Research Article

NEW THREE-PASS PROTOCOL FOR TIME-DEPENDENT INFORMATION

Mukhayo Yunusovna RASULOVA
Institute of Nuclear Physics Academy of Sciences Uzbekistan, Tashkent, 100214, Uzbekistan
e-mail: rasulova@live.com

ABSTRACT

In this paper, a new encryption method based on statistical mechanics is proposed, which enables transmitting information without transmitting the encryption key after sending the information, and also makes it possible to determine its own transformation for each information cell. For these purposes, solutions of the Schrödinger equation (Lieb - Liniger Model) and a hierarchy of quantum kinetic BBGKY equations with the delta function potential are used.

***Keywords**:* Lieb-Liniger model, BBGKY hierarchy of quantum kinetic equations, tree-pass protocol, cryptography

1. INTRODUCTION

One of the most urgent problems of our time is the security of information transfer. This can be seen even from the fact how much spam we receive every day by email. It is known that Advanced Encryption Standard [1], which is the basis of western information encryption, is based on such chaotic actions as permutation of cells, columns and matrix rows, which are the conversion of plaintext to cipher text. These actions are random in nature and therefore do not provide complete confidentiality of information. Complete closeness of information can be provided if each information cell is closed using its own transformation. Such a complete set of transformations can be obtained by solving the equations for a function of N variables, where N is the number of cells. As known, there are very few exactly solvable equations for functions of N variables. One of the most reliable is the Lieb-Liniger Model for describing the system of bosons interacting by means of delta-function potentials. This problem was first solved by Lieb and Liniger [2] and is known in the scientific literature as the Lieb-Liniger Model. Another vulnerable point leading to the loss of information security is the process of the encryption key transmitting after sending encrypted information from the sender (Alice) to the recipient (Bob). This vulnerability can be eliminated if Alice and Bob have their own encryption keys.

Researchers drew attention to the problem of having their own encryption keys long before the development of modern information technologies. Back in the early 30s of the twentieth century, an attempt to play poker at a distance between Professor Niels Boh'r with his son, Heisenberg and other colleagues was unsuccessful, and a problem arose for the players to have their own encryption keys. Only in the 80s of the 20th century, Adi Shamir [3] indicated a way to solve this problem. His method of solving the problem is often called a three-step protocol (Fig.1). It consists of the following steps. Alice encrypts the information with her encryption key and sends it to Bob. Bob encrypts the received information with his own encryption key and returns the information now under the two encryption keys back to Alice. Alice, having received this information, decrypts it with her decryption key and sends the information now under one encryption key back to Bob. Information is now under one encryption key with Bob. Bob, having received this information from Alice, decrypts it with his decryption key. Now the information is without an encryption key and Bob can get acquainted with the information that Alice wanted him to transfer. This problem can be formulated as follows:

$$(D_B(D_A(E_B(E_A P)))) = (D_B(D_A(E_A(E_B P)))) = (D_B(E_B P)) = P,$$

where E_A , E_B the encryption keys of Alice and Bob, respectively, and D_A , D_B the decryption keys of Alice and Bob, respectively.

The encryption keys have the property

$$E_B E_A = E_A E_B$$

that is, the matrices of keys $E_A,\ E_B$ should be commutative. In this paper, we show the possibility of using expressions defined based on the Lieb-Liniger work as commutative Alice and Bob encryption keys for transmit-
ting information based on a three-step protocol. It is shown that to determine the amount of time-dependent information, one can use the solution of the Bogolyubov-Born-Green-Kirkwood-Yvon (BBKGY) hierarchy of quantum kinetic equations, when the equilibrium density matrix is determined through the Bethe ansatz [7].

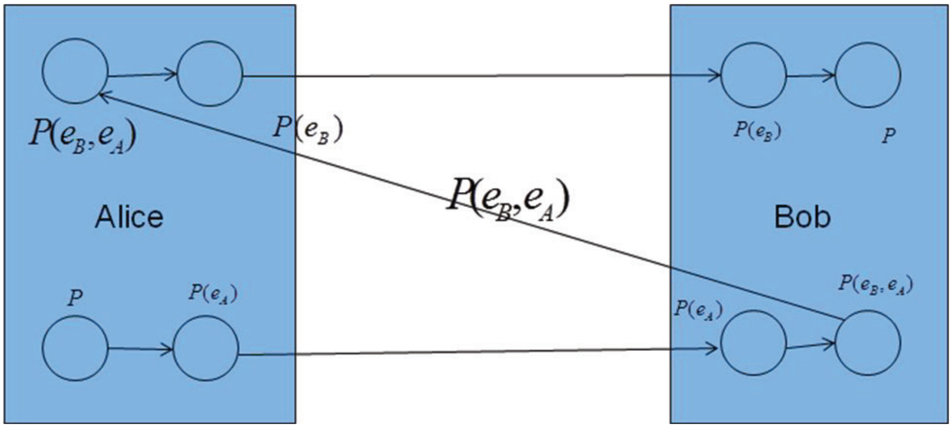

Fig. 1.
Here $P(e_A)=E_A P,\ P(e_B,e_A)=E_B(E_A P),\ P(e_B)=E_B P.$

11. BETHE ANSATZ FOR BOSE GAS

Following [3], consider the solution of the time independent Schrödinger equation for s particles interacting with the potential in the form of a delta function

$$\delta(x-x_0)=\begin{cases}\infty, if\ x=x_0\\ 0, if\ x\neq x_0\end{cases}$$

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

$$-\frac{\hbar^2}{2m}\sum_{i=1}^{s}\Delta\psi(x_1,\dots x_s)+2c\sum_{1\le i<j\le s}\delta(|\,x_i-x_j\,|)\psi(x_1,\dots x_s)=E\psi(x_1,\dots x_s)$$

where the constant $c\geq 0$ and $2c$ is the amplitude of the delta function, $m=1$ - mass of boson, $\hbar=1$ - Plank constant, Δ -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

$$-\sum_{i=1}^{s}\Delta_{x_i}\psi=E\psi, \qquad (1)$$

ith the boundary condition

$$(\frac{\partial\psi}{\partial x_j}-\frac{\partial\psi}{\partial x_i})|_{x_j=x_{i+0}}-(\frac{\partial\psi}{\partial x_j}-\frac{\partial\psi}{\partial x_i})|_{x_j=x_{i-0}}=2c\psi|_{x_j=x_i}$$

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

$$\psi(0,x_1,....,x_s)=\psi(x_1,....,x_s,L), \tag{2}$$

$$\frac{\partial\psi(x,x_2,....,x_s)}{\partial x}|_{x=0}=\frac{\partial\psi(x_2,....,x_s,x)}{\partial x}|_{x=L}\,. \tag{3}$$

Using equation (1) and conditions (2)-(3) we can determine the solution of equation (1) in the form of the Bethe ansatz [3], [4]-[7]:

$$\psi(x_1,...,x_s)=\sum_P a(Per.)Per.\exp(i\sum_{i=1}^{s}k_ix_i) \tag{4}$$

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 $Per.$

of the numbers $\{k\}=k_1,...k_s$ and $a(Per.)$ is a certain coefficient depending on $Per.$:

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

where $\theta_{i,j}=\theta(k_i-k_j)$, $\theta(r)=-2\arctan(r/c)$ and when r is a real value and $-\pi\le\theta(r)\le\pi$. For the case $s=2$, one can find [3], [4] – [7]:

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

and

$$ik_2a_{1,2}+ik_1a_{2,1}-ik_1a_{1,2}-ik_2a_{2,1}=c(a_{1,2}+a_{2,1}),\qquad a_{2,1}=-\frac{c-(k_2-k_1)}{c+(k_2-k_1)}a_{1,2.}\,.$$

If we choose $a_{1,2}=e^{i(k_1x_1+k_2x_2)}$ one gets

$$e^{i(k_2x_1+k_1x_2)}=-\frac{c-(k_2-k_1)}{c+(k_2-k_1)}e^{i(k_1x_1+k_2x_2)}=-e^{i\theta_{2,1}}e^{i(k_1x_1+k_2x_2)}.$$

111. THE BOGOLUBOV-BORN-GREEN-KIRKWOOD-YVON HIERARCHY OF QUANTUM KINETIC EQUATIONS AND ITS SOLUTION

To consider the time-dependent information transfer, we use a chain of Bogoljubov-Born-Green-Kircwood-Yvon quantum kinetic equations in one-dimensional space; in this case, the BBGKY chain with the initial condition has the form [8],[9]:

$$\begin{aligned}&i\frac{\partial\rho_s^{\,L}(x_1,...,x_s;x'_1,...,x'_s,t)}{\partial t}=[H_s^{\,L},\rho_s^{\,L}](x_1,...,x_s;x'_1,...,x'_s,t)+\\&\frac{N}{L}(1-\frac{s}{N})Tr_{x_{s+1}}\sum_{1\le i\le s}(\phi_{i,s+1}(|x_i-x_{s+1}|)-\phi_{i,s+1}(|x'_i-x_{s+1}|)\times\\&\rho_{s+1}^{\,L}(x_1,...,x_s,x_{s+1};x'_1,...,x'_s,x_{s+1},t),\end{aligned} \tag{5}$$

with the initial date

$$\rho_s^{\,L}(x_1,...,x_s;x'_1,...,x'_s,t)|_{t=0}=\rho_s^{\,L}(x_1,...,x_s;x'_1,...,x'_s,0)$$

which has the form

$$i\frac{\partial\rho_s^L(x_1,...,x_s;x'_1,...,x'_s,t)}{\partial t}=[H_s^L,\rho_s^L](x_1,...,x_s;x'_1,...,x'_s,t)+$$
$$\frac{2cN}{L}(1-\frac{s}{N})Tr_{x_{s+1}}\sum_{1\le i\le s}(\delta(|x_i-x_{s+1}|)-\delta(|x'_i-x_{s+1}|)\times$$
$$\rho_{s+1}^L(x_1,...,x_s,x_{s+1};x'_1,...,x'_s,x_{s+1},t),$$

for $1\le s<N$ and

$$i\frac{\partial\rho_s^L(x_1,...,x_s;x'_1,...,x'_s,t)}{\partial t}=[H_s^L,\rho_s^L](x_1,...,x_s;x'_1,...,x'_s,t)$$

for $s=N$.

In Eq. (5), ρ is the density matrix, x_i gives the position of i-th particle in the 1-dimensional space, i=1,2,…,s, t is the time, $m=1$ is the particle mass, $\hbar=1$ is the Planck constant, N is the number of particles in the domain under consideration L (here we consider a system of bosons in the one-dimensional region L , where $\Lambda=L^3$ with volume $V=|\Lambda=L^3|$), [,] denotes the Poisson bracket and H is the Hamiltonian of a system of particles, interacting with a potential in the form of a delta function δ :

$$H=-\sum_{i=1}^{N}\frac{\partial^2}{\partial x_i^2}+\sum_{i<j}\delta(x_i-x_j)$$

Here

$$\rho_s^L(t,x_1,...,x_s;x'_1,...,x'_s)=\sum_i^s\psi_i(t,x_1,...,x_s)\psi^*_i(t,x'_1,...,x'_s).$$

The reduced statistical operator of s particles is $\rho_s^L(x_1,...,x_s;x'_1,...,x'_s)$ when $s>s_0$, s_0 - is a finite value

and the norm is determined as

$$\left|\rho^L\right|_1=\sum_{s=0}^{\infty}\left|\rho_s^L\right|_1,$$

and

$$\left|\rho_s^L\right|_1=\sup\sum_{1\le i\le\infty}\left|\rho_s^L\psi_s^i,\varphi_s^i\right|.$$

The upper bound is taken over all orthonormal systems of finite, twice differentiable functions with compact carrier $\{\psi_i^s\}$ and $\{\varphi_i^s\}$ in $\mathcal{L}_2{}^s(L)$, $s\ge1$ and $|\rho_0^L|_1=|\rho_0^L|$.

Introducing the operator

$$(\Omega(L)\rho_s^L)(x_1,...,x_s;x'_1,...,x'_s)=\frac{N}{L}(1-\frac{s}{N})\int_L\sum_i\rho_{s+1}^L(x_1,...,x_s,x_{s+1};x'_1,...,x'_s,x_{s+1})\times$$
$$g_i^1(x_{s+1})g_i^1(x_{s+1})dx_{s+1},$$

where $g_i^1(x_{s+1)})$ is the complete system of orthogonal vectors in the one-particle space $\mathcal{L}_2(L)$ and using the semigroup method, based on Stone's theorem in the space under consideration, we can determine the unique solution to the BBGKY hierarchy of quantum kinetic equations in the form

$$U^L(T)\rho^L(x_1,...,x_s;x'_1,...,x'_s)=(e^{\Omega(L)}e^{-iH^L{}_s t}e^{-\Omega(L)}\rho e^{iH^L{}_s t})_s(x_1,...,x_s;x'_1,...,x'_s) \tag{6}$$

when $1\leq s<N$ and

$$U^L(t)\rho^L(x_1,....,x_s;x'_1,....,x'_s)=(e^{-iH^L{}_s t}\rho e^{iH^L{}_s t})(x_1,....,x_s;x'_1,....,x'_s), \tag{7}$$

when $s=N$. Here $E_s{}^L=\sum_i^s k^2{}_i$ $0<x_1<...<x_s<L,$ and $0<x'_1<.....<x'_s<L.$

$$\rho_s{}^L(x_1,...,x_s;x'_1,...,x'_s)=\sum_i^s\psi_i(x_1,...,x_s)\psi^*{}_i(x'_1,...,x'_s),$$

where $\psi(x_1,...,x_s)$ Bethe ansatz .

Since the operator $U(t)$ is a unitary operator, then

$$\rho_s{}^L(t,x_1,...,x_s;x'_1,...,x'_s)=\rho_s{}^L(x_1,...,x_s;x'_1,...,x'_s).$$

Therefore

$$\psi(t,x_1,...,x_s)=\psi(x_1,...,x_s),$$

and the tranfer of both stationary information and time-dependent information can be described in terms of the Bethe ansatz..

For formulas (6) and (7), one can determine the von Neumann entropy (amount of information) using the formula: $S=Tr\rho_s{}^L Ln\rho_s{}^L$, where Ln is the natural matrix logarithm.

1V. APPLICATION OF BETHE ANSATZ IN INFORMATION TECHNOLOGY

Consider [7] how the last equation can be used for a three-step transmission of information. Let Alice encrypt information $P=e^{i(k_1x_1+k_2x_2+k_3x_3+k_4x_4)}=e^{i(k_0x_1+k_1x_2+k_1x_3+k_0x_4)}$ using encryption key $E_A=e^{i\theta_{(1+0+0+0),4}}e^{i\theta_{(0+0+1+0),3}}e^{i\theta_{(0+0+0+1),2}}e^{i\theta_{(0+1+0+0),1}}$

in binary and send the encrypted information to Bob:

$$E_AP=e^{i\theta_{(1+0+0+0),4}}e^{i\theta_{(0+0+1+0),3}}e^{i\theta_{(0+0+0+1),2}}e^{i\theta_{(0+1+0+0),1}}e^{i(k_0x_1+k_1x_2+k_1x_3+k_0x_4)}=e^{i(k_1x_1+k_0x_2+k_1x_3+k_0x_4)}.$$

Having received this information, Bob encrypts with his key $E_B=e^{i\theta_{(1+0+0+1),4}}e^{i\theta_{(0+0+1+0),3}}e^{i\theta_{(0+1+0+1),2}}e^{i\theta_{(1+1+0+0),1}}$ and sends the double-encrypted information back to Alice:

$$E_BE_AP=e^{i\theta_{(1+0+0+1),4}}e^{i\theta_{(0+0+1+0),3}}e^{i\theta_{(0+1+0+1),2}}e^{i\theta_{(1+1+0+0),1}}e^{i(k_1x_1+k_0x_2+k_1x_3+k_0x_4)}=e^{i(k_1x_1+k_0x_2+k_1x_3+k_1x_4)}.$$

Having received the last information from Bob, Alice decrypts it using her key $D_A=e^{i\theta_{(0+1+0+0),4}}e^{i\theta_{(0+0+1+0)1,3}}e^{i\theta_{(1+0+0+0),2}}e^{i\theta_{(0+0+0+1),1}}$

$$D_AE_BE_AP\ =e^{i\theta_{(0+1+0+0),4}}e^{i\theta_{(0+0+1+0)1,3}}e^{i\theta_{(1+0+0+0),2}}e^{i\theta_{(0+0+0+1),1}}e^{i(k_1x_1+k_0x_2+k_1x_3+k_1x_4)}=e^{i(k_1x_1+k_1x_2+k_1x_3+k_0x_4)}$$

and sends it back to Bob. Now the information is encrypted with only one key of Bob, and Bob, having received this information, decrypts it with his decryption key : $D_B=e^{i\theta_{(0+0+0+1),4}}e^{i\theta_{(0+0+1+0),3}}e^{i\theta_{(0+1+0+1),2}}e^{i\theta_{(1+1+0+0),1}}$:

$$D_B(D_A(E_B(E_AP)))=e^{-i\theta_{(0+0+0+1),4}}e^{-i\theta_{(0+0+1+0),3}}e^{-i\theta_{(0+1+0+1),2}}e^{-i\theta_{(1+1+0+0),1}}e^{i(k_1x_1+k_1x_2+k_1x_3+k_0x_4)}=$$
$$e^{i(k_0x_1+k_1x_2+k_1x_3+k_0x_4)}=P.$$

The last information is the same as Alice wanted to send Bob.

By expanding encryption keys E_A , E_B and decryption keys D_A , D_B in a matrix form, one can verify that the encryption process and E_A, E_B, D_A. D_B are equivalent to the process of encryption and decryption in matrix form:

$$e^{i(k_2x_1+k_1x_2)} = \sum_{i=0}^{\infty}\frac{i^n}{n!}(\{x_1 \quad x_2\}T\begin{Bmatrix}k_1\\k_2\end{Bmatrix})^n, \text{ where } T=\begin{Bmatrix}0 & 1\\1 & 0\end{Bmatrix}:$$

Example:

$$E_A=\begin{bmatrix}0&1&0&0\\0&0&0&1\\0&0&1&0\\1&0&0&0\end{bmatrix} \qquad E_B=\begin{bmatrix}1&1&0&0\\0&1&0&1\\0&0&1&0\\1&0&0&1\end{bmatrix}$$

$$D_A=\begin{bmatrix}0&0&0&1\\1&0&0&0\\0&0&1&0\\0&1&0&0\end{bmatrix} \qquad D_B=\begin{bmatrix}1&1&0&0\\0&1&0&1\\0&0&1&0\\0&0&0&1\end{bmatrix}.$$

Matrices E_A and E_B are commutative:

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

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

For binary case:

$$\text{Let } P=\begin{bmatrix}0\\1\\1\\0\end{bmatrix} \qquad E_1P=\begin{bmatrix}0&1&0&0\\0&0&0&1\\0&0&1&0\\1&0&0&0\end{bmatrix}\times\begin{bmatrix}0\\1\\1\\0\end{bmatrix}=\begin{bmatrix}1\\0\\1\\0\end{bmatrix}$$

$$E_2E_1P=\begin{bmatrix}1&1&0&0\\0&1&0&1\\0&0&1&0\\1&0&0&1\end{bmatrix}\times\begin{bmatrix}1\\0\\1\\0\end{bmatrix}=\begin{bmatrix}1\\0\\1\\1\end{bmatrix}\qquad D_1E_2E_1P=\begin{bmatrix}0&0&0&1\\1&0&0&0\\0&0&1&0\\0&1&0&0\end{bmatrix}\times\begin{bmatrix}1\\0\\1\\1\end{bmatrix}=\begin{bmatrix}1\\1\\1\\0\end{bmatrix}$$

$$D_2D_1E_2E_1P=\begin{bmatrix}1&1&0&0\\0&1&0&1\\0&0&1&0\\0&0&0&1\end{bmatrix}\times\begin{bmatrix}1\\1\\1\\0\end{bmatrix}=\begin{bmatrix}0\\1\\1\\0\end{bmatrix}=P$$

V. CONCLUSION

In this paper, a new encryption method based on statistical mechanics is put forward, which allows transmitting information without transmitting the encryption key after sending the information, as well as determining its own transformation for each information cell. To this end, solutions of the Schrödinger equation (within Lieb-Liniger Model) and the hierarchy of the BBGKY quantum kinetic equations with a delta-function potential are used.

Advantages of the proposed algorithm and information transfer method:

(1) The presence of a total conversion system ensures full diffusion of bits at each stage of the information transfer in a three-stage protocol.

(2) The algorithm is economically efficient since good diffusion enables using a small number of bits. If in modern programs five cells are required to express letters, then in the proposed approach a letter can beexpressed using one cell.

(3) It is possible to establish a zero correlation between plaintext and encrypted texts, which is condition for perfect encryption.

(4) The proposed method eliminates the encryption keys transfer between partners, which is the most dangerous part of information transfer.

(5) The proposed approach will make it possibleto run programs written using the suggested technique both on current computers and on quantum computers.

(6) The proposed approach will enable boson propagation programming, including bosons of light, in one-dimensional space and in time.

REFERENCES

[1] Daemen J., Rijmen V., The Design of Rijndael, AES The Advanced Encryption Standard Springer, Berlin, 2002.

[2] Lieb E.H., "Liniger W., Exact analysis of an interacting Bose gas. I: The generalsolution and the ground state" , Phys. Rev. vol.130, pp.1605-1616 , 1963.

[3] Shamir A., Rivest R.L. and Adleman L.M., In Mental Poker, Ed. by D. A. Klarner The Mathematical Gardner, Wadsworth, 37-43, 1981.

[4] Bethe H.A., "On the theory of metals. I. Eigenvaluesand eigenfunctions of a linear chain of atoms", Z. Phys., vol.71, pp.205-226, 1931.

[5] Craig A., Tracy I., and Widom H.J., "The dynamics of the one-dimensional delta-function Bose gas", Phys.A: Math. Theor. Vol.41, pp.485204-6, 2008.

[6] Rasulova M.Yu., "The solution of quantum kineticequation with delta potential and its application for information technology", Appl. Math. Inf. Sci. vol.12, pp.685-688, 2018.

[7] Rasulova m.Yu., "The BBGKY Hierarchy of Quantum Kinetic Equations and Its Application in Cryptography" , Physics of Particles and Nuclei, . vol.51(4), pp.781–785, 2020.

[8] Bogolyubov N.N., Lectures on Quantum Statistics, Gordon and Breach, New York, 1967; Mathematical Gardner, Wadsworth, 37-43, 1981.

[9] Bogolyubov N,N,, Bogolyubov N.N.(Jr.), Introductionto Quantum Statistical Mechanics, Nauka, Moscow, 1984 [in Russian].

[10] Petrina D,Ya,, Mathematical Foundation of Quantum Statistical Mechanics, Continuous Systems Kluwer Academic, Dordrecht, 1995.

[11] Rasulova M.Yu., "Cauchi problem for Bogolyubov kinetic equations. Quantum case", Akad. Nauk Uzb.SSR, vol. 2, pp.6-9, 1976 [in Russian].