Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/180508

Creation of a cryptosystem for time-dependent information that satisfies Shannon's perfect secrecy condition

Mukhayo Yunusovna Rasulova

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

Received: 2 Jun. 2024, Revised: 2 Jul. 2024, Accepted: 12 Jul. 2024
Published online: 1 Sep. 2024

Abstract: The research paper proposes applying the Lieb-Liniger statistical mechanics model and the chain of quantum kinetic equations Bogolyubov-Born-Green-Kirkwood-Yvon, to create a cryptosystem that satisfies the Shannon perfect secrecy condition for time dependent information

Keywords: statistical physics, BBGKY chain of quantum kinetic equation, Lieb-Liniger Model, Shannon perfect secresy condition, tree-pass protocol

1 Introduction

One of the most important tasks of our time is the creation of a cryptosystem allowing secure transmission of time-dependent information. Another important problem, is the most urgent problem 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.

In this paper, to create a cryptosystem that allows the secure transmission of time-dependent information, in Chapter 2, information is introduced on the chain of quantum kinetic equations of Bogolyubov-Born-Green-Kirkwood-Yvon (BBGKI) [5] [6] and its decision. The third chapter introduces information about the Lieb-Liniger model for systems of Bose particles interacting with the help of a potential in the form of a delta function. Also in this chapter, the solution of the BBGKY chain for particles interacting through the potential in the form of a delta function is considered. The formula for permutation of variables is defined. In the fourth chapter, using the Lieb-Liniger model and using the eight cell information, information transfer based on the three-pass protocol [7] is shown (see figure below) and this method of information transfer is translated into matrix language.To solve the Shannon problem, in the fifth 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

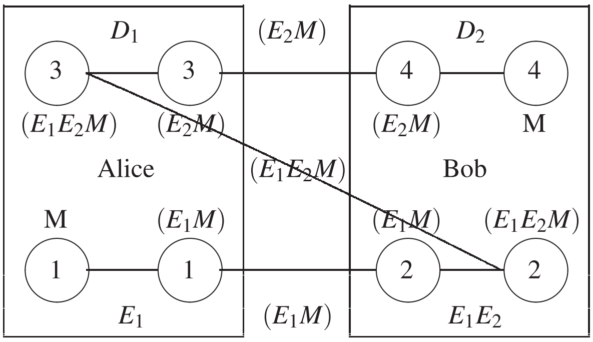

Figure of transfer based on the three-pass protocol between of Alice and Bob.

2 A chain of quantum kinetic equations BBGKY and its solution

Let us consider the BBGKY hierarchy of quantum kinetic equations in the restricted three-dimensional domain Λ [5] [6]:

$$i\frac{\partial\rho_s^\Lambda(t,x_1,\ldots,x_s;x_1',\ldots,x_s')}{\partial t}=[H_s^\Lambda,\rho_s^\Lambda](t,x_1,\ldots,x_s;x_1',\ldots,x_s')$$

$$+\frac{N}{V}\left(1-\frac{s}{N}\right)Tr_{x_{s+1}}\sum_{1\le i\le s}(\phi_{i,s+1}(|x_i-x_{s+1}|)-$$

$$\phi_{i,s+1}(|x_i'-x_{s+1}|))\rho_{s+1}^\Lambda(t,x_1,\ldots,x_s,x_{s+1};x_1',\ldots,x_s',x_{s+1}), \tag{1}$$

with the initial

$$\rho_s^\Lambda(t,x_1,\ldots,x_s;x_1',\ldots,x_s')|_{t=0}=\rho_s^\Lambda(0,x_1,\ldots,x_s;x_1',\ldots,x_s').$$

In Eq. (1),$\rho_s(t,x_1,\ldots,x_s;x_1',\ldots,x_s')$ is the density matrix, x is a three-dimensional coordinate of a particle, t is the time, m is the particle mass, $\hbar$ is the Planck constant, H is the Hamiltonian of a system of particles, N is the number of particles in the domain under consideration, $\phi_{i,j}$ is the interaction potential between the particles.

The Hamiltonian has the form

$$H_s^\Lambda(x_1,\ldots,x_s)=\sum_{1\le i\le s}\left(-\frac{1}{2m}\triangle_{x_i}+u^\Lambda(x_i)\right)+$$

$$\sum_{1\le i<j\le s}\phi_{i,j}(|x_i-x_j|),$$

where $\triangle_{x_i}$ is the Laplace operator.The operators ρ_N^L and Hamiltonian H_N^L assumed to act in the space H with zero boundary condition.

To find the solution of hierarchy (1), we introduce [9],[10], the space of nuclear operators B^Λ, which is the Banach space of sequences of positive definite self-adjoint nuclear operators $\rho_s^\Lambda(x_1,\ldots,x_s;x_1',\ldots,x_s')$:

$$\rho^\Lambda=\{\rho_0^\Lambda,\rho_1^\Lambda(x_1;x_1'),\ldots,\rho_s^\Lambda(x_1,\ldots,x_s;x_1',\ldots,x_s'),\ldots\},$$

where ρ_0^Λ is the complex number, $\rho_s^\Lambda\subset B_s^\Lambda$,

$$\rho_s^\Lambda(x_1,\ldots,x_s;x_1',\ldots,x_s')=0,\qquad where\qquad s>s_0,$$

s_0 is a finite value and the norm is determined as

$$|\rho^\Lambda|_1=\sum_{s=0}^{\infty}|\rho_s^\Lambda|_1.$$

and

$$|\rho_s^\Lambda|_1=sup\sum_{1\le i\le\infty}|(\rho_s^\Lambda\psi_i^s,\varphi_i^s)|,$$

The upper bound is taken over all orthonormal systems of finite, twice differentiable functions with compact support $\{\psi_i^s\}$ and $\{\varphi_i^s\}$ in $L_2^s(\Lambda)$, $s\ge 1$ and $\left|\rho_0^\Lambda\right|_1=\left|\rho_0^\Lambda\right|$.

Introducing the operator

$$\left(\Omega(\Lambda)\rho^\Lambda\right)_s(x_1,..,x_s;x_1',..,x_s')=\frac{N}{V}\left(1-\frac{s}{N}\right)\times$$

$$\int_\Lambda\sum_i\rho_{s+1}^\Lambda(x_1,..,x_s,x_{s+1};x_1',..,x_s',x_{s+1})\times$$

$$g_i^1(x_{s+1})\tilde{g}_i^1(x_{s+1})dx_{s+1},$$

and using the semigroup method we can determine the unique solution to a chain BBGKY of quantum kinetic equations for a potential, satisfying the Kato condition in the form:

$$\rho_s^\Lambda(t,x_1,\ldots,x_s;x_1',\ldots,x_s')=U^\Lambda(t)\rho_s^\Lambda(x_1,..,x_s;x_1',..,x_s')=$$

$$=(e^{\Omega(\Lambda)}e^{-iH^\Lambda t}e^{-\Omega(\Lambda)}\rho^\Lambda e^{iH^\Lambda t})_s(x_1,..,x_s;x_1',..,x_s'), \tag{2}$$

where

$$\rho_s^\Lambda(x_1,\ldots,x_s;x_1',\ldots,x_s')=\sum_{i=1}\psi_i(x_1,\ldots,x_s)\psi_i^*(x_1',\ldots,x_s').$$

3 Bethe Ansatz for Bose gas

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

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

in one-dimensional space:

$$(-\sum_1^s\frac{1}{2m}\triangle_{x_i}+2c\sum_{1\le i<j\le s}\delta(|x_i-x_j|))\psi=E\psi, \tag{3}$$

where $2c \geq 0$ is the amplitude of the delta function, the problem domain is defined as R : all $0 \leq x_i \leq L$ and the wave function ψ satisfies the condition of periodicity in all variables. It was proved in [4] that the definition of a solution ψ in R is equivalent to the definition of a solution to the equation

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

with boundary condition

$$\left(\frac{\partial \psi}{\partial x_j} - \frac{\partial \psi}{\partial x_k}\right)|_{x_j = x_{k+0}} - \left(\frac{\partial \psi}{\partial x_j} - \frac{\partial \psi}{\partial x_k}\right)|_{x_j = x_{k-0}} = 2c\psi|_{x_j = x_k}, \tag{4}$$

for ψ in the region $R_1 : 0 \leq x_1 \leq x_2 \leq .... \leq x_s \leq L$, then knowledge of ψ in R_1 is equivalent to knowledge of ψ in R and the initial periodicity condition is equivalent to the periodicity conditions in R_1

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

$$\psi|_{x_j = x_{k+0}} = \psi|_{x_j = x_{k-0}}.$$

Using equations (5) we can determine the solution of equation (4) in the form of the Bethe ansatz [4], [11]:

$$\psi(x_1, ...x_s) = \sum_P a(P) P exp(i \sum_{j=1}^{s} x_j k_j) \tag{5}$$

in the region $R_1 : 0 \leq x_1 \leq x_2 \leq .... \leq x_s \leq L$ with eigenvalue $E_s = \sum_{i=1}^{s} k_i^2$, where the summation is over all permutations P of the numbers k and $a(P)$ is a certain coefficient depending on P:

$$a(P) = -\frac{c - i(k_\alpha - k_\beta)}{c + i(k_\alpha - k_\beta)} = -exp(i\theta_{\alpha,\beta}),$$

where

$$\theta_{i,j} = \theta(k_i - k_j),$$

$$\theta(r) = -2tan^{-1}(r/c)$$

and when r is real

$$\pi \geq \theta(r) \geq -\pi.$$

For a Hamiltonian with a potential in the form of a delta function

$$-\sum_{1 \leq i \leq s} \frac{1}{2m} \triangle_{x_i} + 2c \sum_{1 \leq i < j \leq s} \delta(|x_i - x_j|)$$

the chain of BBKGI quantum kinetic equations for a one-dimensional domain has the form:

$$i\frac{\partial \rho_s^L(t, x_1, ..., x_s; x_1', ..., x_s')}{\partial t} = [H_s^L, \rho_s^L](t, x_1, ..., x_s; x_1', ..., x_s')$$

$$+2c\frac{N}{|L|}\left(1 - \frac{s}{N}\right) Tr_{x_{s+1}} \sum_{1 \leq i \leq s} (\delta_{i,s+1}(|x_i - x_{s+1}|) -$$

$$\delta_{i,s+1}(|x_i' - x_{s+1}|))\rho_s^L(t, x_1, ..., x_s, x_{s+1}; x_1', ..., x_s', x_{s+1}) \tag{6}$$

for $1 \leq s < N$ and for $s = N$, has the form

$$i\frac{\partial \rho_s^L(t, x_1, ..., x_s; x_1', ..., x_s')}{\partial t} = [H_s^L, \rho_s^L](t, x_1, ..., x_s; x_1', ..., x_s'). \tag{7}$$

Here we consider a system of bosons in a one-dimensional region L, where $\Lambda = L^3$ with volume $V = |\Lambda = L^3|$. It is assumed that the operators ρ_N^L and the Hamiltonian H_N^L act in space H with zero boundary condition [10].

According to formula (2), the solutions of equations (6) and (7) will be, respectively [12], [13], [14]:

$$\rho_s^L(t, x_1, ..., x_s; x_1', ..., x_s') = U^L(t)\rho_s^L(x_1, .., x_s; x_1', .., x_s') =$$

$$= (e^{\Omega(L)} e^{-iH^L t} e^{-\Omega(L)} \rho^L e^{iH^L t})_s(x_1, .., x_s; x_1', .., x_s') \tag{8}$$

and

$$\rho_s^L(t, x_1, ..., x_s; x_1', ..., x_s') = U^L(t)\rho_s^L(x_1, .., x_s; x_1', .., x_s') =$$

$$= (e^{-iTt} \rho^L e^{iTt})_s(x_1, .., x_s; x_1', .., x_s'), \tag{9}$$

where

$$\rho_s^L(x_1, ..., x_s; x_1', ..., x_s') = \sum_{i=1} \psi_i(x_1, ..., x_s) \psi_i^*(x_1', ..., x_s'),$$

$$\psi(x_1, ...x_s) = \sum_P a(P) P exp(i \sum_{j=1}^{s} x_j k_j),$$

$\psi(x_1, ...x_s)$ and $\psi(x_1', ...x_s')$ - Bethe ansatzs in the region $R_1 : 0 \leq x_1 \leq x_2 \leq .... \leq x_s \leq L$ and $R_1 : 0 \leq x_1' \leq x_2' \leq .... \leq x_s' \leq L$ respectively, with eigenvalue $E_s = \sum_{i=1}^{s} k_i^2$.

Since the evolution operator $U(T)$ is a unitary operator in the space B_1, then on this space

$$|U(t)\rho_s^\Lambda|_1 = |\rho_s^\Lambda|_1.$$

For the case $s = 2$, from equations (8),(9) with $t = 0$, one can obtain [13], [15], [16]:

$$a_{1,2}(k_1, k_2) e^{i(k_1 x_1 + k_2 x_2)} + a_{2,1}(k_1, k_2) e^{i(k_2 x_1 + k_1 x_2).}$$

and

$$ik_2 a_{1,2} + ik_1 a_{2,1} - ik_1 a_{1,2} - ik_2 a_{2,1} = c(a_{1,2} + a_{2,1}),$$

or

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

If we choose

$$a_{1,2} = e^{i(k_1 y_1 + k_2 y_2)}$$

we get

$$e^{i(k_2 y_1 + k_1 y_2)} = -\frac{c - i(k_2 - k_1)}{c - i(k_2 - k_1)} e^{i(k_1 y_1 + k_2 y_2)} =$$

$$-e^{i\theta_{2,1}} e^{i(k_1 y_1 + k_2 y_2)}. \tag{10}$$

4 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:

$$(E_1,X) = e^{i\theta_{2,1}} e^{i\theta_{1,2}} e^{i\theta_{8,3}} e^{i\theta_{5,4}} e^{i\theta_{4,5}} e^{i\theta_{7,6}} e^{i\theta_{6,7}} e^{i\theta_{3,8}} \times$$
$$e^{i(k_1x_1+k_2x_2+k_3x_3+k_4x_4+k_5x_5+k_6x_6+k_7x_7+k_8x_8)} =$$
$$e^{i(k_2x_1+k_1x_2+k_8x_3+k_5x_4+k_4x_5+k_7x_6+k_6x_7+k_3x_8)}.$$

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:

$$(E_2(E_1,X)) = e^{i\theta_{5,1}} e^{i\theta_{4,2}} e^{i\theta_{2,3}} e^{i\theta_{3,4}} e^{i\theta_{8,5}} e^{i\theta_{7,6}} e^{i\theta_{6,7}} e^{i\theta_{1,8}} \times$$
$$e^{i(k_2x_1+k_1x_2+k_8x_3+k_5x_4+k_4x_5+k_7x_6+k_6x_7+k_3x_8)} =$$
$$e^{i(k_4x_1+k_5x_2+k_1x_3+k_8x_4+k_3x_5+k_6x_6+k_7x_7+k_2x_8)}.$$

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

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

$$(D_1(E_2(E_1,X))) = e^{i\theta_{2,1}} e^{i\theta_{1,2}} e^{i\theta_{8,3}} e^{i\theta_{5,4}} e^{i\theta_{4,5}} e^{i\theta_{7,6}} e^{i\theta_{6,7}} \times$$
$$e^{i\theta_{3,8}} e^{i(k_4x_1+k_5x_2+k_1x_3+k_8x_4+k_3x_5+k_6x_6+k_7x_7+k_2x_8)} =$$
$$= e^{i(k_5x_1+k_4x_2+k_2x_3+k_3x_4+k_8x_5+k_7x_6+k_6x_7+k_1x_8)}$$

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

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

$$(D_2(D_1(E_2(E_1,X)))) = e^{i\theta_{8,1}} e^{i\theta_{3,2}} e^{i\theta_{4,3}} e^{i\theta_{2,4}} e^{i\theta_{1,5}} e^{i\theta_{7,6}} \times$$
$$e^{i\theta_{6,7}} e^{i\theta_{5,8}} e^{i(k_5x_1+k_4x_2+k_2x_3+k_3x_4+k_8x_5+k_7x_6+k_6x_7+k_1x_8)} =$$
$$e^{i(k_1x_1+k_2x_2+k_3x_3+k_4x_4+k_5x_5+k_6x_6+k_7x_7+k_8x_8)}.$$

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:

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

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

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

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

where

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

Then Alice's encryption key E_1¿:

$$E_1 = \begin{array}{|c|}\hline 01000000 \\ \hline 10000000 \\ \hline 00000001 \\ \hline 00001000 \\ \hline 00010000 \\ \hline 00000010 \\ \hline 00000100 \\ \hline 00100000 \\ \hline \end{array}, \quad E_2 = \begin{array}{|c|}\hline 00001000 \\ \hline 00010000 \\ \hline 01000000 \\ \hline 00100000 \\ \hline 00000001 \\ \hline 00000010 \\ \hline 00000100 \\ \hline 10000000 \\ \hline \end{array},$$

$$D_1 = \begin{array}{|c|}\hline 01000000 \\ \hline 10000000 \\ \hline 00000001 \\ \hline 00001000 \\ \hline 00010000 \\ \hline 00000010 \\ \hline 00000100 \\ \hline 00100000 \\ \hline \end{array}, \quad D_2 = \begin{array}{|c|}\hline 00000001 \\ \hline 00100000 \\ \hline 00010000 \\ \hline 01000000 \\ \hline 10000000 \\ \hline 00000010 \\ \hline 00000100 \\ \hline 00001000 \\ \hline \end{array}.$$

Matrices E_1 and E_2 are commutative:

$$E_1 \times E_2 = \begin{array}{|c|}\hline 01000000 \\ \hline 10000000 \\ \hline 00000001 \\ \hline 00001000 \\ \hline 00010000 \\ \hline 00000010 \\ \hline 00000100 \\ \hline 00100000 \\ \hline \end{array} \times \begin{array}{|c|}\hline 00001000 \\ \hline 00010000 \\ \hline 01000000 \\ \hline 00100000 \\ \hline 00000001 \\ \hline 00000010 \\ \hline 00000100 \\ \hline 10000000 \\ \hline \end{array} =$$

$$E_2 \times E_1 = \begin{array}{|c|}\hline 00001000 \\ \hline 00010000 \\ \hline 01000000 \\ \hline 00100000 \\ \hline 00000001 \\ \hline 00000010 \\ \hline 00000100 \\ \hline 10000000 \\ \hline \end{array} \times \begin{array}{|c|}\hline 01000000 \\ \hline 10000000 \\ \hline 00000001 \\ \hline 00001000 \\ \hline 00010000 \\ \hline 00000010 \\ \hline 00000100 \\ \hline 00100000 \\ \hline \end{array} =$$

$$\begin{array}{|c|}\hline 00010000\\\hline 00001000\\\hline 10000000\\\hline 00000001\\\hline 00100000\\\hline 00000100\\\hline 00000010\\\hline 01000000\\\hline\end{array}.$$

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

$$E_1 \times E_1^{-1}= \begin{array}{|c|}\hline 01000000\\\hline 10000000\\\hline 00000001\\\hline 00001000\\\hline 00010000\\\hline 00000010\\\hline 00000100\\\hline 00100000\\\hline\end{array} \times \begin{array}{|c|}\hline 01000000\\\hline 10000000\\\hline 00000001\\\hline 00001000\\\hline 00010000\\\hline 00000010\\\hline 00000100\\\hline 00100000\\\hline\end{array} =$$

$$\begin{array}{|c|}\hline 10000000\\\hline 01000000\\\hline 00100000\\\hline 00010000\\\hline 00001000\\\hline 00000100\\\hline 00000010\\\hline 00000001\\\hline\end{array}.$$

Similarly:

$D_2 = E_2^{-1}$ and

$$E_2 \times E_2^{-1}= \begin{array}{|c|}\hline 00001000\\\hline 00010000\\\hline 01000000\\\hline 00100000\\\hline 00000001\\\hline 00000010\\\hline 00000100\\\hline 10000000\\\hline\end{array} \times \begin{array}{|c|}\hline 00000001\\\hline 00100000\\\hline 00010000\\\hline 01000000\\\hline 10000000\\\hline 00000010\\\hline 00000100\\\hline 00001000\\\hline\end{array} =$$

$$\begin{array}{|c|}\hline 10000000\\\hline 01000000\\\hline 00100000\\\hline 00010000\\\hline 00001000\\\hline 00000100\\\hline 00000010\\\hline 00000001\\\hline\end{array}.$$

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

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

Then

$$E_1M= \begin{array}{|c|}\hline 01000000\\\hline 10000000\\\hline 00000001\\\hline 00001000\\\hline 00010000\\\hline 00000010\\\hline 00000100\\\hline 00100000\\\hline\end{array} \times \begin{array}{|c|}\hline 0\\\hline 1\\\hline 0\\\hline 1\\\hline 0\\\hline 0\\\hline 1\\\hline 1\\\hline\end{array} = \begin{array}{|c|}\hline 1\\\hline 0\\\hline 1\\\hline 0\\\hline 1\\\hline 1\\\hline 0\\\hline 0\\\hline\end{array}.$$

$$E_2E_1M= \begin{array}{|c|}\hline 00001000\\\hline 00010000\\\hline 01000000\\\hline 00100000\\\hline 00000001\\\hline 00000010\\\hline 00000100\\\hline 10000000\\\hline\end{array} \times \begin{array}{|c|}\hline 1\\\hline 0\\\hline 1\\\hline 0\\\hline 1\\\hline 1\\\hline 0\\\hline 0\\\hline\end{array} = \begin{array}{|c|}\hline 1\\\hline 0\\\hline 0\\\hline 1\\\hline 0\\\hline 0\\\hline 1\\\hline 1\\\hline\end{array}.$$

$$D_1E_1E_2M= \begin{array}{|c|}\hline 01000000\\\hline 10000000\\\hline 00000001\\\hline 00001000\\\hline 00010000\\\hline 00000010\\\hline 00000100\\\hline 00100000\\\hline\end{array} \times \begin{array}{|c|}\hline 1\\\hline 0\\\hline 0\\\hline 1\\\hline 0\\\hline 0\\\hline 1\\\hline 1\\\hline\end{array} = \begin{array}{|c|}\hline 0\\\hline 1\\\hline 1\\\hline 0\\\hline 1\\\hline 1\\\hline 0\\\hline 0\\\hline\end{array}.$$

$$D_2D_1E_2E_1M = \begin{array}{|c|}\hline 00000001\\\hline 00100000\\\hline 00010000\\\hline 01000000\\\hline 10000000\\\hline 00000010\\\hline 00000100\\\hline 00001000\\\hline\end{array} \times \begin{array}{|c|}\hline 0\\\hline 1\\\hline 1\\\hline 0\\\hline 1\\\hline 1\\\hline 0\\\hline 0\\\hline\end{array} = \begin{array}{|c|}\hline 0\\\hline 1\\\hline 0\\\hline 1\\\hline 0\\\hline 0\\\hline 1\\\hline 1\\\hline\end{array} =M.$$

5 Shannon's perfect secrecy cryptosystem

The proposed permutations in chapter 3 (10) 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:

$$p_C(M) = \frac{p(M) \times p_M(C)}{p(C)}, \tag{11}$$

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 [17], [18] 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 with equal probabilities $p(k_i) = \frac{1}{8}$.

Suppose we have plaintext cell $(k_i,\ 1 \leq i \leq 8)$ and suppose these plaintext cells appear in the text with frequencies $p(k_i) = \frac{1}{8}$ and consequently, $p(M) = \sum_{1 \leq i \leq 8} p(k_i)_i = 1$.

In our system for each plaintext cell, k_i and ciphertext cell k_j 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 $p_M(C) = \sum_{1 \leq i \leq 8} p_K(k_{i,j})_i = 1$.

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

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

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

$$p(k_j) = \frac{1}{8} \sum_{1 \leq i \leq 8} p(k_i)_i. \tag{12}$$

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 (12), so we have $\frac{1}{8} \sum_{1 \leq i \leq 8} p(k_i)$ for probability of cell of ciphertext.

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

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

Therefore, from Shannon equality (11) when $p(M) = p(C) = 1$, we get

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

This proves that our system has perfect secrecy.

6 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 Schrödinger equation for the boson system interacting with the potential in the form of a delta function [8].

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 few numbers 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.
7. Time-dependent information due to the unitarity of the evolution operator has the same cryptographic scheme as time-independent information.

References

[1] C.E.Shannon: (July 1948). "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] Daemen J, Rijmen V.: 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] N.N. Bogolyubov, *Lectures on Quantum Statistics*. New York, Gordon and Breach (1967).
[6] N.N. Bogolyubov, N.N.(Jr.)Bogolyubov, *Introduction to Quantum Statistical Mechanics*. Moscow, Nauka (1984.
[7] A.Shamir, R.L.Rivest, L.M.Adleman: Mental Poker, In: Editor D. A. Klarner, The Mathematical Gard- ner, Wadsworth. 37?43 (1981).
[8] Rasulova M.Yu.: The Solution of Quantum Kinetic Equation with Delta Potential and its Application for Information Technology Appl.Math.Inf.Sciences. **12** (4), 685-688 (2018).
[9] M.Yu. Rasulova, Cauchi problem for Bogolyubov kinetic equation, Quantum case. Reports of the Academy of Sciences of the Uzbek SSR, **2**, 6-9 (1976).
[10] D.Ya.Petrina, *Mathematical Foundation of Quantum Statistical Mechanics, Continuous Systems*. Dordrecht-Boston-London, Kluwer Academ.Publishers. 1995.
[11] Bethe H. A.: On the theory of metals, I. Eigenvalues and eigenfunctions of a linear chain of atoms,(German) Zeits. Phys. 205-226 (1931).
[12] Brokate M. and Rasulova M.Yu.: 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).
[13] Rasulova M.Yu.:The BBGKY Hierarchy of Quantum Kinetic Equations and Its Application in Cryptography, Physics of Particles and Nuclei, **51** (4), 781-785 (2020).
[14] Bogolyubov N.N.(Jr.), Rasulova M.Yu.:The Solution of the Hierarchy of Quantum Kinetic Equations for Correlation Matrices with Delta function Potential, Appl.Math.Inf.Sciences. **82** (1), 49 (2024).
[15] Craig A., Tracy I. and Harold Widom J.: The dynamics of the one-dimensional delta-function Bose gas., Phys. A: Math. Theor. **41**, 485204 (2008).
[16] 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).
[17] D.Stinson: Cryptography:Theory and Practice. Second edition, Chapman and Hall/CRC Press (2002).
[18] 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 Kyev, 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 than 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 Endeavours.