Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/190502

Using Bethe Ansatz in the Lieb-Liniger Model for Cryptographic Applications

Mukhayo Yunusovna Rasulova

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

Received: 12 Jan. 2025, Revised: 22 May 2025, Accepted: 19 Jun. 2025
Published online: 1 Sep. 2025

Abstract: This paper explores the use of the Bethe ansatz method of the Lieb-Liniger model with collision coefficients to create cryptographic protocols. The Bethe ansatz method, traditionally used to describe quantum systems with strong correlations, is used to construct wave functions in systems consisting of particles with interactions. An important element is the role of collision coefficients, which affect the structure of wave functions and the spectrum of the system. The paper analyzes how these coefficients can be used to develop new methods in the field of quantum cryptography, proposing approaches for creating secure cryptographic systems. The proposed approach opens up new opportunities for the use of quantum computations and interactions in the development of secure protocols, which has significant potential for strengthening cryptographic resistance in modern information technologies.

Keywords: statistical physics, Lieb-Liniger Model, Bethe ansatz, tree-pass protocol

1 Introduction

Modern cryptography increasingly turns to the fundamental structures of theoretical physics in search of computationally difficult problems that are resistant to quantum attacks. One such direction is the use of integrable quantum models with a rigorous mathematical structure and nontrivial combinatorics of states. Of particular interest is the Lieb-Liniger model [1], which describes a one-dimensional boson gas with delta interaction, whose states can be accurately described by the Bethe ansatz method [2]. In traditional physics, the Bethe ansatz is used to construct wave functions and analyze the spectral properties of a system. However, recent work [3], [4], [5], [6], [7], [8] has shown that the entire set of solutions to the Bethe equations can be viewed as a discrete space with potential for cryptographic coding. The full set of Bethe roots determined by the quantization and interaction conditions defines a highly organized but difficult to invert structure suitable for constructing keys, hash functions, and information exchange protocols. The aim of this paper is to theoretically justify and construct a cryptographic scheme based on complete information about the configuration of Bethe roots, considering them as fundamental cryptographic primitives.

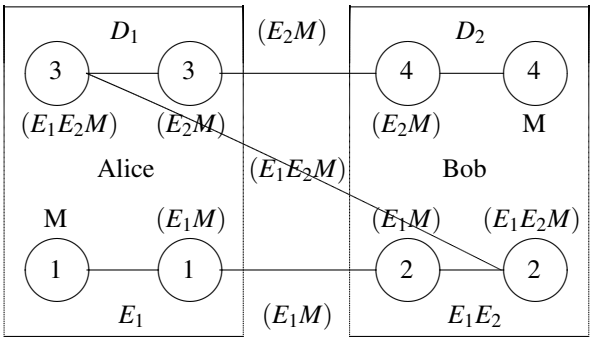

Fig. 1: Flow chart illustrating a communication process between two entities, Alice and Bob, represented by two blue sections.

Each section contains circles connected by arrows, indicating the flow of information. The chart includes probability expressions such as $P(E_B,E_A), P(E_B)$, and $P(E_A)$, showing the relationships and dependencies between different events or states. The diagram

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

emphasizes the interaction and data exchange between Alice and Bob.

2 Bethe Ansatz for Bose gas

Following [1], consider the solution of the time independent Schrödinger equation for s particles interacting with the potential in the form of a delta function

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

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

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

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

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

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

$$(\frac{\partial}{\partial x_{j+1}} - \frac{\partial}{\partial x_j})\psi|_{x_{j+1}=x_j} = c\psi|_{x_{j+1}=x_j}, \tag{2}$$

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

$$\psi(0,x_2,...,x_s) = \psi(x_2,...,x_s,L),$$

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

Using equation (2) we can determine the solution of equation (1) in the form of the Bethe ansatz [1], [2], [10], [3]:

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

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 $\{k\} = k_1,\ldots,k_s$ and $a(P)$ is a certain coefficient depending on *Perm*:

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

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 [1], [10], [4], [5], [6]:

$$\psi(x_1,x_2) = a_{1,2}(k_1,k_2)e^{i(k_1x_1+k_2x_2)} + a_{2,1}(k_1,k_2)e^{i(k_2x_1+k_1x_2)}.$$

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

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

For two bosons with wave numbers k_1 and k_2, the amplitudes $a(P)$ take two values:

If the order is $P(1,2)$ then $a(P) = 1$.

If the order is $P(2,1)$ then $a(P) = S(k_2,k_1)$, where ratio of $a(k_1,k_2)$ and $a(k_2,k_1)$ can be interpreted as the scattering matrix of the two bosons with wave numbers k_1,k_2

$$S(k_1,k_2) = \frac{a(k_2,k_1)}{a(k_1,k_2)}. \tag{4}$$

If we consider a permutation of two bosons, where k_1 and k_2 are their wave numbers, then the wave function corresponding to the changed order $x_1 > x_2$ is related to the original wave function (where $x_1 < x_2$) via the scattering operator. The general form of the wave function will be:

$$\psi(x_1,x_2) = exp(ik_1x_1 + ik_2x_2)+$$

$$S(k_2,k_1)exp(ik_2x_1 + ik_1x_2).$$

If we consider a permutation of two bosons, where k_1 and k_2 are their wave numbers, then the wave function corresponding to the changed order $x_1 > x_2$ is related to the original wave function (where $x_1 < x_2$) via the scattering operator. This is written as [9]:

$$e^{i(k_2x_1+k_1x_2)} = S(k_1,k_2)e^{i(k_1x_1+k_2x_2)}$$

or

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

$$-e^{i\theta(k_1,k_2)}e^{i(k_1x_1+k_2x_2)}, \tag{5}$$

where $\theta(k_1,k_2)$ - phase shift depending on the wave numbers of bosons k_1 and k_2 and $S(k_1,k_2)$ is scattering matrix (4). In integrable systems such as the Lieb-Liniger Model, the unitarity $|e^{i\theta(k_1,k_2)}| = 1$ of the S-matrix,

$$S(k_1,k_2)S(k_2,k_1) = 1 \tag{6}$$

is satisfied automatically, since the interaction of bosons is described by elastic collisions in which energy, momentum, and probability are conserved and the S -

matrix describes only the phase shift without changing the amplitudes of the interacting bosons.

For the $s-$particle wave function (3) $\psi(x_1,...x_s)$, where $x_1 < x_2 < ... < x_s$, the amplitudes $a(P)$ are given in terms of the scattering matrices as follows [10]:

$$a(P) = \prod_{i<j} S(k_{P(i)}, k_{P(j)}), \tag{7}$$

where $S(k_i,k_j)$ - scattering amplitude of bosons with wave numbers k_i and k_j.

For an arbitrary permutation P, the amplitude is obtained as the product of all scattering coefficients that correspond to the sequence of exchanges between pairs of bosons required to achieve the permutation P from the base order (e.g. $P_0 = (1,2,...,s)$).

In previous works, we developed the cryptographic application for the first term of the Bethe ansatz. We limited ourselves to considering only the first term of the Bethe ansatz. In this work we will develop this method for the entire Bethe ansatz, that is, we will take into account all the terms of the Bethe ansatz.

To this end, we will show for a two-particle system of bosons the relation Let us consider the product of ab and ba, where

$$a = -\frac{c - i(k_j - k_i)}{c + (k_j - k_i)}$$

and

$$b = -\frac{c - i(k_l - k_f)}{c + (k_l - k_f)}.$$

Calculating AB:

$$(-\frac{c - i(k_j - k_i)}{c + i(k_j - k_i)})(-\frac{c - i(k_l - k_f)}{c + i(k_l - k_f)})$$

Since the minuses cancel out, we get

$$(\frac{c - i(k_j - k_i)}{c + i(k_j - k_i)})(\frac{c - i(k_l - k_f)}{c + i(k_l - k_f)}).$$

We calculate ba in a similar way

$$(\frac{c - i(k_l - k_f)}{c + i(k_l - k_f)})(\frac{c - i(k_j - k_i)}{c + i(k_j - k_i)}).$$

Since multiplication of numbers is commutative:

$$(c - i(k_j - k_i))(c - i(k_l - k_f)) = (c - i(k_l - k_f))(c - i(k_j - k_i))$$

and

$$(c + i(k_j - k_i))(c - i(k_l - k_f)) = (c + i(k_l - k_f))(c - i(k_j - k_i))$$

then it follows that

$$ab = ba. \tag{8}$$

Thus, this equality is indeed satisfied.

To apply the Bethe ansatz to information technology, we will write the Bethe ansatz in explicit form. For simplicity, we will consider the case when s is equal to 3. The sum over permutations $P \in S_3$ means that we iterate over all 3!=6 permutations of the index set $1,2,3$. In the above decomposition, each of the six terms corresponds to one of these permutations. For example, we can relate the permutations and the terms of the sum as follows: 1.Permutation

$$P = (1,2,3) : e^{i(k_1x_1 + k_2x_2 + k_3x_3)}$$

2.Permutation

$$P = (1,3,2) : a(k_2,k_3)e^{i(k_1x_1 + k_3x_2 + k_2x_3)},$$

where

$$a(k_2,k_3) = S(k_2,k_3)$$

3.Permutation

$$P = (2,1,3) : a(k_1,k_2)e^{i(k_2x_1 + k_1x_2 + k_3x_3)},$$

where

$$a(k_1,k_2) = S(k_1,k_2)$$

4.Permutation

$$P = (2,3,1) : a(k_1,k_2;k_1k_3)e^{i(k_2x_1 + k_3x_2 + k_1x_3)},$$

where

$$a(k_1,k_2;k_1k_3) = S(k_1,k_3)S(k_2,k_3)$$

5.Permutation

$$P = (3,1,2) : a(k_1,k_3)e^{i(k_3x_1 + k_1x_2 + k_2x_3)},$$

where

$$a(k_1,k_3) = S(k_1,k_2)S(k_1,k_3)$$

6.Permutation

$$P = (3,2,1) : a(k_1,k_3;k_2k_3)e^{i(k_3x_1 + k_2x_2 + k_1x_3)},$$

where

$$a(k_1,k_3;k_2k_3) = S(k_1,k_2)S(k_1,k_3)S(k_2,k_3)$$

Thus, the explicit expansion of the wave function for three particles is written as the sum of these six terms:

$$\psi(x_1,x_2,x_3) = e^{i(k_1x_1 + k_2x_2 + k_3x_3)} +$$

$$a(k_2,k_3)e^{i(k_1x_1 + k_3x_2 + k_2x_3)} + a(k_1,k_2)e^{i(k_2x_1 + k_1x_2 + k_3x_3)} +$$

$$a(k_1,k_2;k_1k_3)e^{i(k_2x_1 + k_3x_2 + k_1x_3)} +$$

$$a(k_1,k_3)e^{i(k_3x_1 + k_2x_2 + k_1x_3)} +$$

$$a(k_1,k_3;k_2k_3)e^{i(k_3x_1 + k_2x_2 + k_1x_3)}. \tag{9}$$

3 Application of Bethe ansatz in information technology

Let's consider how the last equation can be used for three-stage information transfer. To do this, we will use the formulas (5)-(9).

Let Alice encrypt information

$$M = \psi(x_1,x_2,x_3) = e^{i(k_1x_1+k_2x_2+k_3x_3)}+$$
$$a(k_2,k_3)e^{i(k_1x_1+k_3x_2+k_2x_3)}+$$
$$+...+a(k_1,k_3;k_2k_3)e^{i(k_3x_1+k_2x_2+k_1x_3)} \quad (10)$$

using the encryption key

$$E_1 = -e^{i\theta_{2,1}}e^{i\theta_{3,2}}e^{i\theta_{1,3}}$$

and send encrypted information to Bob:

$$(E_1M) = -e^{i\theta_{2,1}}e^{i\theta_{3,2}}e^{i\theta_{1,3}}(e^{i(k_1x_1+k_2x_2+k_3x_3)}+$$
$$a(k_2,k_3)e^{i(k_1x_1+k_3x_2+k_2x_3)}+...+$$
$$+a(k_1,k_3;k_2k_3)e^{i(k_3x_1+k_2x_2+k_1x_3)}) =$$
$$= e^{i(k_2x_1+k_3x_2+k_1x_3)}+$$
$$a(k_2,k_3)e^{i(k_3x_1+k_2x_2+k_1x_3)}+...+$$
$$a(k_1,k_3;k_2k_3)e^{i(k_2x_1+k_1x_2+k_3x_3)}$$

Bob receives this information and encrypts it with his key:

$$E_2 = -e^{i\theta_{3,1}}e^{i\theta_{1,2}}e^{i\theta_{2,3}} \quad (11)$$

and sends the double-encrypted information back to Alice:

$$(E_2(E_1M)) = -e^{i\theta_{3,1}}e^{i\theta_{1,2}}e^{i\theta_{2,3}}(e^{i(k_2n_1+k_3n_2+k_1n_3)}+$$
$$a(k_2,k_3)e^{i(k_3x_1+k_2x_2+k_1x_3)}+...+$$
$$a(k_1,k_3;k_2k_3)e^{i(k_2x_1+k_1x_2+k_3x_3)})$$
$$= e^{i(k_1x_1+k_2x_2+k_3x_3)}+$$
$$a(k_2,k_3)e^{i(k_1x_1+k_3x_2+k_2x_3)}+...+$$
$$a(k_1,k_3;k_2k_3)e^{i(k_3x_1+k_2x_2+k_1x_3)}$$

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

$$D_1 = -e^{i\theta_{2,1}}e^{i\theta_{3,2}}e^{i\theta_{1,3}}:$$
$$(D_1(E_2(E_1M))) = -e^{i\theta_{2,1}}e^{i\theta_{3,2}}e^{i\theta_{1,3}}(e^{i(k_1x_1+k_2x_2+k_3x_3)}+$$
$$a(k_2,k_3)e^{i(k_1x_1+k_3x_2+k_2x_3)}+...+$$
$$a(k_1,k_3;k_2,k_3)e^{i(k_3x_1+k_2x_2+k_1x_3)}) =$$
$$e^{i(k_3x_1+k_1x_2+k_2x_3)}+$$
$$a(k_2,k_3)e^{i(k_2x_1+k_1x_2+k_3x_3)}+...+$$
$$a(k_1,k_3;k_2k_3)e^{i(k_1x_1+k_3x_2+k_2x_3)}$$

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

$$D_2 = -e^{i\theta_{2,1}}e^{i\theta_{3,2}}e^{i\theta_{1,3}} \quad (12)$$
$$(D_2(D_1(E_2(E_1M)))) = -e^{i\theta_{2,1}}e^{i\theta_{3,2}}e^{i\theta_{1,3}}(e^{i(k_3x_1+k_1x_2+k_2x_3)}+$$
$$a(k_2,k_3)e^{i(k_2x_1+k_1x_2+k_3x_3)}+...+$$
$$a(k_1,k_3;k_2k_3)e^{i(k_1x_1+k_3x_2+k_2x_3)}) =$$
$$= e^{i(k_1x_1+k_2x_2+k_3x_3)}+$$
$$a(k_2,k_3)e^{i(k_1x_1+k_3x_2+k_2x_3)}+...+$$
$$a(k_1,k_3;k_2k_3)e^{i(k_3x_1+k_2x_2+k_1x_3)}$$

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

Now we will check formula

$$(D_2(D_1(E_2(E_1M)))) = (D_2(D_1(E_1(E_2M)))) =$$
$$(D_2(E_2M)) = M, \quad (13)$$

where E_1,E_2 the encryption keys of Alice and Bob,respectively, and D_1,D_2 the decryption keys of Alice and Bob, respectively. The encryption keys have the property

$$E_2E_1 = E_1E_2.$$

that is, the matrices of keys E_1,E_2 should be commutative. We will use also formulas (10), (11),(12):

$$(E_2M) = -e^{i\theta_{3,1}}e^{i\theta_{1,2}}e^{i\theta_{2,3}}(e^{i(k_1x_1+k_2x_2+k_3x_3)}+$$
$$a(k_2,k_3)e^{i(k_1x_1+k_3x_2+k_2x_3)}+$$
$$+...+a(k_1,k_3;k_2k_3)e^{i(k_3x_1+k_2x_2+k_1x_3)}) =$$
$$e^{i(k_3x_1+k_1x_2+k_2x_3)}+a(k_2,k_3)e^{i(k_2x_1+k_3x_2+k_1x_3)}+...+$$
$$a(k_1,k_3;k_2k_3)e^{i(k_1x_1+k_3x_2+k_2x_3)}.$$

Then

$$(D_2(E_2M)) = -e^{i\theta_{2,1}}e^{i\theta_{3,2}}e^{i\theta_{1,3}}(e^{i(k_3x_1+k_1x_2+k_2x_3)}+$$
$$a(k_2,k_3)e^{i(k_2x_1+k_1x_2+k_3x_3)}+...+$$
$$a(k_1,k_3;k_2k_3)e^{i(k_3x_1+k_1x_2+k_2x_3)}) =$$
$$e^{i(k_1x_1+k_2x_2+k_3x_3)}+$$
$$a(k_2,k_3)e^{i(k_1x_1+k_3x_2+k_2x_3)}+...$$
$$a(k_1,k_3;k_2k_3)e^{i(k_3x_1+k_2x_2+k_1x_3)}.$$

From this it is clear that (13) holds.

If we use the explicit form $a(k_2,k_3),a(k_1,k_2),a(k_1,k_2;k_1k_3),a(k_1,k_3),a(k_1,k_3;k_2k_3)$ we get

$$(E_2M) = e^{i(k_3x_1+k_1x_2+k_2x_3)} - e^{i\theta(k_2,k_3)}e^{i(k_2x_1+k_3x_2+k_1x_3)}+...-$$

$$e^{i\theta(k_1,k_2)}e^{i\theta(k_1,k_3)}e^{i\theta(k_2,k_3)}e^{i(k_3x_1+k_2x_2+k_1x_3)} =$$
$$e^{i(k_3x_1+k_1x_2+k_2x_3)}+e^{i(k_3x_1k_2x_2+k_1x_3)}+...+$$
$$e^{i(k_1x_1+k_2x_2+k_3x_3)}$$

and

$$(D_2(E_2M)) = e^{i(k_1x_1+k_2x_2+k_3x_3)}+$$
$$a(k_2,k_3)e^{i(k_1x_1+k_3x_2+k_2x_3)}+...$$
$$a(k_1,k_3;k_2k_3)e^{i(k_3x_1+k_2x_2+k_1x_3)} =$$
$$e^{i(k_1x_1+k_2x_2+k_3x_3)}-$$
$$e^{i\theta(k_2,k_3)}e^{i(k_1x_1+k_3x_2+k_2x_3)}+...-$$
$$e^{i\theta(k_1,k_2)}e^{i\theta(k_2,k_3)}e^{i\theta(k_1,k_3)}e^{i(k_3x_1+k_2x_2+k_1x_3)} =$$
$$e^{i(k_1x_1+k_2x_2+k_3x_3)}+e^{i(k_1x_1+k_2x_2+k_3x_3)}+...+$$
$$e^{i(k_1x_1+k_2x_2+k_3x_3)}.$$

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:

$$e^{i(k_2x_1+k_1x_2)} = \sum_{n=0}^{\infty}\frac{1}{n!}(k_2x_1+k_1x_2)^n =$$

$$\sum_{n=0}^{\infty}\frac{1}{n!}(\begin{bmatrix}x_1 & x_2\end{bmatrix}\begin{bmatrix}k_2\\k_1\end{bmatrix})^n = \sum_{n=0}^{\infty}\frac{i^n}{n!}(\begin{bmatrix}x_1 & x_2\end{bmatrix}P\begin{bmatrix}k_1\\k_2\end{bmatrix})^n.$$

where

$$\begin{bmatrix}k_2\\k_1\end{bmatrix} = P\begin{bmatrix}k_1\\k_2\end{bmatrix},$$

and

$$P = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}.$$

$$E_1 = \begin{array}{|c|c|c|}\hline 0&1&0\\\hline 0&0&1\\\hline 1&0&0\\\hline\end{array} \quad E_2 = \begin{array}{|c|c|c|}\hline 0&0&1\\\hline 1&0&0\\\hline 0&1&0\\\hline\end{array}$$

$$D_1 = \begin{array}{|c|c|c|}\hline 0&0&1\\\hline 1&0&0\\\hline 0&1&0\\\hline\end{array} \quad D_2 = \begin{array}{|c|c|c|}\hline 0&1&0\\\hline 0&0&1\\\hline 1&0&0\\\hline\end{array}.$$

Matrices E_1 and E_2 are commutative:

$$E_1\times E_2 = \begin{array}{|c|c|c|}\hline 0&1&0\\\hline 0&0&1\\\hline 1&0&0\\\hline\end{array}\times\begin{array}{|c|c|c|}\hline 0&0&1\\\hline 1&0&0\\\hline 0&1&0\\\hline\end{array} =$$

$$E_2\times E_1 = \begin{array}{|c|c|c|}\hline 0&0&1\\\hline 1&0&0\\\hline 0&1&0\\\hline\end{array}\times\begin{array}{|c|c|c|}\hline 0&1&0\\\hline 0&0&1\\\hline 1&0&0\\\hline\end{array} =$$

$$\begin{array}{|c|c|c|}\hline 1&0&0\\\hline 0&1&0\\\hline 0&0&1\\\hline\end{array}.$$

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

$$D_1\times E_1 = \begin{array}{|c|c|c|}\hline 0&0&1\\\hline 1&0&0\\\hline 0&1&0\\\hline\end{array}\times\begin{array}{|c|c|c|}\hline 0&1&0\\\hline 0&0&1\\\hline 1&0&0\\\hline\end{array} =$$

$$\begin{array}{|c|c|c|}\hline 1&0&0\\\hline 0&1&0\\\hline 0&0&1\\\hline\end{array}.$$

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

$$D_2\times E_2 = \begin{array}{|c|c|c|}\hline 0&1&0\\\hline 0&0&1\\\hline 1&0&0\\\hline\end{array}\times\begin{array}{|c|c|c|}\hline 0&0&1\\\hline 1&0&0\\\hline 0&1&0\\\hline\end{array} =$$

$$\begin{array}{|c|c|c|}\hline 1&0&0\\\hline 0&1&0\\\hline 0&0&1\\\hline\end{array}.$$

Let the initial information have the form:

$$\text{M}=\begin{array}{|c|}\hline k_1\\\hline k_2\\\hline k_3\\\hline\end{array}+$$

$$a(k_2,k_3)\times\begin{array}{|c|}\hline k_1\\\hline k_3\\\hline k_2\\\hline\end{array}+...+a(k_1,k_3;k_2,k_3)\times\begin{array}{|c|}\hline k_3\\\hline k_2\\\hline k_1\\\hline\end{array}.$$

Then

$$E_1M = (\begin{array}{|c|c|c|}\hline 0&1&0\\\hline 0&0&1\\\hline 1&0&0\\\hline\end{array}\times\begin{array}{|c|}\hline k_1\\\hline k_2\\\hline k_3\\\hline\end{array} = \begin{array}{|c|}\hline k_2\\\hline k_3\\\hline k_1\\\hline\end{array})+$$

$$(a(k_2,k_3)\begin{array}{|c|c|c|}\hline 0&1&0\\\hline 0&0&1\\\hline 1&0&0\\\hline\end{array}\times\begin{array}{|c|}\hline k_1\\\hline k_3\\\hline k_2\\\hline\end{array} =$$

$$a(k_2,k_3)\begin{array}{|c|}\hline k_3\\\hline k_2\\\hline k_1\\\hline\end{array})+...+$$

$$((a(k_1,k_3;k_2,k_3)\begin{array}{|c|c|c|}\hline 0&1&0\\\hline 0&0&1\\\hline 1&0&0\\\hline\end{array}\times\begin{array}{|c|}\hline k_3\\\hline k_2\\\hline k_1\\\hline\end{array} =$$

$a(k_1,k_3;k_2,k_3)\begin{pmatrix}k_2\\k_1\\k_3\end{pmatrix}$.

$E_2E_1M = \left(\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}\times\begin{pmatrix}k_2\\k_3\\k_1\end{pmatrix}=\begin{pmatrix}k_1\\k_2\\k_3\end{pmatrix}\right)+$

$(a(k_2,k_3)\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}\times\begin{pmatrix}k_3\\k_2\\k_1\end{pmatrix}=$

$a(k_2,k_3)\begin{pmatrix}k_1\\k_3\\k_2\end{pmatrix}+\ldots+$

$(a(k_1,k_3;k_2,k_3)\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}\times\begin{pmatrix}k_2\\k_1\\k_3\end{pmatrix}=$

$a(k_1,k_3;k_2,k_3)\begin{pmatrix}k_3\\k_2\\k_1\end{pmatrix}$.

$D_1E_2E_1M = \left(\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}\times\begin{pmatrix}k_1\\k_2\\k_3\end{pmatrix}=\begin{pmatrix}k_3\\k_1\\k_2\end{pmatrix}\right)+$

$(a(k_2,k_3)\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}\times\begin{pmatrix}k_1\\k_3\\k_2\end{pmatrix}=$

$a(k_2,k_3)\begin{pmatrix}k_2\\k_1\\k_3\end{pmatrix}+\ldots+$

$(a(k_1,k_3;k_2,k_3)\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}\times\begin{pmatrix}k_3\\k_2\\k_1\end{pmatrix}=$

$a(k_1,k_3;k_2,k_3)\begin{pmatrix}k_1\\k_3\\k_2\end{pmatrix}$.

$D_2D_1E_2E_1M = \left(\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}\times\begin{pmatrix}k_3\\k_1\\k_2\end{pmatrix}=\begin{pmatrix}k_1\\k_2\\k_3\end{pmatrix}\right)+$

$((a(k_2,k_3)\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}\times\begin{pmatrix}k_2\\k_1\\k_3\end{pmatrix}=$

$a(k_2,k_3)\begin{pmatrix}k_1\\k_3\\k_2\end{pmatrix}+\ldots+$

$(a(k_1,k_3;k_2,k_3)\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}\times\begin{pmatrix}k_1\\k_3\\k_2\end{pmatrix}=$

$a(k_1,k_3;k_2,k_3)\begin{pmatrix}k_3\\k_2\\k_1\end{pmatrix}=M$.

Here $a(k_2,k_3)=\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}$

and

$a(k_1,k_3;k_2,k_3)=\begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix}\times\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}\times$

$\begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix}=\begin{pmatrix}0&0&1\\0&1&0\\1&0&0\end{pmatrix}$.

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:

$$p_C(M) = \frac{p(M)\times p_M(C)}{p(C)}, \tag{14}$$

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 [13], [14] 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 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 $s = 3$ letters $k_i \in M$ with equal probabilities $p(k_i) = \frac{1}{3}$. Suppose we have plaintext cell k_i, $(1 \leq i \leq 3)$ and suppose these plaintext cells appear in the text with frequencies $p(k_i) = \frac{1}{3}$ and consequently, $p(M) = \sum_{1 \leq i \leq 3} p_i = 1$.

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 $p_K(k_{i,j}) = \frac{1}{3}$ consequently $p_M(C) = \sum_{1 \leq i \leq 3} K(k_{i,j}) = 1$.

If we have the probabilities $p(k_i)$ and of keys $p_K(k_{i,j}) = \frac{1}{3}$ we provide to find the probability of ciphertext $p(k_j)$ using the formula

$$p(k_j) = \sum_{1 \leq i \leq 3} p(k_i) p_K(k_{i,j}).$$

When all keys are independent, each key has an equal probability of $1/3$, so we can replace $p_K(k_{i,j}) = \frac{1}{3}$. Accordingly, we can obtain

$$p(k_j) = \frac{1}{3} \sum_{1 \leq i \leq 3} p(k_i). \tag{15}$$

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 (15), so we have $\frac{1}{3} \sum_{1 \leq i \leq 3} p(k_i)$ for probability of cell of ciperhtext.

But the sum of the probabilities of all possible plaintext cells k_i is 1, so we obtain $p(k_j) = \frac{1}{3}$ and $p(C) = \sum_{1 \leq j \leq 3} p(k_j) = 1$. Hence, every ciphertext occurs with an equal probability and

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

Therefore, from Shannon equality (14) when $p(M) = p(C) = 1$, we get

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

This proves that our system has perfect secrecy.

5 Conclusion

In this paper, the concept of using the full set of Bethe states of the Lieb-Liniger ansatz model as a source of cryptographic constructions was presented. The approach is based on the method of M.Yu.Rasulova allowed interpreting the spectral data of a quantum system as a discrete space suitable for encoding information and generating keys. The analysis showed that the inverse problem of restoring the system parameters from the Bethe roots is nontrivial and potentially computationally difficult, especially with an increase in the number of particles and the complexity of the boundary conditions. This opens up prospects for constructing quantum-resistant protocols in which fundamental symmetry and integrability are used as a means of creating structural cryptographic protection. Further research will be aimed at numerical modeling of the resistance of such schemes and formal justification of their cryptographic properties from the point of view of the theory of computational complexity.

References

[1] 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).

[2] H.A.Bethe, On the theory of metals, I. Eigenvalues and eigenfunctions of a linear chain of atoms,(German), *Zeits. Phys.*, 205-226 (1931).

[3] 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, Singapore, 165-170, (2017).

[4] 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).

[5] 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).

[6] 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).

[7] M. Yu. Rasulova, Approach to Cryptography from the Lieb-Liniger Model, App.Math.Inf.Sciences, **7** (3), 431-436 (2023).

[8] M. Yu. Rasulova, Creation of a crypto system that satisfies Shannon's perfect secrecy condition based on the Lieb-Liniger Model, App.Math.Inf.Sciences, **7** (4), 631-637 (2023).

[9] L.D.Landau, E.M.Lifshitz, *Quantum Mechanics*, Non-Relativistic Theory, 3rd Edition, Elsevier (2013).

[10] 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).

[11] C.E.Shannon, A mathematical theory of communication, *Bell System Technical Journal*, **27**(3), 379-423 (1948).

[12] C.E.Shannon, A mathematical theory of communication, *Bell System Technical Journal*, **27**(4), 623-656 (1948).

[13] D.Stinson, *Cryptography:Theory and Practice. Second edition*, Chapman and Hall/CRC Press (2002).

[14] 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.