ЗИП / Г.Н. Черкесов // Надежность. – 2013. – №2. – С.3-33.

REFERENCES

1. Prikaz Mintransa RF ot 23.07.2015 № 226.
2. Chernova A.I., Starzhinskaya N.V. Ekspluatacionnaya nadyozhnost' beregovogo radiooborudovaniya s uchyotom primeneniya ZIP dlya vosstanovleniya rabotosposobnosti// Transportnoe delo Rossii. – Morskie vesti Rossii, Moskva. – 2019. – № 3. – S. 129-132.
3. Cherkesov, G.N. Ocenka nadezhnosti sistem s uchetom ZIP: ucheb. posobie / G. N. Cherkesov – SPb.: BHV-Peterburg, 2012. – 480 s. – il.
4. Cherkesov, G.N. O kriteriyah vybora komplektov ZIP / G.N. CHerkesov // Nadezhnost'. – 2013. – №2. – S.3–33.

УДК 681.3.001:518.5
DOI: 10.34046/aumsuomt95/23

ИСПОЛЬЗОВАНИЕ КРОНЕКЕРОВА ПРОИЗВЕДЕНИЯ МАТРИЦ ДЛЯ МОДИФИКАЦИИ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

Е.И. Духнич, доктор технических наук, профессор
А.Г. Чефранов, доктор технических наук, профессор

В статье рассматривается использование произведения Кронекера (КП) для повышения эффективности криптографических алгоритмов. Формирование матриц большого размера с заданными свойствами с помощью КП матриц малого размера может использоваться при разработке новых блочных криптографических алгоритмов, в которых используются матрицы со следующими свойствами: ортогональные (унитарные), обращаемые, инволютивные. Модификации шифра Хилла с ключевой матрицей размером открытого текста, $T = 2^K$ байтов, представленной как произведение Кронекера из K обратимых элементарных матриц (ОЭМ), рассматривается в ряде работ. Они имеют квадратичную вычислительную сложностиО(T^2). Мы предлагаем модификации шифра Хилла на основе КР, НКР и I-НКР, где матрица ключей квадратичного размера фактически не рассчитывается. Вместо этого ОЭМ итеративно умножаются на открытый текст за время O($T\log_2 T$) и требуют линейной сложности памяти. Оценка времени шифрования таких модифицированных алгоритмов аналогична оценке шифров AES и RC4.
Ключевые слова: произведение Кронекера, шифр Хилла, одноразовый шифр, обратимая элементарная матрица.

The article discusses the use of the Kronecker product (KP) to improve the efficiency of cryptographic algorithms. The formation of large matrices with specified properties using KP of small matrices can be used in the development of new block cryptographic algorithms that use matrices with the following properties: orthogonal (unitary), invertible, involutive. Hill cipher modifications with a plaintext key matrix, $T = 2^K$ bytes, represented as a Kronecker product of K invertible elementary matrices (IEM), are considered in a number of works. They have quadratic computational complexity O(T^2). We propose modifications of the Hill cipher based on KP where the matrix of keys of a quadratic size is not actually calculated. Instead, IEMs are iteratively multiplied by the plaintext in O ($T\log_2 T$) time and need linear memory complexity. The estimation of the encryption time for such modified algorithms is similar to the estimation of the AES and RC4 ciphers.
Keywords: Kronecker product, Hill cipher, one-time cipher, invertible elementary matrix

Введение. Кронекерово произведение (КП) матриц сходно с тензорным произведением и широко используется во многих приложениях, в том числе, при обработке сигналов и изображений [1-5]. Формирование матриц большого размера с заданными свойствами с помощью КП матриц малого размера может использоваться при разработке новых вычислительных алгоритмов. Например, известны подходы к построению матриц для обработки сигналов и блочных криптографических алгоритмов со следующими свойствами:

- ортогональные (унитарные) матрицы [2];
- обращаемые матрицы [3];
- инволютивные матрицы [4].

Имея набор матриц, необходимо многократно выполнять операцию умножения их КП на вектор. Эта операция является критическим ядром для итерационных алгоритмов, так как умножение квадратной матрицы размера $\boldsymbol{n} \times \boldsymbol{n}$на вектор имеет вычислительную сложность O(n^2), и поэтому ее необходимо эффективно ускорять.

Размер КП элементарных матриц (ЭМ) может быть значительным, например, КП десяти ЭМ с$n = 10$ равен n^{10}, соответственно, умножение на вектор имеет сложность порядка10^{20}. Известны эффективные алгоритмы выполнения умножения вектора на КП произвольных матриц, которые оптимизируют и организацию использования памяти системы. В [3] предложен эффективный алгоритм умножения КП произвольных матриц на вектор (далее, УКПВ), рассмотрена задача о выборе размера участвующих в КП матриц, минимизирующего вычислительную сложность УКПВ, и

показано, что минимальная сложность $O(n\log_2 n)$ достигается при использовании в КП элементарных квадратных матриц размера $m = 2$. На его основе в [3] предложен алгоритм быстрого вычисления УКПВ (АБУКПВ) умножением очередной элементарной матрицы на части входного вектора. АБУКПВ допускает его параллельную реализацию за время $O(log_2 n)$.

В данной статье приведены определения и свойства КП, используемые АБУКПВ. Приведен иллюстрирующий АБУКПВ пример с $n = 8$, на основе которого предложена вычислительная схема его реализации для произвольного n, являющаяся гиперкубом. Приведены примеры модифицированных шифров с использованием АБУКПВ.

Кронекерово произведение матриц и его свойства. КП матриц $\boldsymbol{A(m,n)}$ и $\boldsymbol{B(p,r)}$ представляет собой блочную матрицу $(\boldsymbol{m \cdot p, n \cdot r})$ размера такую, что

$$(A \otimes B)_{ij} = A_{\lfloor (i-1)/p \rfloor+1,(\lfloor j-1)/r \rfloor+1} B_{(i-1) \bmod p+1,(j-1) \bmod r+1},$$
$$i = \overline{1,mp}, j = \overline{1,nr}, \quad (1)$$

где $\lfloor x \rfloor$ - целая часть x.

Из (1), если $m=n=p=r=2$, следует:

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B \\ a_{21}B & a_{22}B \end{pmatrix} =$$
$$= \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{pmatrix}.$$

КП порядка K это произведение K элементарных матриц, $\boldsymbol{P}_j$. $j = \overline{1,K}$:

$$P = P_1 \otimes (P_2 \otimes \ldots (P_{l-1} \otimes P_l) \ldots) = \bigotimes_{j=1}^{l} P_j, \quad (2)$$

при этом размер матрицы

$$sizeof(P) = (\prod_{i=1}^{l} m_i, \prod_{i=1}^{l} n_i), \quad (3)$$

где $sizeof(P_i) = (m_i, n_i)$, $i = \overline{1,l}$.

Свойство 1. Если A^{-1} и B^{-1} существуют, то $(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$.

Свойство 2. Пусть $C(mp,nr) = A(m,n) \otimes B(p,r)$. Тогда сложность матрично-векторного умножения

$$Y(mp) = C(mp,nr)X(nr) \quad (4)$$

равна $O(mnpr)$, но может быть уменьшена до $O(npr + pmn)$, если использовать структуру КП матрицы С.

Доказательство: Рассмотрим сперва алгоритм вычисления $Y = CX$, используя структуру КП. Из (1) следует:

$$Y_i = Y_{(i_1-1)p+i_2} =$$
$$\sum_{j=1}^{nr} C_{ij}X_j = \sum_{j_1=1}^{n} \sum_{j_2=1}^{r} A_{i_1 j_1} B_{i_2 j_2} X_{(j_1-1)r+j_2} =$$
$$\sum_{j_1=1}^{n} A_{i_1 j_1} Y^1_{(j_1-1)r+i_2}, \quad (5)$$

где
$$i_1 = \lfloor (i-1)/p \rfloor + 1, i_2 = (i-1) \bmod p + 1,$$
$$j_1 = \lfloor (j-1)/r \rfloor + 1, j_2 = (j-1) \bmod r + 1$$

$$Y^1_{(j_1-1)r+i_2} = \sum_{j_2=1}^{r} B_{i_2 j_2} X_{(j_1-1)r+j_2}, i = \overline{1,mp}, j = \overline{1,nr}. \quad (6)$$

Из (5), (6) следует, что вычислительная сложность вычисления (6) равна $O(nrp)$, а сложность вычисления (5), с помощью Y^1 из (6), равна $O(mnp)$. Таким образом, сложность вычисления (4) равна $O(nrp)+O(mnp)=O(pn(m+r))$, ЧТД.

Из Свойства 2 следует

Следствие 1. Вычислительная сложность УКПВ (4) $K=2$ при $m=n=p=r$ равна

$$BC\_KP(2,m)=O(2m^3). \quad (7)$$

Пример для n=8, КП порядка $\boldsymbol{K = log_2 n = 3}$. АБУКПВ основан на использовании Свойства 2. Рассмотрим вычисление

$$\boldsymbol{Y = (A \otimes B \otimes C) \cdot X = (A \otimes (B \otimes C)) \cdot X} \quad (8)$$

При размерности матриц-сомножителей $m \times m$, где m=2, выражение (8) можно представить как

$$(y1,y2,y3,y4,y5,y6,y7,y8)^{Tr} =$$
$$\begin{pmatrix} a11\begin{pmatrix} b11\begin{pmatrix} c11 & c12 \\ c21 & c22 \end{pmatrix}\cdot\begin{pmatrix} x1 \\ x2 \end{pmatrix} + & b12\begin{pmatrix} c11 & c12 \\ c21 & c22 \end{pmatrix}\cdot\begin{pmatrix} x3 \\ x4 \end{pmatrix} \\ b21\begin{pmatrix} c11 & c12 \\ c21 & c22 \end{pmatrix}\cdot\begin{pmatrix} x1 \\ x2 \end{pmatrix} + & b22\begin{pmatrix} c11 & c12 \\ c21 & c22 \end{pmatrix}\cdot\begin{pmatrix} x3 \\ x4 \end{pmatrix} \end{pmatrix} + \\ +a12\begin{pmatrix} b11\begin{pmatrix} c11 & c12 \\ c21 & c22 \end{pmatrix}\cdot\begin{pmatrix} x5 \\ x6 \end{pmatrix} + & b12\begin{pmatrix} c11 & c12 \\ c21 & c22 \end{pmatrix}\cdot\begin{pmatrix} x7 \\ x8 \end{pmatrix} \\ b21\begin{pmatrix} c11 & c12 \\ c21 & c22 \end{pmatrix}\cdot\begin{pmatrix} x5 \\ x6 \end{pmatrix} + & b22\begin{pmatrix} c11 & c12 \\ c21 & c22 \end{pmatrix}\cdot\begin{pmatrix} x7 \\ x8 \end{pmatrix} \end{pmatrix} \\ a21\begin{pmatrix} b11\begin{pmatrix} c11 & c12 \\ c21 & c22 \end{pmatrix}\cdot\begin{pmatrix} x1 \\ x2 \end{pmatrix} + & b12\begin{pmatrix} c11 & c12 \\ c21 & c22 \end{pmatrix}\cdot\begin{pmatrix} x3 \\ x4 \end{pmatrix} \\ b21\begin{pmatrix} c11 & c12 \\ c21 & c22 \end{pmatrix}\cdot\begin{pmatrix} x1 \\ x2 \end{pmatrix} + & b22\begin{pmatrix} c11 & c12 \\ c21 & c22 \end{pmatrix}\cdot\begin{pmatrix} x3 \\ x4 \end{pmatrix} \end{pmatrix} + \\ +a22\begin{pmatrix} b11\begin{pmatrix} c11 & c12 \\ c21 & c22 \end{pmatrix}\cdot\begin{pmatrix} x5 \\ x6 \end{pmatrix} + & b12\begin{pmatrix} c11 & c12 \\ c21 & c22 \end{pmatrix}\cdot\begin{pmatrix} x7 \\ x8 \end{pmatrix} \\ b21\begin{pmatrix} c11 & c12 \\ c21 & c22 \end{pmatrix}\cdot\begin{pmatrix} x5 \\ x6 \end{pmatrix} + & b22\begin{pmatrix} c11 & c12 \\ c21 & c22 \end{pmatrix}\cdot\begin{pmatrix} x7 \\ x8 \end{pmatrix} \end{pmatrix} \end{pmatrix} X \quad (9)$$

Видим, что в правой части (9) каждая матрица С четыре раза умножается на одну и ту же часть вектора X (из четырех). Умножая, получаем:

$$\begin{pmatrix} a11\begin{pmatrix} b11\begin{pmatrix} y1^3 \\ y2^3 \end{pmatrix} + & b12\begin{pmatrix} y3^3 \\ y4^3 \end{pmatrix} \\ b21\begin{pmatrix} y1^3 \\ y2^3 \end{pmatrix} + & b22\begin{pmatrix} y3^3 \\ y4^3 \end{pmatrix} \end{pmatrix} + a12\begin{pmatrix} b11\begin{pmatrix} y5^3 \\ y6^3 \end{pmatrix} + & b12\begin{pmatrix} y7^3 \\ y8^3 \end{pmatrix} \\ b21\begin{pmatrix} y5^3 \\ y6^3 \end{pmatrix} + & b22\begin{pmatrix} y7^3 \\ y8^3 \end{pmatrix} \end{pmatrix} \\ a21\begin{pmatrix} b11\begin{pmatrix} y1^3 \\ y2^3 \end{pmatrix} + & b12\begin{pmatrix} y3^3 \\ y4^3 \end{pmatrix} \\ b21\begin{pmatrix} y1^3 \\ y2^3 \end{pmatrix} + & b22\begin{pmatrix} y3^3 \\ y4^3 \end{pmatrix} \end{pmatrix} + a22\begin{pmatrix} b11\begin{pmatrix} y5^3 \\ y6^3 \end{pmatrix} + & b12\begin{pmatrix} y7^3 \\ y8^3 \end{pmatrix} \\ b21\begin{pmatrix} y5^3 \\ y6^3 \end{pmatrix} + & b22\begin{pmatrix} y7^3 \\ y8^3 \end{pmatrix} \end{pmatrix} \end{pmatrix}$$
$$= (y1,y2,y3,y4,y5,y6,y7,y8)^{Tr} \quad (10)$$

где

$y1^3 = c11 \cdot x1 + c12 \cdot x2$, $y2^3 = c21 \cdot x1 + c22 \cdot x2$, $y3^3 = c11 \cdot x3 + c12 \cdot x4$, $y4^3 = c21 \cdot x3 + c22 \cdot x4$, $y5^3 = c11 \cdot x5 + c12 \cdot x6$, $y6^3 = c21 \cdot x5 + c22 \cdot x6$, $y7^3 = c11 \cdot x7 + c12 \cdot x8$, $y8^3 = c21 \cdot x7 + c22 \cdot x8$

и Tr означает транспонирование матрицы.

Переставляя ряды в левой части и элементы вектора в правой части (10), получаем

$$\begin{pmatrix} a11\begin{pmatrix}\begin{pmatrix}b11 & b12\\ b21 & b22\end{pmatrix}\begin{pmatrix}y1^3\\ y3^3\end{pmatrix}\\ \begin{pmatrix}b11 & b12\\ b21 & b22\end{pmatrix}\begin{pmatrix}y2^3\\ y4^3\end{pmatrix}\end{pmatrix} + a12\begin{pmatrix}\begin{pmatrix}b11 & b12\\ b21 & b22\end{pmatrix}\begin{pmatrix}y5^3\\ y7^3\end{pmatrix}\\ \begin{pmatrix}b11 & b12\\ b21 & b22\end{pmatrix}\begin{pmatrix}y6^3\\ y8^3\end{pmatrix}\end{pmatrix}\\ a21\begin{pmatrix}\begin{pmatrix}b11 & b12\\ b21 & b22\end{pmatrix}\begin{pmatrix}y1^3\\ y3^3\end{pmatrix}\\ \begin{pmatrix}b11 & b12\\ b21 & b22\end{pmatrix}\begin{pmatrix}y2^3\\ y4^3\end{pmatrix}\end{pmatrix} + a22\begin{pmatrix}\begin{pmatrix}b11 & b12\\ b21 & b22\end{pmatrix}\begin{pmatrix}y5^3\\ y7^3\end{pmatrix}\\ \begin{pmatrix}b11 & b12\\ b21 & b22\end{pmatrix}\begin{pmatrix}y6^3\\ y8^3\end{pmatrix}\end{pmatrix}\end{pmatrix} = \begin{pmatrix}y1\\ y3\\ y2\\ y4\\ y5\\ y7\\ y6\\ y8\end{pmatrix} \quad (11)$$

В (11) каждая матрица В умножается теперь два раза на одну и ту же часть вектора X (из четырех). Умножая, получаем:

$$\begin{pmatrix} a11\begin{pmatrix}\begin{pmatrix}y1^2\\ y2^2\end{pmatrix}\\ \begin{pmatrix}y3^2\\ y4^2\end{pmatrix}\end{pmatrix} + a12\begin{pmatrix}\begin{pmatrix}y5^2\\ y6^2\end{pmatrix}\\ \begin{pmatrix}y7^2\\ y8^2\end{pmatrix}\end{pmatrix}\\ a21\begin{pmatrix}\begin{pmatrix}y1^2\\ y2^2\end{pmatrix}\\ \begin{pmatrix}y3^2\\ y4^2\end{pmatrix}\end{pmatrix} + a22\begin{pmatrix}\begin{pmatrix}y5^2\\ y6^2\end{pmatrix}\\ \begin{pmatrix}y7^2\\ y8^2\end{pmatrix}\end{pmatrix}\end{pmatrix} = \begin{pmatrix}y1\\ y3\\ y2\\ y4\\ y5\\ y7\\ y6\\ y8\end{pmatrix}, \quad (12)$$

где

$y1^2 = b11 \cdot y1^3 + b12 \cdot y3^3$, $y2^2 = b21 \cdot y1^3 + b22 \cdot y3^3$,
$y3^2 = b11 \cdot y2^3 + b12 \cdot y4^3$, $y4^2 = b21 \cdot y2^3 + b22 \cdot y4^3$,
$y5^2 = b11 \cdot y5^3 + b12 \cdot y7^3$, $y6^2 = b21 \cdot y5^3 + b22 \cdot y7^3$,
$y7^2 = b11 \cdot y6^3 + b12 \cdot y8^3$, $y8^2 = b21 \cdot y6^3 + b22 \cdot y8^3$.

Переставляя ряды матрицы в левой части и соответствующие элементы вектора в правой части (12), получаем

$$\begin{pmatrix}\begin{pmatrix}a11 & a12\\ a21 & a22\end{pmatrix}\cdot\begin{pmatrix}y1^2\\ y5^2\end{pmatrix}\\ \begin{pmatrix}a11 & a12\\ a21 & a22\end{pmatrix}\cdot\begin{pmatrix}y2^2\\ y6^2\end{pmatrix}\\ \begin{pmatrix}a11 & a12\\ a21 & a22\end{pmatrix}\cdot\begin{pmatrix}y3^2\\ y7^2\end{pmatrix}\\ \begin{pmatrix}a11 & a12\\ a21 & a22\end{pmatrix}\cdot\begin{pmatrix}y4^2\\ y8^2\end{pmatrix}\end{pmatrix} = \begin{pmatrix}y1^1\\ y2^1\\ y3^1\\ y4^1\\ y5^1\\ y6^1\\ y7^1\\ y8^1\end{pmatrix} = \begin{pmatrix}y1\\ y5\\ y2\\ y6\\ y3\\ y7\\ y4\\ y8\end{pmatrix}. \quad (13)$$

В (13) каждая матрица А умножается теперь однократно на каждую из четырех частей вектора X. Преобразования (9)-(13) можно представить в виде схемы на Рис. 1, где для каждой из четырех экземпляров каждой из матриц A, B, C, указаны соответствующие входные и выходные данные. Можно видеть, что схема КП имеет$log_2 n = 3$ уровня и в каждом по $\frac{n}{2} = 4$ схемы матричного 2×2 умножения.

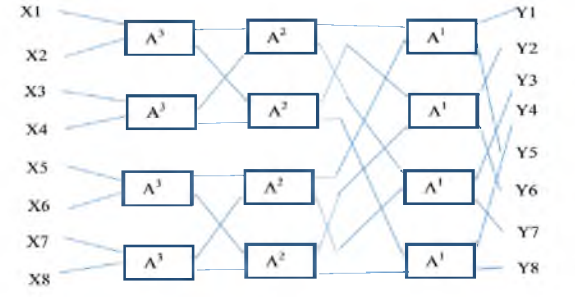

Рисунок 1– Схема вычислений,
где $\mathbf{A^1 = A,\ A^2 = B, A^3 = C}$.

В общем случае схема АБУКПВ для n= 2^K имеет $log_2 n = K$уровней с $\frac{n}{2}$ матричными $m \times m$ умножителями. При этом вычислительная сложность АБУКПВ будет равна

$$\text{ВС}(X, K, m) = Km^{K+1}(\text{умнож.}) \quad (14)$$

Модифицированные блочные шифры.

Наосновепредложенного АБУКПВнамибылиразработаныдвамодифицированных шифра Хилла:

- алгоритм НКР [3], использующий КП обращаемых элементарных матриц;

- алгоритм I-НКР [5], использующий КП инволютивных элементарных матриц.

Шифр НКР шифрует исходный текст размером T байт, равным степени размера m элементарной матрицы IEM, определяющего порядок КП$K=log_m T$.

НКРшифр.

Вход:

- N-значение модуля для модульной арифметики,

- исходный текст, $P \in Z_N^T$ размером$T=m^K$, $K>1$,

- алгоритм генератора псевдо случайных чисел, PRNG, и его начальный параметр, SEED,

Выход:

- участвующие в шифровании обращаемые элементарные матрицы IEM, $A^1,..,A^K$, элементы которых сгенерированы PRNG;

- шифротекст, $C \in Z_N^{m^K}$.

Begin //НКР шифрование

1. Сгенерировать K матриц IEM, $A^1(m,m),..,A^K(m,m)$,с элементами a,bиз Z_N, используя PRNG(SEED). Для $m=2$, $A_{11}=a$, $A_{12}=b$, $A_{21}=0$, $A_{22}=a^{-1} mod\ N$

2. Вычислить $C = (\overset{K}{\underset{i=1}{\otimes}} A^i) P \bmod N$, используя АБУКПВ

3. End //НКР шифрование

НКР Дешифрование

Вход:

- N-значение модуля для модульной арифметики,

- шифротекст, $C \in Z_N^T$ размера $T=m^K$, $K>1$,

- алгоритм генератора псевдо случайных чисел, PRNG, и его начальный параметр, SEED,

Выход:

- участвующие в дешифровании элементарные матрицы IEM, $A^1,..,A^K$, элементы которых сгенерированы PRNG;

- исходный текст, $C \in Z_N^{m^K}$.

Begin //НКРдешифрование

1. Сгенерировать K матриц IEM, $A^1(m,m),..,A^K(m,m)$, с элементами a,b из Z_N, используя PRNG(SEED). Для $m=2$, $A_{11}=a$, $A_{12}=b$, $A_{21}=0$, $A_{22}=a^{-1} mod\ N$

2. Вычислить обратные матрицы IEM, $(A^1)^{-1},..,(A^K)^{-1}$: $Y=A^{-1} modN$, где $Y_{11}=a^{-1} modN$, $Y_{12}=-b$, $Y_{21}=0$, $Y_{22}=a$.

3. Вычислить

$$P=(\overset{K}{\underset{i=1}{\otimes}}(A^i)^{-1})C \bmod N$$, используя АБУКПВ

End //НКР дешифрование.

Главное достоинство НКР шифра заключается в том, что процесс формирования ключевой матрицы в виде КР элементарных матриц происходит одновременно с процессом шифрования(дешифрования).Учитывая, что K = $\log_m$T и m = 2, из (14) вычислительная сложность алгоритма НКР:

$$BC = log_2 T \cdot (2^{log_2 T+1}) = 2 \cdot T \cdot log_2 T = = O(T \cdot log_2 T) \quad (15)$$

I-НКР шифр.

Вход:

- N-значение модуля для модульной арифметики,
- исходный текст, $P \in Z_N^T$ размером $T=m^K$, $K>1$,
- алгоритм генератора псевдо случайных чисел, PRNG, и его начальный параметр, SEED,

Выход:

- участвующие в шифровании элементарные инволютивные матрицыEIM, $A^1,..,A^K$, элементы которых сгенерированы PRNG;
- шифротекст, $C \in Z_N^{m^K}$.

Begin //I-НКРшифрование

1. Сгенерировать K матриц EIM, $A^1(m,m),..,A^K(m,m)$, с элементами a,b из Z_N, используяPRNG(SEED).
Для $m=2$, $A_{11}=a$, $A_{12}=b$, $A_{21}=(1-a^2)b^{-1} mod\ N$, $A_{22}=-a$

2. Вычислить

$$C=(\overset{K}{\underset{i=1}{\otimes}}A^i)P \bmod N$$, используя АБУКПВ

3. End //I-НКР шифрование

I-НКР Дешифрование

Вход:

- N-значение модуля для модульной арифметики,
- шифротекст, $C \in Z_N^T$ размера $T=m^K$, $K>1$,
- алгоритм генератора псевдослучайных чисел, PRNG, и его начальный параметр, SEED,

Выход:

- участвующие в дешифровании элементарные матрицы EIM, $A^1,..,A^K$, элементы которых сгенерированы PRNG;
- исходный текст, $C \in Z_N^{m^K}$.

Begin //НКРдешифрование

1. Сгенерировать KматрицEIM, $A^1(m,m),..,A^K(m,m)$, с элементами a,b из Z_N, используяPRNG(SEED). Для $m=2$,$A_{11}=a$, $A_{12}=b$, $A_{21}=(1-a^2)b^{-1} mod\ N$, $A_{22}=-a$

2. Получить исходный текст $P=(\otimes_{i=1}^{K} A^i)\cdot C\ mod\ N$, используя АБУКПВ

End //НКРдешифрование.

Главное достоинствоI-НКР шифра заключается в том, что процесс формирования ключевой матрицы в виде КР элементарных матриц происходит одновременно с процессом шифрования (дешифрования), кроме того, для дешифрования используются те же инволютивные (самообратимые) элементарные матрицы, что и для шифрования. Вычислительная сложность I-НКР шифра ниже, чем у НКР шифра, так как отпадает необходимость обращения матрицEIM.

Заключение. На основе предложенного ускоренного умножения кронекерова произведения матриц на вектор представлены модификации шифра Хилла: НКР-шифр и I-НКР-шифр, которые существенно повышают его эффективность за счет исключения предварительного отдельного вычисления КП и отсутствия необходимости хранения в памяти ключевой матрицы (КП).

Литература

1. C. F. Van Loan. The ubiquitous Kronecker product. Journal of Computational and Applied Mathematics, 123, 2000, p. 85–100.
2. C. Koukouvinos, E. Lappas, D. E. Simos. Encryption schemes using orthogonal arrays, Journal of Discrete Mathematical Sciences & Cryptography, 12 (5), 2009, pp. 615–628.
3. Alexander Chefranov, Evgeny Dukhnich. One-Time Kronecker Product-Based Hill Cipher Modification. International Journal of Information Assurance and Security (JIAS), V.12, N3, 2017, pp.94-103.
4. Духнич Е.И., Шапель А.П. Эффективный метод формирования инволютивных матриц для модифицированного шифра Хилла// Материалы Национальной конференции «Научно-технические, экономические и правовые аспекты развития транспортного комплекса».– 2019.– ч.1.– С.71-72.
5. Alexander Chefranov, Evgeny Dukhnich, Alexander Shapel. One-Time Involutory Matrix-Based Hill Ci-

pher Modification. International Journal of Information Assurance and Security (JIAS), V.15, N4, 2020, pp.165-174.

References

1. C. F. Van Loan. The ubiquitous Kronecker product. Journal of Computational and Applied Mathematics, 123, 2000, p. 85–100.
2. C. Koukouvinos, E. Lappas, D. E. Simos. Encryption schemes using orthogonal arrays, Journal of Discrete Mathematical Sciences & Cryptography, 12 (5), 2009, pp. 615–628.
3. Alexander Chefranov, Evgeny Dukhnich. One-Time Kronecker Product-Based Hill Cipher Modification. International Journal of Information Assurance and Security (JIAS), V.12, N3, 2017, pp.94-103.
4. Dukhnich E.I., Shapel A.P. An effective method for the formation of involutive matrices for the modified Hill cipher, Materials of the National Conference "Scientific, technical, economic and legal aspects of the development of the transport complex", 2019, part 1, pp. 71-72
5. Alexander Chefranov, Evgeny Dukhnich, Alexander Shapel. One-Time Involutory Matrix-Based Hill Cipher Modification. International Journal of Information Assurance and Security (JIAS), V.15, N4, 2020, pp.165-174.

УДК 53.05; 004.02
DOI: 10.34046/aumsuomt95/24

ВИЗУАЛИЗАЦИЯ СЛОЖЕНИЯ КОЛЕБАТЕЛЬНЫХ ДВИЖЕНИЙ МЕТОДОМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Е.Н. Сюсюка, кандидат технических наук, доцент
А. А. Колесников, курсант
А.Е. Чупин, курсант

В статье представлены методы сложения гармонических колебаний в Pascal ABC и MicrosoftExcel с оживлением и возможностью изменения по алгоритму. Цель данной работы заключается в ознакомлении читателей о технологиисложения гармонических колебаний, как направленных вдоль одной прямой, так и взаимно перпендикулярных, а также реализации этих технологий средствами Pascal ABC и MicrosoftExcel. В статье приведены результаты исследований, которые дают представления о реализации сложения гармонических колебаний средствами Pascal ABC и MicrosoftExcel.Данный алгоритм можно использовать для моделирования наложения волновых процессов как в любой упругой средепри изучении устойчивости судна на воде, конструкций, вибродиагностики механизмов, так и для анализа интерференционных явлений в оптике и при распространении электромагнитных волнв радио- и оптической связи. Кроме того, методику можно применять с целью визуализации моделирования сложения колебаний в учебном процессе.
Ключевые слова: гармонические колебания, сложение гармонических колебаний, направленные вдоль одной прямой колебания, взаимно перпендикулярные колебания, фигуры Лиссажу, Pascal ABC, Microsoft Excel.

The article presents methods of addition of harmonic oscillations in Pascal ABC and Microsoft Excel with revival and possibility of change by algorithm. The purpose of this work is to familiarize readers about the technologies of addition of harmonic oscillations, both directed along one straight line and mutually perpendicular, as well as the implementation of these technologies by means of Pascal ABC and Microsoft Excel. The article presents the results of studies that give an idea of the implementation of the addition of harmonic oscillations by means of Pascal ABC and Microsoft Excel.
Keywords: harmonic oscillations, addition of harmonic oscillations, directed along one straight line oscillations, mutually perpendicular oscillations, lissajou figures, Pascal ABC, Microsoft Excel.

Актуальность визуализации сложения колебаний методом информационных технологий

Различные виды колебаний имеют совершенно разную физическую природу и объединяютсялишь единством их математического описания. Естественно, что при такомшироком взгляде на проблему не удается в рамках одного учебного предметаотразить спецификуколебательных явлений в каждом из рассматриваемых областей техники.Изучение колебательных процессов имеет большое значение для развития современной техники, так как с её помощью могут быть корректно рассмотрены практически важные проблемы создания систем стабилизации, измерения вибрационных характеристик и т.п. Это позволяет проектировать приборы и системы, способные функционировать на подвижных объектах, находя свое применение в авиации, судостроении и других областях техники.

На море, как известно, вода всегда находится в движении. В основном всегда, мы видим волны на поверхности воды. Колебания ей придают подземные толчки, движение воздушных масс, гравитационная сила Луны, течения, взаимные движения судов и т.д. Когда колебания в воде идут сонаправленно и с одинаковой частотой, происходит сложение волн, и высота волны увеличивается. Однако, если одной водной