ВЫЧИСЛЕНИЯ ОПРЕДЕЛИТЕЛЯ ЗАШИФРОВАННОЙ КВАДРАТНОЙ МАТРИЦЫ

@ М.Г. Бабенко, Н.Н. Кучеров
mgbabenko@ncfu.ru, nkuchеров@ncfu.ru

УДК 004.042

DOI: 10.33184/mnkuomsh2t-2021-10-06.57.

Задача вычисления определителя возникает при решении целого практических ряд задач. Однако вычисления определителя зашифрованной матрицы является вычислительно сложной задачей. Существующие на данный момент алгоритмы вычисления определителя зашифрованной квадратной матрицы приводят к частичной или полной кражи секретного ключа несанкционированным пользователем. В работе предлагаем два алгоритма вычисления определителя зашифрованной матрицы. Первый алгоритм основан на определении, он применим для матриц 2 и 3 порядка. Вторым алгоритм основан на модификации формулы дополнения по Шура, позволяющий уменьшить количество шагов по сравнению с первым алгоритмом.

Ключевые слова: вычисление определителя, шифрование, секретный ключ.

Calculating the determinant of an encrypted square matrix

The problem of calculating the determinant arises when solving a number of practical problems. However, computing the determinant of an encrypted matrix is computationally challenging. Moreover, the currently existing algorithms for calculating the determinant of an encrypted square matrix lead to partial or complete theft of the secret key by an unauthorized user. In this paper, we propose two algorithms for calculating the determinant of an encrypted matrix. The first algorithm is based on the definition applicable for matrices of orders 2 and 3. The second algorithm is based on modifying the Schur complement formula, making it possible to reduce the number of steps compared to the first algorithm.

Keywords: calculation of determinant, encryption, secret key.

Пусть задана квадратная матрица A для которой необходимо вычислить определитель.

Работа выполнена при финансовой поддержке РНФ (проект № 19-71-10033).

Бабенко Михаил Григорьевич, к.ф.-м.н., доцент, СКФУ (Ставрополь, Россия); Mikhail Babenko (North Caucasus Federal University, Stavropol, Russia)

Кучеров Николай Николаевич, к.т.н., СКФУ (Ставрополь, Россия); Nikolay Kuchеров (North Caucasus Federal University, Stavropol, Russia)

Определение [1]. Определителем квадратной матрицы $A = (a_{i,j})$, порядка n называется число

$$\det A = \sum_{k_1, k_2, \dots, k_n} \text{sign}(k_1, k_2, \dots, k_n) \cdot a_{1, k_1} \cdot a_{2, k_2} \cdots a_{n, k_n}$$

где знак перестановки $(k_1, k_2, \dots, k_n)$ обозначается через $\text{sign}(k_1, k_2, \dots, k_n)$.

Рассмотрим алгоритм вычисления определения, основанный на Определении 1, мы получим:

Алгоритм. Вычисления определителя зашифрованной квадратной матрицы $A_i(x) = (a_{i,j})$ порядка n по определению:

Input: Матрица A представленная в зашифрованном виде n -многочленами $A_i(x)$, где i -я строка матрицы A закодирована многочленом $A_i(x)$. Единичная матрица E порядка n , представленная в зашифрованном виде n многочленами $E_i(x)$, где i -я строка матрицы E закодирована многочленом $E_i(x)$.

Output: $A(x)$ – значение определителя $\det A$ в зашифрованном виде.

1. $Per = (1, 2, \dots, n)$
2. $A(x) = A_1(x) \otimes E_1(x)$
3. **For** $i = 2$ **to** n **do**:
 - (a) $a(x) = A_i(x) \otimes E_i(x)$
 - (b) $A(x) = A(x) \otimes a(x)$
4. **while** ($\text{nextPermutation}(Per)$):
 - (a) $S = \text{sign}(Per)$
 - (b) $Temp(x) = A_1(x) \otimes E_{Per_1}(x)$
 - (c) **For** $i = 2$ **to** n **do**:
 - i. $a(x) = A_i(x) \otimes E_{Per_i}(x)$
 - ii. $Temp(x) = Temp(x) \otimes a(x)$
 - (d) **IF** $S > 0$ **then** $A(x) = A(x) \oplus Temp(x)$ **else** $A(x) = A(x) \ominus Temp(x)$
5. **return**($A(x)$)

Функция $\text{nextPermutation}(Per)$ возвращает True в случае, если существует следующая перестановка в лексикографическом порядке, и False, если нет.

Если функция *nextPermutation(Per)* вернула True, то значение следующей в лексикографическом порядке перестановки будет записано в переменную Per. Оценим необходимое количество арифметических операций с зашифрованными числами: глубина умножений равна $2 \cdot n - 1$, количество сложений зашифрованных чисел $n! - 1$ (так как количество перестановок равно $n!$ [2]).

Литература

1. Винберг Э.Б. Курс алгебры: Электронное издание // М.: МЦНМО. – 2014.
2. Воеводин В.В., Кузнецов Ю.А. Матрицы и вычисления // М.: Наука. Главная редакция физико-математической литературы, 1984, 320 с.