Applied Mathematics & Information Sciences
*An International Journal*

http://dx.doi.org/10.18576/amis/170304

# Approach to Cryptography from the Lieb-Liniger Model

*Mukhayo Rasulova*

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

Received: 7 Dec. 2022, Revised: 21 Feb. 2023, Accepted: 13 Apr. 2023
Published online: 1 May 2023

**Abstract:** In this paper, using the method of statistical physics, a new encryption method is proposed that provides its own transformation for each cell of information, i.e., the perfect secrecy of information. This new method is based on the Lieb-Liniger model, which describes a gas of bosons in one-dimensional space.

**Keywords:** Statistical physics, Lieb-Liniger Model, advanced encryption system, tree-pass protocol

## 1 Introduction

At the present time, information technology penetrates into all spheres of people's lives. Therefore, the most urgent task of our time is to ensure the security of coding and transmission of information.

Information security is directly related to: 1-probabilistic nature of the compilation of coding programs (even on the basis of AES [1] at present and 2-process of information transfer, namely, the process of transferring the program code of the transmitted information from the sender to the receiving side of the information, which is associated with the possibility of getting information to a third party, or misinformation by the third party.

Eliminating these shortcomings is possible by switching from the probabilistic nature of programming, when several cells of information are covered by one transformation, to the transition to the exact definition of the transformations of each own cell, by solving the equation for functions of s (s-the total number of cells) of variables.

With the probabilistic nature of the encoding, each letter corresponds to several cells with binary symbols, and when deciphering the information, it is easy to calculate the original information due to the difference in the probabilities of the symbols corresponding to the letters.

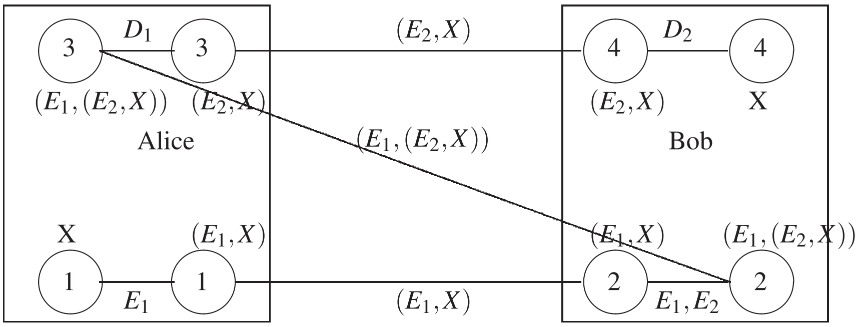
With an exact definition of the transformations of individual cells, each letter corresponds to one cell and, accordingly, the probability of each cell will be equal (that is, the Shannon's perfect secrecy condition [2] is satisfied) and this ensures perfect secrecy of information.

The second drawback associated with the transmission of information can be eliminated by providing own codes and decodes to the sender and recipient of information.

In this paper, using the example of information from 6 cells based on the methods of statistical physics, namely, on the basis of the Lieb-Lineger model [3] and [4] for systems of bosons, as well as on the basis of the Shamir's three pass protocol [5] method (see figure below) for information transfer, the elimination of the above two shortcomings is shown.

Earlier, in works [6], [7], [8] this elimination method is shown on the basis of information consisting of 3 and 4 cells for binary characters. Part 2 of the article is devoted to an overview of the work of Lieb-Lineger and [3], in the third part of the article, the example shows three pass transmission of 6 cell encoded information. In the 4th part of the article, for clarity, this transmission is shown in matrix form. Part 5 is devoted to conclusions.

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




## 2 Bethe Ansatz for Bose gas

Following [3], consider the solution of the time independent Schr*o*dinger equation for $s$ particles interacting with the potential in the form of a delta function

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

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

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

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

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

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 $\psi$ satisfies the periodicity condition in all variables. In [3], it was proved that defining a solution $\psi$ 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

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

for $\psi$ in the domain $\mathbb{R}_1 : 0 < x_1 < x_2 < \ldots < x_s < L$

and the initial periodicity condition is equivalent to the periodicity conditions in

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

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

Using equation (2) we can determine the solution of equation (1) in the form of the Bethe ansatz [3], [9], [10]:

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

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 $P$:

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

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 [3], [4],[7], [8]:

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

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

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

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

## 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

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

using the encryption key

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

and send encrypted information to Bob:

$$(E_1, X) = e^{i\theta_{2,1}}e^{i\theta_{4,2}}e^{i\theta_{1,3}}e^{i\theta_{6,4}}e^{i\theta_{3,5}}e^{i\theta_{5,6}} \times$$
$$e^{i(k_1x_1+k_2x_2+k_3x_3+k_4x_4+k_5x_5+k_6x_6)} =$$
$$e^{i(k_2x_1+k_4x_2+k_1x_3+k_6x_4+k_3x_5+k_5x_6)}.$$

Bob receives this information and encrypts it with his key:

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

and sends the double-encrypted information back to Alice:

$$(E_2(E_1, X)) = e^{i\theta_{4,1}}e^{i\theta_{6,2}}e^{i\theta_{2,3}}e^{i\theta_{5,4}}e^{i\theta_{1,5}}e^{i\theta_{3,6}} \times$$
$$e^{i(k_2x_1+k_4x_2+k_1x_3+k_6x_4+k_3x_5+k_5x_6)} =$$
$$e^{i(k_4x_1+k_6x_2+k_2x_3+k_5x_4+k_1x_5+k_3x_6)}.$$

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

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

$$(D_1(E_2(E_1, X))) = e^{i\theta_{3,1}}e^{i\theta_{1,2}}e^{i\theta_{5,3}}e^{i\theta_{2,4}}e^{i\theta_{6,5}}e^{i\theta_{4,6}} \times$$
$$e^{i(k_4x_1+k_6x_2+k_2x_3+k_5x_4+k_1x_5+k_3x_6)} =$$
$$= e^{i(k_3x_1+k_1x_2+k_5x_3+k_2x_4+k_6x_5+k_4x_6)}$$

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

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

$$(D_2(D_1(E_2(E_1, X)))) = e^{i\theta_{5,1}}e^{i\theta_{3,2}}e^{i\theta_{6,3}}e^{i\theta_{1,4}}e^{i\theta_{4,5}}e^{i\theta_{2,6}} \times$$
$$e^{i(k_3x_1+k_1x_2+k_5x_3+k_2x_4+k_6x_5+k_4x_6)} =$$
$$e^{i(k_1x_1+k_2x_2+k_3x_3+k_4x_4+k_5x_5+k_6x_6)}.$$

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:

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

where

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

Then Alice's encryption key

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

can be represented in matrix form:

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

Similarly, Bob's Encryption key and Decription keys in matrix form are:

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

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

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

Matrices $E_1$ and $E_2$ are commutative:

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

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

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

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

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

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

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

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

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

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

Similarly:

$$D_2 = E_2^{-1} \text{ and } D_2 \times E_2 = \begin{bmatrix} & & & & 1 & \\ & & 1 & & & \\ & & & & & 1 \\ 1 & & & & & \\ & & & 1 & & \\ & 1 & & & & \end{bmatrix}$$

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

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

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

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

Then

$$E_1 X = \begin{bmatrix} & 1 & & & & \\ & & & 1 & & \\ 1 & & & & & \\ & & & & & 1 \\ & & 1 & & & \\ & & & & 1 & \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

$$E_2E_1X=\begin{array}{|c|c|c|c|c|c|}\hline & & & 1 & & \\ \hline & & & & & 1 \\ \hline & 1 & & & & \\ \hline & & & & 1 & \\ \hline 1 & & & & & \\ \hline & & 1 & & & \\ \hline \end{array}\times\begin{array}{|c|}\hline 0\\ \hline 1\\ \hline 1\\ \hline 1\\ \hline 0\\ \hline 0\\ \hline \end{array}=\begin{array}{|c|}\hline 1\\ \hline 0\\ \hline 1\\ \hline 0\\ \hline 0\\ \hline 1\\ \hline \end{array}$$

$$D_1E_2E_1X=\begin{array}{|c|c|c|c|c|c|}\hline & & 1 & & & \\ \hline 1 & & & & & \\ \hline & & & & 1 & \\ \hline & 1 & & & & \\ \hline & & & & & 1 \\ \hline & & & 1 & & \\ \hline \end{array}\times\begin{array}{|c|}\hline 1\\ \hline 0\\ \hline 1\\ \hline 0\\ \hline 0\\ \hline 1\\ \hline \end{array}$$

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

$$D_2D_1E_2E_1X=\begin{array}{|c|c|c|c|c|c|}\hline & & & & 1 & \\ \hline & & 1 & & & \\ \hline & & & & & 1 \\ \hline 1 & & & & & \\ \hline & & & 1 & & \\ \hline & 1 & & & & \\ \hline \end{array}\times\begin{array}{|c|}\hline 1\\ \hline 1\\ \hline 0\\ \hline 0\\ \hline 1\\ \hline 0\\ \hline \end{array}$$

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

## 4 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.

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. The possibility of using the proposed programs, both on modern computers and in quantum computers.
7. Possibility of programming the direction of propagation of bosons in one-dimensional space.

## References


[1] J.Daemen and V.Rijmen, *The Design of Rijndael AES-The Advanced Encryption Standard*, Springer, (2002).

[2] C.E.Shannon, A mathematical theory of communication, *Bell System Techn Journ.*, **27**(3), 379-423, 623-656 (1948).

[3] 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).

[4] 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).

[5] A.Shamir, R.L.Rivest and L.M.Adleman, *Mental Poker*, in The Mathematical Gardner, D. A. Klarner Ed. Wadsworth International, 37–43, (1981).

[6] 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).

[7] 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).

[8] 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).

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

[10] M.Brokate and M.Yu.Rasulova, *The Solution of the Hierarchy of Quantum Kinetic Equations with Delta Potential*, in Industrial Mathematics and Complex Systems, A.H.Siddiqi Ed., Springer, Springer. 165-170, (2017).


**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.