Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/170411

Creation of a Cryptosystem that Satisfies Shannon's Perfect Secrecy Condition Based on the Lieb-Liniger Model

Mukhayo Yunusovna Rasulova

Institute of Nuclear Physics, Academy of Sciences of Uzbekistan, Tashkent, 100214 Uzbekistan

Received: 25 Mar. 2023, Revised: 2 May 2023, Accepted: 15 Jun. 2023
Published online: 1 Jul. 2023

Abstract: The paper proposes the Lieb-Liniger model of statistical mechanics for creating a cryptosystem that satisfies the Shannon perfect secrecy condition.

Keywords: statistical physics, Lieb-Liniger Model, advanced encryption system, tree-pass protocol.

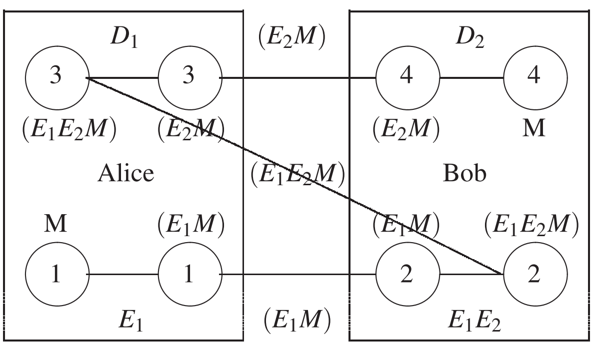
1 Introduction

One of the most pressing problems of our time is the creation of a cryptosystem that satisfies Shannon's conditions of perfect secrecy [1], [2]. This problem was posed by Shannon back in 1948 and remains relevant to this day. Advanced Encryption Standard [3], which is the basis of the Western system, and other standards could not solve this problem because they are probabilistic in nature and this does not allow them to determine their own keys for each cell of information.

Such an opportunity can be created if it is possible to solve the equation of functions N variables, where N is the number of information cells. There are several exactly solvable such equations in the world, and one of the possible applications of the problem of a perfect secret cryptosystem is the Lieb-Liniger model [4] of statistical mechanics.

As is known, in well-known cryptosystems, several cells are used to express each letter of the alphabet, and such letters have different ciphertext probabilities. This can be easily used to break the encoded information. The definition of a complete system of own keys for each cell based on the Lieb-Liniger model, due to the equal probability of letters in each cell, does not allow information hacking. Therefore, this model allows you to create a cryptosystem that satisfies the conditions of perfect secrecy of information.

To solve the Shannon problem, the second chapter of this paper considers the Lieb-Liniger model. In the third chapter, using the Lieb-Liniger model, using the eight cell information, information transfer based on the three-pass protocol [5] is shown (see figure below). In the third chapter, also, this method of information transfer is translated into matrix language. In the fourth chapter, the Lieb-Lineger based information transfer method is proved to create a perfect secrecy cryptosystem. The last chapter is devoted to the conclusion.



* Corresponding author e-mail: rasulova@live.com

2 Bethe Ansatz for Bose gas

Following [4], consider the solution of the time independent Schrödinger equation for s particles interacting with the potential in the form of a delta function

$$\delta(|x_i - x_j|) = \{^{\infty,}_{0} \quad ^{if}_{if} \quad ^{x_i = x_j,}_{x_i \neq x_j}.$$

in one-dimensional space $\mathbb{R}$:

$$-\frac{\hbar^2}{2m}\sum_{i=1}^{s} \triangle_i \psi(x_1, x_2, \dots, x_s) +$$

$$2c \sum_{1 \le i < j \le s} \delta(x_i - x_j)\psi(x_1, x_2, \dots, x_s) =$$

$$E\psi(x_1, x_2, \dots, x_s), \tag{1}$$

where the constant $c \geq 0$ and 2c is the amplitude of the delta function, $m = 1$-massa of boson, $\hbar = 1$-Plank constant, $\triangle$-Laplasian, the domain of the problem is defined in $\mathbb{R}$: all $0 \leq x_i \leq L$ and the wave function ψ satisfies the periodicity condition in all variables. In [3], it was proved that defining a solution ψ in $\mathbb{R}$ is equivalent to defining a solution to the equation

$$-\sum_{i=1}^{s} \frac{1}{2m} \triangle_{x_i} \psi = E\psi,$$

with the boundary condition

$$(\frac{\partial \psi}{\partial x_j} - \frac{\partial \psi}{\partial x_k})|_{x_j = x_{k+0}} - (\frac{\partial \psi}{\partial x_j} - \frac{\partial \psi}{\partial x_k})|_{x_j = x_{k-0}} = 2c\psi|_{x_j = x_k}, \tag{2}$$

$\mathbb{R}_1 : 0 < x_1 < x_2 < \dots < x_s < L$ and the initial periodicity condition is equivalent to the periodicity conditions in

$$\psi(0, x_1, ..., x_s) = \psi(x_1, ..., x_s, L),$$

$$\frac{\partial \psi(x, x_2, ..., x_s)}{\partial x}|_{x=0} = \frac{\partial \psi(x_2, ..., x_s, x)}{\partial x}|_{x=L}.$$

Using equation (2) we can determine the solution of equation (1) in the form of the Bethe ansatz [4], [6], [7], [8]:

$$\psi(x_1, \dots, x_s) = \sum_P a(P) P exp\left(i\sum_{i=1}^{s} k_{P_i} x_i\right) \tag{3}$$

in the region $\mathbb{R}_1$ with eigenvalue $E_s = \sum_{i=1}^{s} k_i^2$ where the summation is performed over all permutations P of the numbers $\{k\} = k_1, \dots, k_s$ and $a(P)$ is a certain coefficient depending on P:

$$a(Q) = -a(P)exp(i\theta_{i,j}),$$

where $\theta_{i,j} = \theta(k_i - k_j)$, $\theta(r) = -2\arctan(r/c)$ and when r is a real value and $-\pi \leq \theta(r) \leq \pi$.

For the case $s = 2$, one can find [4], [7], [9], [10], [11]:

$$a_{1,2}(k_1, k_2)e^{i(k_1x_1 + k_2x_2)} + a_{2,1}(k_1, k_2)e^{i(k_2x_1 + k_1x_2).}$$

and

$$ik_2a_{1,2} + ik_1a_{2,1} - ik_1a_{1,2} - ik_2a_{2,1} = c(a_{1,2} + a_{2,1}),$$

or

$$a_{2,1} = -\frac{c - (k_2 - k_1)}{c + (k_2 - k_1)}a_{1,2}$$

If we choose

$$a_{1,2} = e^{i(k_1x_1 + k_2x_2)}$$

one gets

$$e^{i(k_2x_1 + k_1x_2)} = -\frac{c - (k_2 - k_1)}{c + (k_2 - k_1)}e^{i(k_1x_1 + k_2x_2)} =$$

$$-e^{i\theta_{2,1}}e^{i(k_1x_1 + k_2x_2)}. \tag{4}$$

3 Application of Bethe ansatz in information technology

Let's consider how the last equation can be used for three-stage information transfer. Let Alice encrypt information

$$M = e^{i(k_1x_1 + k_2x_2 + k_3x_3 + k_4x_4 + k_5x_5 + k_6x_6 + k_7x_7 + k_8x_8)}$$

using the encryption key

$$E_1 = e^{i\theta_{2,1}}e^{i\theta_{1,2}}e^{i\theta_{8,3}}e^{i\theta_{5,4}}e^{i\theta_{4,5}}e^{i\theta_{7,6}}e^{i\theta_{6,7}}e^{i\theta_{3,8}}$$

and send encrypted information to Bob:

$$(E_1, M) =^{i\theta_{2,1}} e^{i\theta_{1,2}}e^{i\theta_{8,3}}e^{i\theta_{5,4}}e^{i\theta_{4,5}}e^{i\theta_{7,6}}e^{i\theta_{6,7}}e^{i\theta_{3,8}} \times$$

$$e^{i(k_2x_1 + k_1x_2 + k_8x_3 + k_5x_4 + k_4x_5 + k_7x_6 + k_6x_7 + k_3x_8)} =$$

$$e^{i(k_2x_1 + k_1x_2 + k_8x_3 + k_5x_4 + k_4x_5 + k_7x_6 + k_6x_7 + k_3x_8)}.$$

In M in binary, $k_1 = 0$, $k_2 = 1$, $k_3 = 0$, $k_4 = 1$, $k_5 = 0$, $k_6 = 0$, $k_7 = 1$, $k_8 = 1$.

(In this case, in binary

$$(E_1, M) = e^{i(1x_1 + 0x_2 + 1x_3 + 0x_4 + 1x_5 + 1x_6 + 0x_7 + 0x_8)}).$$

Bob receives this information and encrypts it with his key:

$$E_2 = e^{i\theta_{5,1}}e^{i\theta_{4,2}}e^{i\theta_{2,3}}e^{i\theta_{3,4}}e^{i\theta_{8,5}}e^{i\theta_{7,6}}e^{i\theta_{6,7}}e^{i\theta_{1,8}}$$

and sends the double-encrypted information back to Alice:

$$(E_2(E_1,M)) = e^{i\theta_{5,1}}e^{i\theta_{4,2}}e^{i\theta_{2,3}}e^{i\theta_{3,4}}e^{i\theta_{8,5}}e^{i\theta_{7,6}}e^{i\theta_{6,7}}e^{i\theta_{1,8}}\times$$
$$e^{i(k_2x_1+k_1x_2+k_8x_3+k_5x_4+k_4x_5+k_7x_6+k_6x_7+k_3x_8)} =$$
$$e^{i(k_5x_1+k_4x_2+k_2x_3+k_3x_4+k_8x_5+k_7x_6+k_6x_7+k_1x_8)}.$$

(In binary

$$(E_2(E_1,M)) = e^{i\theta_{5,1}}e^{i\theta_{4,2}}e^{i\theta_{2,3}}e^{i\theta_{3,4}}e^{i\theta_{8,5}}e^{i\theta_{7,6}}e^{i\theta_{6,7}}e^{i\theta_{1,8}}\times$$
$$e^{i(1x_1+0x_2+1x_3+0x_4+1x_5+1x_6+0x_7+0x_8)} =$$
$$e^{i(1x_1+0x_2+0x_3+1x_4+0x_5+0x_6+1x_7+1x_8)}).$$

Having received the latest information from Bob, Alice decrypts it with her key

$$D_1 = e^{i\theta_{2,1}}e^{i\theta_{1,2}}e^{i\theta_{8,3}}e^{i\theta_{5,4}}e^{i\theta_{4,5}}e^{i\theta_{7,6}}e^{i\theta_{6,7}}e^{i\theta_{3,8}}:$$

$$(D_1(E_2(E_1,M))) = e^{i\theta_{2,1}}e^{i\theta_{1,2}}e^{i\theta_{8,3}}e^{i\theta_{5,4}}e^{i\theta_{4,5}}e^{i\theta_{7,6}}e^{i\theta_{6,7}}\times$$
$$e^{i\theta_{3,8}}e^{i(k_5x_1+k_4x_2+k_2x_3+k_3x_4+k_8x_5+k_7x_6+k_6x_7+k_1x_8)} =$$
$$= e^{i(k_2x_1+k_1x_2+k_8x_3+k_5x_4+k_4x_5+k_7x_6+k_6x_7+k_3x_8)}$$

(In binary

$$(D_1(E_2(E_1,M))) = e^{i\theta_{2,1}}e^{i\theta_{1,2}}e^{i\theta_{8,3}}e^{i\theta_{5,4}}e^{i\theta_{4,5}}e^{i\theta_{7,6}}e^{i\theta_{6,7}}\times$$
$$e^{i\theta_{3,8}}e^{i(1x_1+0x_2+0x_3+1x_4+0x_5+0x_6+1x_7+1x_8)} =$$
$$= e^{i(0x_1+1x_2+1x_3+0x_4+1x_5+1x_6+0x_7+0x_8)})$$

and send it back to Bob. Now the information is covered by Bob's key just one time.

Bob, having received this information, decrypts it with his decoder key

$$D_2 = e^{i\theta_{8,1}}e^{i\theta_{3,2}}e^{i\theta_{4,3}}e^{i\theta_{2,4}}e^{i\theta_{1,5}}e^{i\theta_{7,6}}e^{i\theta_{6,7}}e^{i\theta_{5,8}}$$

$$(D_2(D_1(E_2(E_1,M)))) = e^{i\theta_{8,1}}e^{i\theta_{3,2}}e^{i\theta_{4,3}}e^{i\theta_{2,4}}e^{i\theta_{1,5}}e^{i\theta_{7,6}}\times$$
$$e^{i\theta_{6,7}}e^{i\theta_{5,8}}e^{i(k_2x_1+k_1x_2+k_8x_3+k_5x_4+k_4x_5+k_7x_6+k_6x_7+k_3x_8)} =$$
$$e^{i(k_8x_1+k_3x_2+k_4x_3+k_2x_4+k_1x_5+k_7x_6+k_6x_7+k_5x_8)}.$$

(In binary

$$(D_2(D_1(E_2(E_1,M)))) = e^{i\theta_{8,1}}e^{i\theta_{3,2}}e^{i\theta_{4,3}}e^{i\theta_{2,4}}e^{i\theta_{1,5}}e^{i\theta_{7,6}}\times$$
$$e^{i\theta_{6,7}}e^{i\theta_{5,8}}e^{i(0x_1+1x_2+1x_3+0x_4+1x_5+1x_6+0x_7+0x_8)} =$$
$$e^{i(0x_1+1x_2+0x_3+1x_4+0x_5+0x_6+1x_7+1x_8)}).$$

Therefore

$$(D_2(D_1(E_2(E_1,X)))) =$$
$$e^{i(0x_1+1x_2+0x_3+1x_4+0x_5+0x_6+1x_7+1x_8)} = M.$$

The latest information matches the information that Alice wanted to send to Bob.

To adapt the results obtained in Chapter 3 for modern computers, which are based on matrix coding, we introduce a permutation operator P, which we denote as follows:

$$e^{i(k_2x_1+k_1x_2)} = \sum_{i=0}^{\infty}\frac{i^n}{n!}(k_2x_1+k_1x_2)^n =$$

$$\sum_{i=0}^{\infty}\frac{i^n}{n!}(\begin{bmatrix}x_1 & x_2\end{bmatrix}\begin{bmatrix}k_2\\ k_1\end{bmatrix})^n = \sum_{i=0}^{\infty}\frac{i^n}{n!}(\begin{bmatrix}x_1 & x_2\end{bmatrix}P\begin{bmatrix}k_1\\ k_2\end{bmatrix})^n.$$

From the last equation, after taking the logarithm, we obtain equality:

$$E_1=\begin{array}{|c|c|c|c|c|c|c|c|}\hline & 1 & & & & & & \\ \hline 1 & & & & & & & \\ \hline & & & & & & & 1 \\ \hline & & & & 1 & & & \\ \hline & & & 1 & & & & \\ \hline & & & & & & 1 & \\ \hline & & & & & 1 & & \\ \hline & & 1 & & & & & \\ \hline\end{array}$$

$$E_2=\begin{array}{|c|c|c|c|c|c|c|c|}\hline & & & & 1 & & & \\ \hline & & & 1 & & & & \\ \hline & 1 & & & & & & \\ \hline & & 1 & & & & & \\ \hline & & & & & & & 1 \\ \hline & & & & & & 1 & \\ \hline & & & & & 1 & & \\ \hline 1 & & & & & & & \\ \hline\end{array}$$

$$D_1=\begin{array}{|c|c|c|c|c|c|c|c|}\hline & 1 & & & & & & \\ \hline 1 & & & & & & & \\ \hline & & & & & & & 1 \\ \hline & & & & 1 & & & \\ \hline & & & 1 & & & & \\ \hline & & & & & & 1 & \\ \hline & & & & & 1 & & \\ \hline & & 1 & & & & & \\ \hline\end{array}$$

$$D_2=\begin{array}{|c|c|c|c|c|c|c|c|}\hline & & & & & & & 1 \\ \hline & & 1 & & & & & \\ \hline & & & 1 & & & & \\ \hline & 1 & & & & & & \\ \hline 1 & & & & & & & \\ \hline & & & & & & 1 & \\ \hline & & & & & 1 & & \\ \hline & & & & 1 & & & \\ \hline\end{array}$$

Matrices E_1 and E_2 are commutative:

$$E_1 \times E_2 = \begin{bmatrix} &1&&&&&& \\ 1&&&&&&& \\ &&&&&&&1 \\ &&&&1&&& \\ &&&1&&&& \\ &&&&&&1& \\ &&&&&1&& \\ &&1&&&&& \end{bmatrix} \times$$

$$\begin{bmatrix} &&&&1&&& \\ &&&1&&&& \\ &1&&&&&& \\ &&1&&&&& \\ &&&&&&&1 \\ &&&&&&1& \\ &&&&&1&& \\ 1&&&&&&& \end{bmatrix} =$$

$$E_2 \times E_1 = \begin{bmatrix} &&&&1&&& \\ &&&1&&&& \\ &1&&&&&& \\ &&1&&&&& \\ &&&&&&&1 \\ &&&&&&1& \\ &&&&&1&& \\ 1&&&&&&& \end{bmatrix} \times$$

$$\begin{bmatrix} &1&&&&&& \\ 1&&&&&&& \\ &&&&&&&1 \\ &&&&1&&& \\ &&&1&&&& \\ &&&&&&1& \\ &&&&&1&& \\ &&1&&&&& \end{bmatrix} =$$

$$\begin{bmatrix} &&&1&&&& \\ &&&&1&&& \\ 1&&&&&&& \\ &&&&&&&1 \\ &&1&&&&& \\ &&&&&1&& \\ &&&&&&1& \\ &1&&&&&& \end{bmatrix}.$$

We can also show that $D_1 = E_1^{-1}$ is inverse to E_1 and:

$$D_1 \times E_1 = \begin{bmatrix} &1&&&&&& \\ 1&&&&&&& \\ &&&&&&&1 \\ &&&&1&&& \\ &&&1&&&& \\ &&&&&&1& \\ &&&&&1&& \\ &&1&&&&& \end{bmatrix} \times$$

$$\begin{bmatrix} &1&&&&&& \\ 1&&&&&&& \\ &&&&&&&1 \\ &&&&1&&& \\ &&&1&&&& \\ &&&&&&1& \\ &&&&&1&& \\ &&1&&&&& \end{bmatrix} =$$

$$\begin{bmatrix} 1&&&&&&& \\ &1&&&&&& \\ &&1&&&&& \\ &&&1&&&& \\ &&&&1&&& \\ &&&&&1&& \\ &&&&&&1& \\ &&&&&&&1 \end{bmatrix}.$$

Similarly, $D_2 = E_2^{-1}$ and

$$D_2 \times E_2 = \begin{bmatrix} &&&&&&&1 \\ &&1&&&&& \\ &&&1&&&& \\ &1&&&&&& \\ 1&&&&&&& \\ &&&&&&1& \\ &&&&&1&& \\ &&&&1&&& \end{bmatrix} \times$$

$$\begin{bmatrix} &&&&1&&& \\ &&&1&&&& \\ &1&&&&&& \\ &&1&&&&& \\ &&&&&&&1 \\ &&&&&&1& \\ &&&&&1&& \\ 1&&&&&&& \end{bmatrix} =$$

$$\begin{bmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & 1 & \\ & & & & & & & 1 \end{bmatrix}.$$

Let the initial information in a binary representation have the form:

$$M=\begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}.$$

Then

$$E_1M=\begin{bmatrix} & 1 & & & & & & \\ 1 & & & & & & & \\ & & & & & & & 1 \\ & & & & 1 & & & \\ & & & 1 & & & & \\ & & & & & & 1 & \\ & & & & & 1 & & \\ & & 1 & & & & & \end{bmatrix} \times \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix},$$

$$E_2E_1M = \begin{bmatrix} & & & & 1 & & & \\ & & & 1 & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & & & & & 1 \\ & & & & & & 1 & \\ & & & & & 1 & & \\ 1 & & & & & & & \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix},$$

$$D_1E_2E_1M = \begin{bmatrix} & 1 & & & & & & \\ 1 & & & & & & & \\ & & & & & & & 1 \\ & & & & 1 & & & \\ & & & 1 & & & & \\ & & & & & & 1 & \\ & & & & & 1 & & \\ & & 1 & & & & & \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

$$D_2D_1E_2E_1M = \begin{bmatrix} & & & & & & & 1 \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & 1 & & & & & & \\ 1 & & & & & & & \\ & & & & & & 1 & \\ & & & & & 1 & & \\ & & & & 1 & & & \end{bmatrix} \times \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} = M.$$

4 Shannon’s perfect secrecy cryptosystem

The proposed permutations in chapter 2 (4) provide the perfect secrecy of information.

As is known, the necessary and sufficient conditions for the system to be perfectly secret can be formulated in the form of Bayes’ theorem:

Theorem *A necessary and sufficient condition for perfect secrecy is that*

$$p_M(C) = p(C)$$

for all M and C, i.e. $p_M(C)$ should not depend on M. Indeed, according to the Shannon formula:

$$p_C(M) = \frac{p(M) \times p_M(C)}{p(C)}, \qquad (5)$$

where $p(M)$ - prior probability of message M;

$p_M(C)$ - the conditional probability of the cryptogram C, provided that the message M is selected, i.e. the sum of the probabilities of all those keys that translate the message M into a cryptogram C;

$p(C)$ - probability of receiving a cryptogram C;

$p_C(M)$ - posterior probability of the message M, provided that the cryptogram C is intercepted.

For the system to be perfect secrecy [12], [13] the values $p_C(M)$ and $p(M)$ must be equal for all C and M.

Therefore, one of the equalities must be satisfied: either $p(M) = 0$ this the solution must be discarded, since it is required that the equality be carried out for any value of $p(M)$), or

$$p_M(C) = p(C)$$

for any M and C.

Conversely, if $p_M(C) = p(C)$, then $p_C(M) = p(M)$, and the system is perfect secrecy.

Indeed, let us have plaintext M with $N = 8$ letters $k_i \in M$ with equal probabilities $p(k_i) = \frac{1}{8}$. Suppose we have plaintext cell k_i, $(1 \le i \le 8)$ and suppose these plaintext cells appear in the text with frequencies $p(k_i) = \frac{1}{8}$ and consequently, $p(M) = \sum_{1 \le i \le 8} p_i = 1$.

In our system for each plaintext cell, k_i and ciphertext cell $k_j \in C$ there is exactly one key, such as $K(k_{i,j})k_i = k_j$.

The probabilities of these keys are equal and $p_K(k_{i,j}) = \frac{1}{8}$ consequently $p_M(C) = \sum_{1 \le i \le 8} K(k_{i,j}) = 1$.

If we have the probabilities $p(k_i)$ and of keys $p_K(k_{i,j}) = \frac{1}{8}$, we provide to find the probability of ciphertext $p(k_j)$ using the formula

$$p(k_j) = \sum_{1 \le i \le 8} p(k_i) p_K(k_{i,j}).$$

When all keys are independent, each key has an equal probability of $1/8$, so we can replace $p_K(k_{i,j}) = \frac{1}{8}$. Accordingly, we can obtain

$$p(k_j) = \frac{1}{8} \sum_{1 \le i \le 8} p(k_i). \qquad (6)$$

In our system for each plaintext cell, k_i and ciphertext cell k_j there is exactly one key like that, $K(k_{i,j})$. Therefore, each occurs exactly once in the last sum (6), so we have $\frac{1}{8} \sum_{1 \le i \le 8} p(k_i)$ for probability of cell of ciperhtext.

But the sum of the probabilities of all possible plaintexts cells k_i is 1, so we obtain $p(k_j) = \frac{1}{8}$ and $p(C) = \sum_{1 \le j \le 8} p(k_j) = 1$. Hence, every ciphertext occurs with an equal probability and

$$p_M(C) = p(C).$$

Therefore, from Shannon equality (5) when $p(M) = p(C) = 1$, we get

$$p_M(C) = p(C).$$

This proves that our system has perfect secrecy.

5 Conclusion

This work proposes a new encryption method based on the Lieb-Liniger model, which allows the translation to provide for each cell its own encryption transformation. For this purpose, we use the solutions of the Schr*ö*dinger equation for the boson system interacting with the potential in the form of a delta function.

The advantages of this algorithm and information transfer method:

1. Complete diffusion of component bits at each stage of information transfer.
2. The cost-effectiveness of the algorithm, since good diffusion is provided by a small number of bits. If modern programs require 5 cells to express letters, then in our approach it is possible to express letters in one cell.
3. Since each information cell has its own transformation, it follows that the prior probabilities and posterior probabilities of each cell are 1/N (where N is the number of information cells), which means that the system satisfies the Shannon perfect secrecy condition.
4. Equality of zero correlation between plaintext and ciphertext, which is a condition for perfect encryption.
5. The lack of a key transfer process between partners is the most dangerous part of information transfer.
6. Possibility of programming the direction of propagation of bosons in one-dimensional space.

References

[1] C.E.Shannon, A mathematical theory of communication, *Bell System Technical Journal*, **27**(3), 379-423 (1948).
[2] C.E.Shannon, A mathematical theory of communication, *Bell System Technical Journal*, **27**(4), 623-656 (1948).
[3] J.Daemen, V.Rijmen, The Design of Rijndael AES-The Advanced Encryption Standard, Springer, (2002).
[4] E.H.Lieb and W.Liniger, Exact analysis of an interacting Bose gas. I: the general solution and the ground state, *Phys. Rev.*, **130**, 1605-1616 (1963).
[5] A.Shamir, R.L.Rivest, L.M.Adleman, *Mental Poker*, In: Editor D. A. Klarner, The Mathematical Gardner, Wadsworth. 37-43, (1981).

[6] H.A.Bethe, On the theory of metals, I. Eigenvalues and eigenfunctions of a linear chain of atoms,(German), *Zeits. Phys.*, 205-226 (1931).
[7] A.Craig, I.Tracy and J.Harold Widom, The dynamics of the one-dimensional delta-function Bose gas, *Phys. A: Math. Theor.*, **41**, (485204) (2008).
[8] M.Brokate and M.Yu.Rasulova, *The Solution of the Hierarchy of Quantum Kinetic Equations with Delta Potential*, In:Editor Siddiqi A.H., Manchanda P. Industrial Mathematics and Complex Systems. Springer, Singapour, 165-170, (2017).
[9] M.Yu.Rasulova, The Solution of Quantum Kinetic Equation with Delta Potential and its Application for Information Technology, *Appl.Math.Inf.Sciences*, **12** (4), 685-688 (2018).
[10] M.Yu.Rasulova, The BBGKY Hierarchy of Quantum Kinetic Equations and Its Application in Cryptography. *Physics of Particles and Nuclei*, **51**(4), 781-785 (2020).
[11] Mukhayo Rasulova and Jakhongir Yunusov, Definition of a three-pass protocol using the Lieb-Liniger Model, *Appl.Math.Inf.Sciences*, **15**(6), 677-680 (2021).
[12] D.Stinson, *Cryptography:Theory and Practice. Second edition*, Chapman and Hall/CRC Press (2002).
[13] W. Trappe, L.C.Washington: *Introduction to Cryptography with Coding Theory*, Pearson Education (2006).

Mukhayo Yunusovna Rasulova earned her B.Sc. and M.Sc. in Theoretical Physics from Tashkent State University, Uzbekistan in 1971. She earned her Ph.D. degree from the Institute of Theoretical Physics, Ukraine National Academy of Sciences in Kiev, Ukraine in 1978 and a doctoral degree of sciences in Mathematics and Physics from the Institute of Nuclear Physics, Uzbekistan Academy of Sciences, Tashkent, Uzbekistan, in 1995. Her main research work belongs to the field of Theoretical and Mathematical Physics. Her scientific interests are devoted to investigation of kinetic and thermodynamic properties of systems interacting with different potential particles using the Bogoluibob-Born-Green-Kirkwood-Yvon's hierarchy of quantum kinetic equations. Also, her current research work is devoted to studying statistical and kinetic properties of nonlinear optics, the theory of quantum information and cryptography. She has more then 100 scientific publications in the field of Statistical Physics, Theoretical and Mathematical Physics. She has been an invited speaker at many international conferences. She is an academician of the International Academy of Creative Endeavors.