Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/150601

Definition of a Three-Pass Protocol using the Lieb-Liniger Model

*Mukhayo Rasulova** *and Jakhongir Yunusov*

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

Received: 2 May 2021, Revised: 12 Jun. 2021, Accepted: 12 Sep. 2021
Published online: 1 Nov. 2021

Abstract: In this work it is proposed a new encryption method which provides its own transformation for each cell of information. This new method is based on the Lieb-Liniger Model describing a gas of bosons in one dimensional space.

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

1 Introduction

In the past two decades, quantum computing research has attracted more and more attention. ”Mental poker” is the general name for a number of cryptographic problems associated with playing fair at a distance without the need for a trusted third party. Niels Bohr, his son and friends first tried to play poker at a distance without cards in 1933, but the attempt was unsuccessful. In cryptography, a three-step protocol for sending messages is a structure that allows one party to send a message securely to another without the need to exchange or distribute encryption keys. It is called the three-step protocol because the sender and receiver exchange three encrypted messages. The first three-step protocol was developed by Adi Shamir in 1980 [1]. The basic concept of the three-step protocol is that each party has a private encryption key and a private decryption key. Both parties use their keys independently, first to encrypt the message and then to decrypt the message. The protocol uses the encryption function E and the decryption function D. The encryption function uses the encryption key E to convert the plaintext X into an encrypted message. Key D decrypts encrypted information $D(E,X) = X$. Each encryption key E corresponds to a decryption key D, which allows you to recover the message using the decryption function, $D_2(D_1,E_2(E_1,X)) = X$. Sometimes the encryption and decryption functions are the same. Commutative encryption is order independent encryption, that is, it satisfies $D_2(D_1,E_2(E_1,X)) = D_2(D_1,E_1(E_2,X))$ for all keys encryption E_1, E_2 and all messages X. The three-step protocol works as follows:

1. The sender chooses the private encryption key E_1 and the corresponding decryption key D_1. The sender encrypts the message X with the key E_1 and sends the encrypted message (E_1,X) to the recipient.
2. The recipient chooses the private encryption key E_2 and the corresponding key deencryption D_2, super-encrypts the first message $(E_2(E_1,X))$ with the key E_2 and sends the double-encrypted message $(E_2(E_1,X))$ back to the sender.
3. The sender decrypts the second message with the key D_1. Due to the commutative property described above, $(D_1(E_2,(E_1,X))) = (E_2,X)$ is a message encrypted only with the recipient’s private key. The sender sends this to the recipient. The recipient can now decrypt the message using the key D_2, namely $(D_2(E_2,X)) = X$ of the original message.

The basis of modern Western encryption is ”The Design of Rijndael AES-The Advanced Encryption Standard” [2]. It is based on such chaotic actions as permutation of cells, columns and matrix rows, which are the conversion of plaintext to ciphertext. Therefore, it does not provide complete information security. The complete set of transformations, providing each cell of the matrix representing information, can be provided with its own transformation if it is possible to solve the equation for many variables, where the number of variables coincides with the number of cells required for information. Currently, there are several such exactly

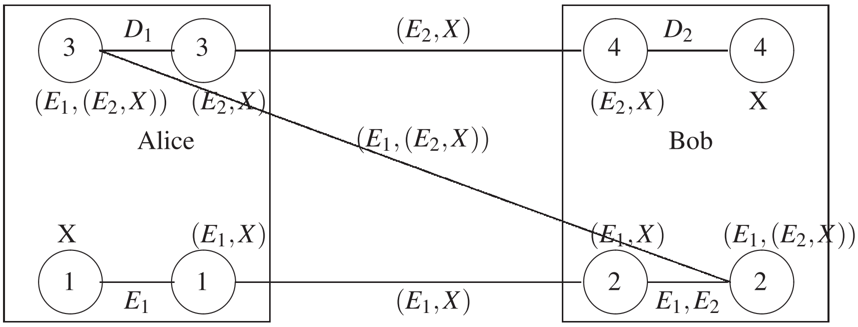
* Corresponding author e-mail: rasulova@live.com

solvable equations that can be used for this purpose. One of the most suitable of these is the Lieb-Liniger Model [3]. In this work, using Lieb-Liniger Model for three-cell information, the possibility of information transmission based on a three-stage protocol is shown.

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 ψ in the domain



2 Bethe Ansatz for Bose gas

Following [3], consider the solution of the time independent Schrődinger 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 $\mathbb{R}$:

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

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

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

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

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

$\mathbb{R}_1: 0<x_1<x_2<\dots<x_s<L$

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 [3], [4] - [8]:

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

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 $\{k\}=k_1,\dots,k_s$ 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 [3], [5] - [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

$$e^{i(k_2y_1+k_1y_2)}=-\frac{c-(k_2-k_1)}{c+(k_2-k_1)}e^{i(k_1y_1+k_2y_2)}=$$

$$-e^{i\theta_{2,1}}e^{i(k_1y_1+k_2y_2)}.$$

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 $X=e^{i(k_1x_1+k_2x_2+k_3x_3)}$ using the encryption key $E_1=-e^{i\theta_{2,1}}e^{i\theta_{1,2}}e^{i\theta_{3,3}}$ and send encrypted information to Bob: $(E_1,X)=-e^{i\theta_{2,1}}e^{i\theta_{1,2}}e^{i\theta_{3,3}}e^{i(k_1x_1+k_2x_2+k_3x_3)}=e^{i(k_2x_1+k_1x_2+k_3x_3)}$. Bob receives this information and encrypts it with his key: $E_2=-e^{i\theta_{2,1}+i\theta_{1,2}+i\theta_{1+2+3,3}}$ and sends the double-encrypted information back to Alice:

$$(E_2(E_1,X))=-e^{i\theta_{2,1}+i\theta_{1,2}+i\theta_{1+2+3,3}}e^{i(k_2x_1+k_1x_2+k_3x_3)}=$$

$$e^{i(k_1x_1+k_2x_2+k_{1+2+3}x_3)}.$$

Having received the latest information from Bob, Alice decrypts it with her key $D_1=-e^{i\theta_{2,1}}e^{i\theta_{1,2}}e^{i\theta_{3,3}}$:

$$(D_1(E_2(E_1,X)))=-e^{i\theta 2,1}e^{i\theta 1,2}e^{i\theta 3,3}\times$$

$$e^{i(k_1x_1+k_2x_2+k_{1+2+3}x_3)}=e^{i(k_2x_1+k_1x_2+k_{1+2+3}x_3)}$$

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 $D_2=-e^{i\theta_{2,1}+i\theta_{1,2}+i\theta_{1+2+3,3}}$:

$$(D_2(D_1(E_2(E_1,X))))=-e^{i\theta_{2,1}+i\theta_{1,2}+i\theta_{1+2+3,3}}\times$$

$$e^{i(k_2x_1+k_1x_2+k_{1+2+3}x_3)}=e^{i(k_1x_1+k_2x_2+k_3x_3)}.$$

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

Expanding in a series of encryption keys E_1, E_2 and decryption D_1, D_2 in matrix form, we can make sure that the encryption process and E_1, E_2, D_1, D_2 are equivalent to the encryption and decryption process in matrix form:

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

$$D_1=\begin{array}{|c|c|c|}\hline & 1 & \\ \hline 1 & & \\ \hline & & 1 \\ \hline\end{array}\qquad D_2=\begin{array}{|c|c|c|}\hline & 1 & \\ \hline 1 & & \\ \hline 1 & 1 & 1 \\ \hline\end{array}$$

Matrices E_1 and E_2 are commutative:

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

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

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

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

Similarly:

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

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

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

Then

$$E_1X=\begin{array}{|c|c|c|}\hline & 1 & \\ \hline 1 & & \\ \hline & & 1 \\ \hline\end{array}\times\begin{array}{|c|}\hline 0 \\ \hline 1 \\ \hline 1 \\ \hline\end{array}=\begin{array}{|c|}\hline 1 \\ \hline 0 \\ \hline 1 \\ \hline\end{array}$$

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

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

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

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. Equality of zero correlation between plaintext and ciphertext, which is a condition for perfect encryption.
4. The lack of a key transfer process between partners is the most dangerous part of information transfer.
5. The possibility of using the proposed programs, both on modern computers and in quantum computers.
6. Possibility of programming the direction of propagation of bosons in one-dimensional space.

Conflict of interest

The authors declare that they have no conflict of interest.

References

[1] Shamir A., Rivest R.L., Adleman L.M.: in Mental Poker, Ed. by D. A. Klarner (The Mathematical Gard- ner, Wadsworth), p. 37–43 (1981).

[2] Daemen J, Rijmen V The Design of Rijndael AES-The Advanced Encryption Standard, Springer, 2002

[3] Lieb E. H. and Liniger W.: Exact analysis of an interacting Bose gas. I: the general solution and the ground state, Phys. Rev., 130. 1605-1616 (1963).

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

[5] 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)

[6] Brokate M. and Rasulova M.Yu.: The Solution of the Hierarchy of Quantum Kinetic Equations with Delta Potential. Industrial Mathematics and Complex Systems.Singapour: Springer. 165-170 (2017).

[7] 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).

[8] 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).

Mukhayo Rasulova is earned her B.Sc. and M.Sc. in Theoretical Physics from Tashkent State University, Uzbekistan in 1971. She earned her Ph.D. degree from Institute of Theoretical Physics, Ukraine National Academy of Sciences in Kiev, Ukraine 1978 and a doctoral degree of sciences in Mathematics and Physics from Institute of Nuclear Physics, Uzbekistan Academy of Sciences, Tashkent, Uzbekistan, in 1995. Her main research works belong to the field of Theoretical and Mathematical Physics. Her scientific interests are devoted to investigation of kinetic and thermodynamic properties of system of interacting particles and infinite systems of charges and inhomogeneity, the BBGKY's hierarchy of quantum kinetic equations for Bose and Fermi particles with different potentials. Also her current research works are devoted to study statistical and kinetic properties of nonlinear optics, theory of quantum information and cryptography. She has more then 80 scientific publications in the field of Statistical Physics, Theoretical and Mathematical Physics. She has been an invited speaker in many international conferences. She is academician of the International Academy of Creative Endeavors.

Jakhongir Yunusov is earned his B.Sc. and M.Sc. from the Tashkent State University of Communications, Uzbekistan. Since 2017 he has been working at the Institute of Nuclear Physics of the Academy of Sciences of Uzbekistan. His current research works belong to the cryptography.