УДК 004.9

МОЩНЫЕ ФРАКТАЛЬНЫЕ МАТРИЧНЫЕ МНОЖЕСТВА ДЛЯ РЕАЛИЗАЦИИ И СТОЙКОСТИ КРИПТОГРАФИЧЕСКОГО АЛГОРИТМА

Шенгелия София

Сухумский государственный университет

Аннотация

Целью работы является создание мощных матричных множеств высокого порядка для реализации алгоритма обмена ключами по открытому каналу связи. Эта задача связана с глобальной проблемой, поскольку нет другой односторонней функции (известной и признанной), которая имеет высокую эффективность по сравнению с односторонними функциями, используемыми в асимметричных алгоритмах Диффи – Хеллмана и RSA.

Abstract

The goal of the work is to construct a set of high order strong matrixes for an open channel key exchange matrix algorithm and create a quick one-way matrix function. This issue concerns a global problem as nowadays there is no other one-way function (known and recognized), which is quicker compared to the one-way functions used in Diffie-Hellman and RSA asymmetric algorithms.

Введение

Алгоритм представляет собой оригинальный криптографический подход, особенно надо отметить его быстродействие. Для стойкости и реализации криптографического алгоритма предлагаются мощные фрактальные матричные множества [1-5].

Алгоритм обмена ключами по открытому каналу связи

Для реализации однонаправленной матричной функции задается матрица A(n x n). Для простоты изложения, матрицы рассматриваются над полем GF(2). Матрица A представляет собой секретный параметр, выбранный случайным образом из множества Â высокой мощности; т.е. $A \in \hat{A}$, $v \in V_n$, где V_n - векторное пространство над GF(2) (v - открытый параметр). Тогда, однонаправленная матричная функция имеет следующий вид:

$$v A = u; \quad (1)$$

где

$u \in V_n$ и u – также открытый параметр.

Матричный алгоритм обмена ключами по открытому каналу осуществляется следующим образом:

- Алиса (случайно) выбирает матрицу $A_1(n \times n) \in \hat{A}$ и посылает Бобу вектор
$$u_1 = v A_1, \quad (2)$$
- Боб (случайно) выбирает матрицу $A_2(n \times n) \in \hat{A}$ и посылает Алисе вектор
$$u_2 = vA_2, \quad (3)$$

где α - n -размерный вектор (открытый), A_1 и A_2 суть (секретные) матричные ключи.

- Алиса вычисляет
$$k_1 = u_2 A_1. \quad (4)$$
- Боб вычисляет
$$k_2 = u_1 A_2, \quad (5)$$

где k_1 и k_2 секретные ключи. $k_1 = k_2 = k$ потому, что $k = v A_1 A_2 = v A_2 A_1$.

Построение исходных матриц размерности (n x n)

Исследования были проведены с использованием программного обеспечения. Мы изучили мощные матричные множества размерности n=400 (400x400).

Порядок e, для всех матриц, равен числу Мерсенна или максимально достигаемому значению (размерность матрицы n, максимальное значение $e = 2^n-1$). Исследования были проведены для фрактальных матричных структур (см. рис.1). Для каждой размерности $n > 1$ исходная матрица (n x n) должна генерировать либо максимальное число матриц (2^n -1), либо количество матриц, равное числу Мерсенна, т.е. 2^j -1, где $j<n$.

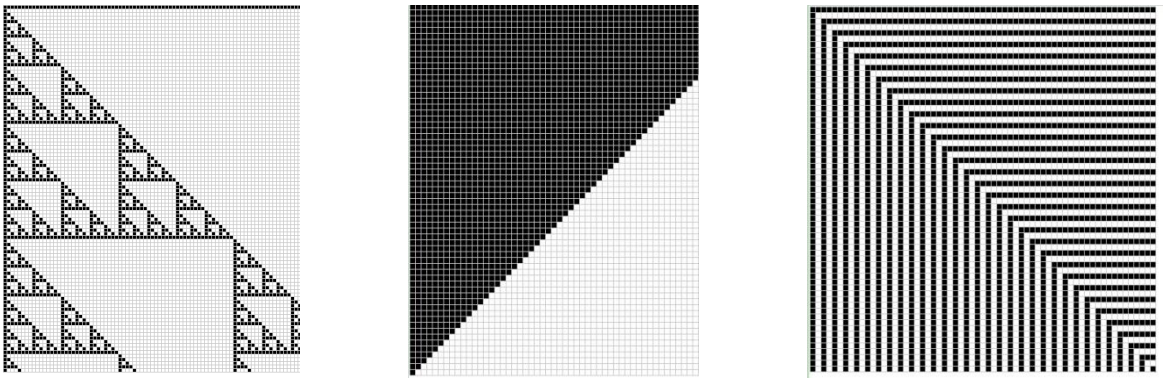

Рисунок 1 – Фрактальные структуры

Матричные структуры:

$$A=\begin{pmatrix}1&1&1&1&1\\1&0&0&0&0\\1&1&0&0&0\\1&0&1&0&0\\1&1&1&1&0\end{pmatrix}\quad B=\begin{pmatrix}1&1&1&1&1\\1&1&1&1&0\\1&1&1&0&0\\1&1&0&0&0\\1&0&0&0&0\end{pmatrix}\quad C=\begin{pmatrix}1&1&1&1&1\\1&0&0&0&0\\1&0&1&1&1\\1&0&1&0&0\\1&0&1&0&1\end{pmatrix} \tag{6}$$

Список использованных источников:

1. R.Megrelishvili, M. Chelidze, K. Chelidze, On the construction of secret and public-key cryptosystems, Iv. Javakhishvili Tbilisi State University I.Vekua Institute of Applied Mathematics, Applied Mathematics, Informatics and Mechanics, AMIM, v.11, N2, 2006, pp. 29-36.

2. Мегрелишвили Р.П., Челидзе М.А., Бесиашвили Г.М., Джинджихадзе М.В., Построение новой однонаправленной матричной функции и ее применение в криптографии, Оптико-электронные информационно-энергетические технологии, N2 (20), 2010, с. 67-71.

3. Мегрелишвили Р. , Шенгелия С.; "Оригинальная матричная однонаправленная функция и вопросы ее реализации", System Analysis and information technologies ,Conference SAIT 2013, Ukraine, Kyiv, cc. 465-466, 2013.

4. Мегрелишвили Р. , Шенгелия С.; "Фрактальные матрицы в криптографии", System Analysis and information technologies ,Conference SAIT 2014, Ukraine, Kyiv, cc. 418-419, 2014.

5. Мегрелишвили Р., Шенгелия С., Исследование и синтез матричных структур, System Analysis and information technologies ,Conference SAIT 2017, Ukraine, Kyiv, cc. 301-302, 2017.