An Iterative Process Involving Interlacing and Decoposition in the Devlopment of a Block Cipher

S. Udaya Kumar†, V. U. K. Sastry†, and A. Vinaya babu††

†SreeNidhi Institute of Science & Technology, Hyderabad, India

††JNT University, Hyderabad, India

Summary

In this paper, we have developed a block cipher by introducing the basic concepts interlacing and decomposition. Here, we have taken the key in the form of matrices, and the plaintext as column vectors, wherein all are containing binary bits. In the process of encryption, we have employed an iterative procedure. In the process of decryption, we have used the modular arithmetic inverses of the key matrices. The cryptanalysis carried out in this paper clearly shows that the cipher cannot be broken by any cryptanalytic attack.

Key words: *Block cipher, key matrix, modular arithmetic inverse of the key matrix, interlacing, decomposition*

1. Introduction

In the classical literature of cryptography, Hill cipher [1] occupies a prominent place. In this, the characters A to Z are represented by the numbers 0 to 25, and the ciphertextis written in terms of the numbers. A secret key is taken in the form of a matrix, which contains numbers, wherein each number is less than 26. Here, we get the ciphertext by operating with the key matrix on the plaintext vector and performing mod 26.

Following Hill, Feistel [2-3], made an attempt to develop block cipher, wherein the plaintext and the key matrix are represented in terms of binary bits and mod 2 operation is carried out on the result obtained by multiplying the plaintext vector with the key matrix. However, he found that the cipher can be broken by the known plaintext attack.

In the present paper, our objective is to develop a block cipher, wherein the key is taken in terms of a number matrices and the plaintext is represented in the form of column vectors. Here our interest is to see how the process consisting of iteration, interlacing, and decomposition play a vital role in strengthening the cipher.

2. Development of the cipher

Let us consider a plaintext consisting of n characters. By using the ASCII code, each character can be represented in terms of seven binary bits. Then the plaintext comprising 7n binary bits can be viewed as n sub strings, wherein each one contains seven binary bits.

Let us take a key containing 7n numbers, wherein each number lies between 0 and 127. Thus each number can be represented in the form of seven binary bits. Then we can have n matrices of size 7x7, formed from the given key. Let us denote the key matrices by K_i, i = 1 to n, and the plaintext column vectors by p_i , i = 1 to n. Before we proceed to the process of iteration, let us take p_i^0 ($p_i^0 \equiv p_i$), i = 1 to n, be the initial (given) plaintext column vectors. In the process of encryption, after the first iteration, on multiplying p_i^0 by K_i, i =1 to n, we get

$$Q_i^1 = K_i \, p_i^0 \bmod 2, \; i = 1 \text{ to } n, \quad (2.1)$$

where each one of the Q_i^1 s is a column vector consisting of seven binary bits, which can be denoted by

$$Q_{i1}^1 , Q_{i2}^1 , \ldots, Q_{i7}^1 .$$

Now let us describe the process of interlacing. In this, we arrange all the 7n bits of Q_i^1, i = 1 to n in a row as follows.

$$Q_{11}^1 , Q_{12}^1 , \ldots, Q_{17}^1 , Q_{21}^1 , Q_{22}^1 , \ldots, Q_{27}^1 , \ldots , Q_{n1}^1 , Q_{n2}^1 , \ldots, Q_{n7}^1 . \quad (2.2)$$

Then we place the last element of the row, i.e. Q_{n7}^1 as the first element of the column vector Q_1^1, the last but one element of the row Q_{n6}^1 as the first element of the column vector Q_2^1, and so on, till we exhaust all the first elements positions of the n column vectors Q_i^1, i = 1 to n.

Subsequently, we carryout the process of placing the elements of the row in the second element position of each of the column vectors, and continue the same procedure till we place all the elements of the row in the column vectors. Thus, finally, all the seven positions of the n column vectors are completely filled as we have 7n elements in the row under consideration.

Let us now represent the column vectors obtained from the first iteration after interlacing as

$$p_i^1 = <Q_i^1>, \text{ i = 1 to n,} \qquad (2.3)$$

where < > denotes the process of interlacing.

On performing the second iteration and interlacing we have

$$Q_i^2 = \text{K}_\text{i}\, p_i^1 \bmod 2, \text{ i = 1 to n,} \qquad (2.4)$$

and $p_i^2 = <Q_i^2>.$ (2.5)

Thus the process of encryption, which includes iteration and interlacing, can in general be written as follows.

$$Q_i^j = \text{K}_\text{i}\, P_i^{j-1} \bmod 2, \qquad (2.6)$$
$$P_i^j = <Q_i^j>, \qquad (2.7)$$

where i = 1 to n, and j = 1 to m, in which m denotes the number of iterations.

Let us now concatenate the sub strings corresponding to the column vectors in P_i^m and obtain the ciphertext, denoted by C.

The process of decryption, which depends upon iteration and decomposition (a procedure opposite to that of interlacing) is carried out by reversing all the above steps, one after another, starting from the last step. Now let us describe the process of decomposition.

Consider the ciphertext C. Divide this into n sub strings, wherein each one contains 7 binary bits. Now, we represent these sub strings as column vectors and hence we get P_i^m , i = 1 to n.

We place the first element of the first column vector (p_1^m) as the last element of the row, the first element of the second column vector (p_2^m) as the last but one element of the row, and so on. Thus by placing the first elements of the n column vectors (p_i^m, i =1 to n), in the row we get the last n elements of the row. Then we place the second elements of each of the n column vectors in a similar manner. We continue this process till we exhaust all the elements of the n column vectors. Thus the row consists of 7n elements given by (2.2).

We now divide the row into n sub strings and consider each sub string as a column vector. Hence we get

$$Q_i^m, \text{ i = 1 to n,} \qquad (2.7)$$

where $Q_i^m = [\, Q_{i1}^m, Q_{i2}^m, \ldots, Q_{i7}^m]^T$, in which T denotes the transpose of the vector.

We may now write

$$Q_i^m => p_i^m <, \qquad (2.8)$$

where > < denotes the process of decomposition.

On obtaining the modular arithmetic inverse [7] of each K_i denoted by K_i^{-1}, i = 1 to n, and using the equation (2.6), we get

$$p_i^{m-1} = K_1^{-1}\, Q_i^m \bmod 2. \qquad (2.9)$$

It may be noted that $K_i\, K_1^{-1} \bmod 2 = K_1^{-1} K_i \bmod 2 = I$. Now the process of iteration governing decryption, which involves the decomposition procedure can be written as follows.

$$Q_i^j => p_i^j <, \qquad (2.10)$$

and $$p_i^{j-1} = K_1^{-1}\, Q_i^j \bmod 2, \qquad (2.11)$$

where i = 1 to n, and j = m to 1.

At the end of the iteration, we get the plaintext p_i^0.

For clarity of understanding of the basic concepts interlacing and decomposition introduced in the above development of the cipher, we have presented them by giving a simple example in Appendix A.

In what follows, we design algorithms for encryption and decryption, and write procedure for obtaining the modular arithmetic inverse of the key matrix.

3. Algorithms

3.1 Algorithm for Encryption

{

1. for i =1 to n, read p_i^0 and K_i
2. for j = 1 to m

   {

   for i = 1 to n

   {

   $Q_i^j = K_i\, p_i^{j-1} \bmod 2$

   $p_i^j = < Q_i^j >$

   }

   }
3. Find C by concatenating p_i^m.
4. Write C.

}

3.2 Algorithm for decryption

{

1. Read C
2. Divide C into n sub strings and obtain P_i^m for i = 1 to n.
3. for i =1 to n

   {

   Read K_i

   Find K_i^{-1}

   }
4. for j = m to 1

   {

   for i =1 to n

   {

   $Q_i^j = >P_i^j<$

   $P_i^{j-1} = K_i^{-1} Q_i^j$ mod 2

   }

   }
5. for i =1 to n, write P_i^0

}

3.3 Algorithm for the modular arithmetic inverse

{

1. for i = 1 to n,

   {

   Read K_i

   Find K_i^{-1} by calling the procedure for the modular arithmetic inverse

   }

2. Procedure for the modular arithmetic inverse

{

i. Let A = K. Find the determinant of A. Let it be denoted by Δ.

ii. Find the inverse of A. The inverse is given by $A^{-1} = \frac{[A_{ji}]}{\Delta}$

i =1 to n, j = 1 to n,

where A_{ij} are the cofactors of a_{ij}, which are elements of A, and Δ is the determinant of A.

iii. for i = 1 to n,

{

if ((iΔ) mod N = 1) d = i;

break;

}

B = [dA_{ji}] mod N.

// B is the modular arithmetic inverse of A.

}

Here it is to be noted that the modular arithmetic inverse of a matrix A exists only when A is non-singular, and Δ is relatively prime to N. In the present analysis, we take N = 2, and obtain the modular arithmetic inverse of A such that AB mod 2 = BA mod 2 = I.

4. Illustration of the cipher

Let us take a key K_0 in the form

$$K_0 = \{79, 65, 98, 37, 55, 119, 123, 29, 79, 94, 86, 55, 69, 125, 59, 91, 43, 86, 35, 69, 25, 39, 19, 23, 86, 95, 49, 75, 9, 59, 56, 77, 35, 84, 29, 49, 77, 41, 82, 72, 65, 38, 79, 87, 11, 42, 72, 25, 23, 73, 81, 17, 45, 79, 22, 63\}. \quad (4.1)$$

This key consists of 56 numbers, wherein each number lies between 0 and 127. Here, repetition of the numbers is allowed. Let us divide this key into 8 sub keys, wherein each sub key consists of 7 numbers. We form the first sub key K_1 by taking the first seven numbers of (4.1), and the second sub key K_2 by taking the second seven numbers, and so on till we exhaust all the 56 numbers.

On writing each number in terms of binary bits, the first sub key can be written in the form of a matrix of size 7x7. Similarly we can write the other sub keys also in terms of matrices of size 7x7. Thus we have eight matrices, K_i, i = 1 to 8, given by

$$K_1 = \begin{bmatrix} 1&0&0&1&1&1&1 \\ 1&0&0&0&0&0&1 \\ 1&1&0&0&0&1&0 \\ 0&1&0&0&1&0&1 \\ 0&1&1&0&1&1&1 \\ 1&1&1&0&1&1&1 \\ 1&1&1&1&0&1&1 \end{bmatrix}, \quad K_2 = \begin{bmatrix} 0&0&1&1&1&0&1 \\ 1&0&0&1&1&1&1 \\ 1&0&1&1&1&1&0 \\ 1&0&1&0&1&1&0 \\ 0&1&1&0&1&1&1 \\ 1&0&0&0&1&0&1 \\ 1&1&1&1&1&0&1 \end{bmatrix},$$

$$K_3 = \begin{bmatrix} 0&1&1&1&0&1&1 \\ 1&0&1&1&0&1&1 \\ 0&1&0&1&0&1&1 \\ 1&0&1&0&1&1&0 \\ 0&1&0&0&0&1&1 \\ 1&0&0&0&1&0&1 \\ 0&0&1&1&0&0&1 \end{bmatrix}, \quad K_4 = \begin{bmatrix} 0&1&0&0&1&1&1 \\ 0&0&1&0&0&1&1 \\ 0&0&1&0&1&1&1 \\ 1&0&1&0&1&1&0 \\ 1&0&1&1&1&1&1 \\ 0&1&1&0&0&0&1 \\ 1&0&0&1&0&1&1 \end{bmatrix},$$

$$K_5 = \begin{bmatrix} 0&0&0&1&0&0&1 \\ 0&1&1&1&0&1&1 \\ 0&1&1&0&1&1&0 \\ 1&0&0&1&1&0&1 \\ 0&1&0&0&0&1&1 \\ 1&0&1&0&1&0&0 \\ 0&0&1&1&1&0&1 \end{bmatrix}, \quad K_6 = \begin{bmatrix} 0&1&1&0&0&0&1 \\ 1&0&0&1&1&0&1 \\ 0&1&0&1&0&0&1 \\ 1&0&1&0&0&1&0 \\ 1&0&0&1&0&0&0 \\ 1&0&0&0&0&0&1 \\ 0&1&0&0&1&1&0 \end{bmatrix},$$

$$K_7 = \begin{bmatrix} 1&0&0&1&1&1&1 \\ 1&0&1&0&1&1&1 \\ 0&0&0&1&0&1&1 \\ 0&1&0&1&0&1&0 \\ 1&0&0&1&0&0&0 \\ 0&0&1&1&0&0&1 \\ 0&0&1&0&1&1&1 \end{bmatrix}, \quad K_8 = \begin{bmatrix} 1&0&0&1&0&0&1 \\ 1&0&1&0&0&0&1 \\ 0&0&1&0&0&0&1 \\ 0&1&0&1&1&0&1 \\ 1&0&0&1&1&1&1 \\ 0&0&1&0&1&1&0 \\ 0&1&1&1&1&1&1 \end{bmatrix}. \quad (4.2)$$

Consider the plaintext: All the enemies are killed, no worry for the country. (4.3)
Let us now take the first 8 characters of the plaintext namely, All ƀ the ƀ into consideration. This includes two blank spaces.

On using the ASCII code, the above 8 characters can be represented as 8 column vectors given by

$$P_1^0 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, P_2^0 = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, P_0^3 = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \; P_0^4 = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix},$$

$$P_0^5 = \begin{bmatrix} 1\\1\\1\\0\\1\\0\\0 \end{bmatrix}, P_0^6 = \begin{bmatrix} 1\\0\\0\\1\\0\\0\\0 \end{bmatrix}, P_0^7 = \begin{bmatrix} 1\\1\\0\\0\\1\\0\\1 \end{bmatrix}, P_0^8 = \begin{bmatrix} 0\\0\\0\\1\\0\\0\\0 \end{bmatrix}. \quad (4.4)$$

On applying the encryption algorithm mentioned in section (3.1), taking m = 16, and carrying out sixteen iterations, we get the ciphertext given by

1001011011001001111111111111001100100001001 1
0111001000110. (4.5)

On adopting the procedure for obtaining the modular arithmetic inverse, we get

$$K_1^{-1} = \begin{bmatrix} 0&0&0&0&1&1&0\\ 1&1&1&0&1&0&1\\ 1&1&0&1&1&1&1\\ 1&0&1&1&0&0&0\\ 1&0&1&1&0&1&1\\ 1&1&0&0&0&1&1\\ 0&1&0&0&1&1&0 \end{bmatrix}, \quad K_2^{-1} = \begin{bmatrix} 0&1&0&0&1&1&1\\ 1&1&0&0&1&1&0\\ 1&1&1&1&1&0&1\\ 0&0&1&1&0&0&0\\ 1&1&0&1&0&0&0\\ 0&1&1&1&0&1&0\\ 1&0&0&1&1&0&1 \end{bmatrix},$$

$$K_3^{-1} = \begin{bmatrix} 0&1&1&1&1&1&0\\ 1&0&1&1&1&1&0\\ 1&0&1&0&0&0&0\\ 0&0&1&0&1&0&0\\ 1&1&1&1&0&0&1\\ 0&0&1&1&1&1&1\\ 1&0&0&0&1&0&1 \end{bmatrix}, \quad K_4^{-1} = \begin{bmatrix} 1&0&0&1&0&1&0\\ 1&1&0&0&1&0&1\\ 0&1&1&0&1&0&1\\ 1&0&1&1&1&1&0\\ 0&1&1&0&0&0&0\\ 1&0&0&0&1&1&1\\ 1&0&1&0&0&1&0 \end{bmatrix},$$

$$K_5^{-1} = \begin{bmatrix} 1&0&0&0&0&1&1\\ 0&1&1&0&1&0&0\\ 1&0&0&1&0&1&0\\ 1&1&0&1&1&1&0\\ 0&0&0&1&0&1&1\\ 0&0&1&1&1&1&0\\ 0&1&0&1&1&1&0 \end{bmatrix}, \quad K_6^{-1} = \begin{bmatrix} 1&1&0&1&1&0&1\\ 0&0&1&0&1&1&0\\ 0&1&1&1&0&0&1\\ 1&1&0&1&0&0&1\\ 1&0&0&1&0&1&1\\ 1&0&1&1&1&0&0\\ 1&1&0&1&1&1&1 \end{bmatrix},$$

$$K_7^{-1} = \begin{bmatrix} 0&1&0&0&0&0&1\\ 1&1&1&1&0&1&0\\ 1&0&0&0&1&0&1\\ 0&1&0&0&1&0&1\\ 1&1&1&0&0&0&1\\ 1&0&1&0&1&1&1\\ 1&1&0&0&0&1&0 \end{bmatrix}, \quad K_8^{-1} = \begin{bmatrix} 0&1&1&0&0&0&0\\ 1&1&1&0&0&1&1\\ 1&0&0&0&1&1&0\\ 0&1&0&0&1&1&0\\ 0&0&0&1&0&1&1\\ 1&0&0&1&1&1&1\\ 1&0&1&0&1&1&0 \end{bmatrix}. \quad (4.6)$$

We can readily find that $K_i K_i^{-1} \bmod 2 = K_i^{-1} K_i \bmod 2 = I$.

On using the decryption algorithm presented in section 3.2, we get back the plaintext – All b̸ the b̸ .

On applying the encryption algorithm for the entire plaintext given by (4.3), we get the corresponding ciphertext as

1001011011001001111111111111001100100001001101 1
1001000110001011101100001011000001001010010111
1001011001100000000000011101000001000110110000 1
1101010111001001011101001110110101101001011110
1010110110001010100001101000000100011110111110 1
1100001000111110000110110101100000110010010010
1010100101010101101010110101100101101010100111
0000001100100010001010100101100011010010000110
1011101010101001100011 10. (4.7)

Then by applying the decryption algorithm on (4.7), we get back the plaintext given by (4.3).

5. Cryptanalysis

Let us consider the brute force attack on this cipher. The key K_0 is consisting of 56 numbers, which are equivalent to 392 binary bits. Thus the key space of the key under consideration is $2^{392} \approx (2^{10})^{40} \approx (10^3)^{40} = 10^{120}$. Hence, the cipher can never be broken by brute force attack.

Now let us examine the known plaintext attack.

$$P_i^1 = \langle K_i P_i^0 \bmod 2 \rangle = \langle K_i P_i^0 \rangle \bmod 2. \quad (5.1)$$

$$\begin{aligned} P_i^2 &= \langle K_i P_i^1 \bmod 2 \rangle = \langle K_i P_i^1 \rangle \bmod 2 \\ &= \langle K_i \langle K_i P_i^0 \rangle \bmod 2 \rangle \bmod 2 \\ &= \langle K_i \langle K_i P_i^0 \rangle\rangle \bmod 2. \end{aligned} \quad (5.2)$$

.

.

.

$$\begin{aligned} P_i^m &= \langle K_i \langle \ldots \langle K_i \langle K_i P_i^0 \bmod 2 \rangle \bmod 2 \\ &\quad \rangle \ldots \rangle \bmod 2 \rangle. \\ &= \langle K_i \langle \ldots \langle K_i \langle K_i P_i^0 \rangle \ldots \rangle\rangle\rangle \\ &\quad \bmod 2. \end{aligned} \quad (5.3)$$

Here, it is to be noted that the interlacing and the mod 2 operations are interchangeable.

On concatenating P_i^m, i =1 to n, we get the ciphertext C.

Thus

$$C = P_1^m \, P_2^m \ldots P_n^m . \quad (5.4)$$

Though we can have as many pairs of plaintext and ciphertext as we want, the sub keys K_i cannot be determined as the equation (5.3) is a peculiar nonlinear one in K as it involves interlacing and multiplication. Thus the ciphertext cannot be broken by the known plaintext attack.

6. Avalanche Effect

Taking the first eight characters of the plaintext namely, All b̸ the b̸ (see (4.3)), we have obtained the ciphertext given by (4.5). On changing the first character of the above plaintext from A to C (the ASCII codes of A and C differ in one bit), we obtain the corresponding ciphertext as

1110010011000000001100001010110010110000011
01010100010010. (6.1)

Comparing (4.5) and (6.1), we notice that the two ciphertexts differ in 29 bits out of 56 bits. This shows that the algorithm exhibits a strong avalanche effect.

Now we change the key in one bit. This is achieved by changing the number 9 to 8 in the key K_0 given by (4.1). Then we obtain the corresponding ciphertext for the plaintext – All ƀ the ƀ . This is given by

1011010001000011111100100000100011010110011001000000010111. (6.2)

On comparing (6.2) and (4.5), we readily notice that the ciphertexts differ in 22 bits out of 56 bits. It may be noted here that though the change in the key is only one bit out of 392 bits, the change in the corresponding ciphertext containing 56 bits is 22 bits. This also shows a pronounced avalanche effect.

7. Computational Experiments and Conclusions

In this paper, we have developed a block cipher for a block of size 56 bits. The length of the key is 392 bits, and it is represented as eight matrices, wherein each matrix is of size 7x7. The plaintext is represented by eight column vectors, wherein each one is of size 7x1. The development of the cipher essentially depends upon an iterative method and the modular arithmetic inverse of each of the key matrices.

The algorithms for the encryption and the decryption, given in section 3, are implemented in C language.

From the cryptanalysis presented in section 5, we have found that the cipher cannot be broken by any cryptanalytic attack.

Based on the analysis presented in this paper, we have seen that the cipher exhibits a strong avalanche effect.

Keeping all the above aspects in view, we conclude that the cipher is a very interesting one and it cannot be broken by any cryptanalytic attack.

References

[1] William Stallings, “Cryptography and Network Security: Principles and Practices”, Third edition, 2003, Chapter 2, pp.37.

[2] Feistel, H. “Cryptography and Computer Privacy”, Scientific American, vol. 228, No. 5, pp.15-23, 1973.

[3] Feistel, H., Notz. W., and Smith, J. “Some Cryptographic Techniques for Machine-to-Machine Data Communications”, Proceedings of the IEEE, vol. 63, No. 11, pp. 1545-1554, Nov. 1975.

[4] V.U.K.Sastry, V.Janaki, “On the Modular Arithmetic Inverse in the

Cryptology of Hill Cipher”, Proceedings of North American Technology and Business Conference, September 2005, Montreal, Canada.

Appendix A

As an example consider the interlacing of the column vectors Q_1^1, Q_2^1, and Q_3^1 given below in Fig.1.

$$Q_1^1 = \begin{bmatrix} a \\ b \\ c \\ d \\ e \\ f \\ g \end{bmatrix} \quad Q_2^1 = \begin{bmatrix} h \\ i \\ j \\ k \\ l \\ m \\ n \end{bmatrix} \quad Q_3^1 = \begin{bmatrix} o \\ p \\ q \\ r \\ s \\ t \\ u \end{bmatrix}$$

$$[a \; b \; c \; d \; e \; f \; g \; h \; i \; j \; k \; l \; m \; n \; o \; p \; q \; r \; s \; t \; u]$$

$$P_1^1 = \begin{bmatrix} u \\ r \\ o \\ l \\ i \\ f \\ c \end{bmatrix} \quad P_2^1 = \begin{bmatrix} t \\ q \\ n \\ k \\ h \\ e \\ b \end{bmatrix} \quad P_3^1 = \begin{bmatrix} s \\ p \\ m \\ j \\ g \\ d \\ a \end{bmatrix}$$

Figure1. Interlacing of three column vectors.

The column vectors are placed one adjacent to the other in a row as shown Fig.1. Then the elements in the row are arranged in the column vectors P_1^1, P_2^1, and P_3^1 as shown in Fig.1.

Thus we get

$P_i^1 = < Q_1^1 >$, i = 1 to 3.

The process of decomposition is shown in Fig.2.

$$P_1^1 = \begin{bmatrix} u \\ r \\ o \\ l \\ i \\ f \\ c \end{bmatrix} \quad P_2^1 = \begin{bmatrix} t \\ q \\ n \\ k \\ h \\ e \\ b \end{bmatrix} \quad P_3^1 = \begin{bmatrix} s \\ p \\ m \\ j \\ g \\ d \\ a \end{bmatrix}$$

$$[a \; b \; c \; d \; e \; f \; g \; h \; i \; j \; k \; l \; m \; n \; o \; p \; q \; r \; s \; t \; u]$$

$$Q_1^1 = \begin{bmatrix} a \\ b \\ c \\ d \\ e \\ f \\ g \end{bmatrix} \quad Q_2^1 = \begin{bmatrix} h \\ i \\ j \\ k \\ l \\ m \\ n \end{bmatrix} \quad Q_3^1 = \begin{bmatrix} o \\ p \\ q \\ r \\ s \\ t \\ u \end{bmatrix}$$

Figure 2. Decomposition into three column vectors

Hence we get

$Q_1^1 => P_i^1 <$, i = 1 to 3.

It may be noted here that the process of interlacing and decomposition are reversible.