,2}^4 =$$

$$= k_{0,3}^1 \oplus k_{0,1}^1 \oplus \frac{1}{k_{3,1}^1} \oplus \frac{1}{k_{1,3}^1} \oplus k_{0,2}^1 \oplus k_{0,1}^1 \oplus \frac{1}{k_{1,3}^1 \oplus k_{1,1}^1 \oplus \frac{1}{k_{2,3}^1} \oplus \frac{1}{k_{3,2}^1} \oplus \frac{1}{\bigoplus_{w=0}^{3} k_{2,w}^1 \oplus \frac{1}{k_{3,3}^1}}} \oplus '04';$$

$$k_{1,3}^4 = k_{1,3}^3 \oplus k_{1,2}^4 = k_{1,3}^1 \oplus \frac{1}{k_{2,3}^1} \oplus \frac{1}{k_{3,2}^1} \oplus k_{1,2}^1 \oplus \frac{1}{k_{2,3}^1 \oplus k_{2,1}^1 \oplus \frac{1}{\bigoplus_{w=0}^{3} k_{3,w}^1 \oplus \frac{1}{k_{0,3}^1}}};$$

$$k_{2,3}^4 = k_{2,3}^3 \oplus k_{2,2}^4 = k_{2,3}^1 \oplus k_{2,2}^1 \oplus \frac{1}{k_{3,3}^1 \oplus k_{3,1}^1 \oplus \frac{1}{k_{0,3}^1} \oplus \frac{1}{k_{3,0}^1} \oplus \frac{1}{\bigoplus_{w=0}^{3} k_{0,w}^1 \oplus \frac{1}{k_{3,1}^1} \oplus '01'}};$$

$$k_{3,3}^4 = k_{3,3}^3 \oplus k_{3,2}^4 =$$

$$= k_{3,3}^1 \oplus k_{3,1}^1 \oplus \frac{1}{k_{0,3}^1} \oplus \frac{1}{k_{3,0}^1} \oplus \frac{1}{k_{0,3}^1 \oplus k_{0,1}^1 \oplus \frac{1}{k_{3,1}^1} \oplus \frac{1}{k_{1,3}^1} \oplus \frac{1}{\bigoplus_{w=0}^{3} k_{1,w}^1 \oplus \frac{1}{k_{2,3}^1}} \oplus '02'}.$$

Таким образом, в результате проведенных исследований получена алгебраических уравнений, связывающих значения открытого текста, секретного ключа и полученного шифр-текста. При этом был использован математический аппарат цепных дробей.

Для подтверждения корректности и достоверности полученных аналитических выражений в работе были проведены экспериментальные исследования, которые состояли в проверке полученных формул при перехвате разного количества крипто пар после осуществления следующего раунда. Экспериментально была проверена система уравнений (7), полученные результаты сведены в таблицу 1.

Табл. 1. – Число решений алгебраической системы уравнений (7)

Количество крипто пар	Число решений
1	4284867295
2	16771824
3	65291
4	267
5	1

Таким образом, при перехвате 5 крипто пар, существует только одно решение, которое удовлетворяет одновременно всем уравнениям системы (7). Эта оценка раскрывает сложность организации алгебраической атаки в виде числа пар «криптограмма-открытый текст», необходимых для однозначного восстановления секретного ключа шифрования.

4. Выводы

Проведенные исследования показали, что принятый в США национальный стандарт шифрования AES (FIPS-197) обладает специфической алгебраической структурой, которая может быть эффективно описана в терминах математического аппарата цепных дробей. В частности, удалось получить системы алгебраических уравнений (5-9), связывающих значения открытого текста, секретного ключа и полученного шифр-текста. Поиск неизвестных байтов ключа $k_{i,j}^u$ по известным байтам Состояния $a_{i,j}^u$ составляет задачу

криптографического анализа. В данном случае задача криптоанализа сведена к поиску решений системы нелинейных алгебраических уравнений.

Проведенные экспериментальные исследований подтвердили корректность аналитических выражений, кроме того, получена оценка сложности организации алгебраической атаки в виде числа пар «криптограмма-открытый текст», необходимых для однозначного восстановления секретного ключа шифрования. Перспективным направлением дальнейших исследований является разработка эффективных методов решения полученных систем нелинейных уравнений и их апробация на реальных тестовых примерах шифрования.

ЛИТЕРАТУРА

1. National Institute of Standards and Technology, “FIPS-197: Advanced Encryption Standard”, November 2001 [Электронный ресурс]. Режим доступа: http://csrc.nist.gov/publications/ fips/fips197/fips-197.pdf
2. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Монографія. Харків, ХНУРЕ, Форт, 2012 р., 1 та 2 видання, 868 с.
3. Есин В.И., Кузнецов А.А., Сорока Л.С. Безопасность информационных систем и технологий. Х.:ООО «ЭДЭНА», 2010. – 656с.
4. Кузнецов А.А., Иваненко Д.В., Костенко С.В. Алгебраическая структура шифра AES. Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку: збірник тез доповідей. – Х.: Академія ВВ МВС України. – 2014. – С. 22 - 24.
5. T. Jakobsen and L.R. Knudsen, "The interpolation attack on block ciphers," Fast Software Encryption, LNCS 1267, E. Biham, Ed., Springer-Verlag, 1997, pp. 28-40.
6. Joan Daemen and Vincent Rijmen. AES proposal: Rijndael. In AES Round 1 Technical Evaluation, CD-1: Documentation. NIST, August 1998. See http://www.esat.kuleuven.ac.be/~rijmen/rijndael/ or http://www.nist.gov/aes.
7. Niels Ferguson, Richard Schroeppel, and Doug Whiting A simple algebraic representation of Rijndael // Selected Areas in Cryptography, Proc. SAC 2001, Lecture Notes in Computer Science #2259. — Springer Verlag, 2001. — P. 103–111.

Надійшла – 14.05.2014.