Appl. Math. Inf. Sci. **20**, No. 2, 339-345 (2026)

Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/200203

Quantum Cryptography and Key Encoding on Ion Chains via the Lieb-Liniger Model

Mukhayo Yunusovna Rasulova

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

Received: 14 Nov. 2025, Revised: 22 Dec. 2025, Accepted: 23 Jan. 2026

Abstract: The development of quantum computers is one of the central challenges of modern science. Among various physical platforms, trapped ion–based systems have emerged as a promising approach for information processing. In this work, we present a method for quantum cryptography using one-dimensional ion chains modeled by the Lieb–Liniger Hamiltonian. Effective contact interactions naturally arise in the short-range limit of screened Coulomb potentials between ions, providing a controllable and analytically tractable framework.

Keywords: statistical physics, Bethe ansatz, Lieb-Liniger Model, Shannon perfect secresy condition, tree-pass protocol

1 Introduction

One of the central challenges of modern science is the development of quantum computers. To address this challenge, various physical platforms have been explored, including photons, spins, ions, and other quantum particles. Among these, trapped ion–based systems have emerged as particularly promising for information processing. Research on the design and development of software and algorithms for such systems has been reported in Refs. [1]–[7].

In the present study, we propose a novel approach to quantum cryptography based on one-dimensional chains of trapped ions modeled by the Lieb–Liniger Hamiltonian. Effective contact interactions between ions arise in the short-range limit of screened Coulomb potentials, providing a controllable and analytically tractable system.

The phases of collective excitations in the ion chain are employed to encode cryptographic keys. The integrable dynamics of the Lieb–Liniger model [8,9], solved via the Bethe ansatz, allow precise control over these phases and reliable extraction of keys [10]–[17]. This approach establishes a direct connection between integrable many-body models and practical trapped ion systems, creating a theoretically grounded platform for secure quantum information transmission.

The three-pass cryptographic communication protocol is employed for information transformation in this work. As shown in Fig. 1, the proposed three-stage protocol consists of successive encryption and decryption operations. Alice applies the encryption operations E_1 and E_2, while Bob performs the corresponding inverse operations D_1 and D_2.

2 Effective δ-Interaction in a 1D Ion Chain

2.1 Reduction to one dimension (key step)

Realistic ion chains are inherently three-dimensional, with Coulomb interactions extending in all spatial directions. However, when ions are confined to a tight linear geometry, the transverse motion is strongly suppressed.

The total wave function can be factorized as

$$\Psi(\mathbf{r}) = \psi(x)\,\phi_\perp(y,z),$$

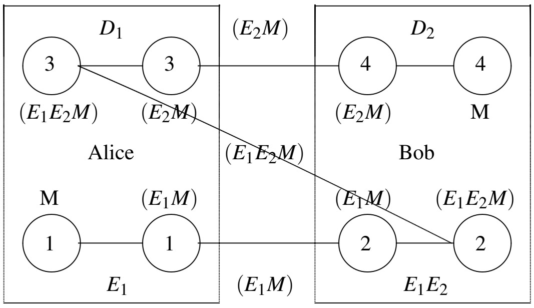
where x, y, and z denote the spatial coordinates of the ion.

Integrating over the transverse coordinates y and z, one obtains an **effective one-dimensional potential**

$$V_{\text{eff}}(x) = \int dy\,dz\,|\phi_\perp(y,z)|^2 \frac{e^2}{\sqrt{x^2+y^2+z^2}} e^{-\kappa\sqrt{x^2+y^2+z^2}},$$

---

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



Intermediate message states are indicated by circles.

Fig. 1: Three-stage cryptographic communication protocol between Alice and Bob. Message M is transformed by encryption operators E_1, E_2 and recovered using decryption operators D_1, D_2.

where κ is the inverse screening length.

This expression defines a smooth short-range interaction in one-dimensional space, where e is the ionic charge. As a result, the dynamics can be effectively reduced to a one-dimensional model in which only the longitudinal coordinate along the chain is relevant.

The key conditions for this reduction are:

- the transverse confinement is sufficiently strong, such that the energy associated with transverse motion greatly exceeds the characteristic interaction energy;
- the typical inter-ion spacing along the chain is much larger than the transverse confinement length scale, justifying the neglect of transverse degrees of freedom;
- screening effects or environmental factors render the effective interaction along the chain short-ranged, allowing a one-dimensional description to capture the dominant correlations.

Under these conditions, the screened Coulomb interaction along the chain can be replaced by an effective one-dimensional potential $V_{\mathrm{eff}}(x)$, which serves as the starting point for the subsequent low-energy analysis and the derivation of a δ-function interaction in the s-wave limit.

2.2 *Low-energy limit (s-wave)*

In the low-energy regime, only s-wave scattering contributes significantly to the interaction between ions. In this limit, the effective inter-ion potential can be approximated by a contact δ-function interaction,

$$V_\delta(x) = g\,\delta(x),$$

where the effective coupling constant g is defined as

$$g = \int_{-\infty}^{\infty} V_{\mathrm{eff}}(x)\,dx.$$

This approximation captures the dominant short-range correlations and is particularly suitable for ion chains without external trapping potentials, where the dynamics are governed primarily by intrinsic interactions.

Under the condition

$$kr_0 \ll 1,$$

where k is the longitudinal momentum and r_0 denotes the characteristic range of the effective interaction (set by the transverse confinement or the screening length κ^{-1}), the dynamics are determined **solely by the one-dimensional scattering length** a_{1D}.

In this regime, any short-range interaction potential can be replaced by

$$V_{\mathrm{eff}}(x) \to g_{1D}\,\delta(x),$$

with

$$g_{1D} = \frac{2\hbar^2}{ma_{1D}},$$

where a_{1D} is the effective one-dimensional scattering length, defined in the low-energy limit of even-parity scattering [18].

In this strict physical and mathematical limit:

- all information about the detailed shape of the Coulomb potential is lost;
- only the scattering parameter remains.

3 Bethe Ansatz for the One-Dimensional Bose Gas

Following Lieb and Liniger [8], we consider a system of s identical bosons interacting via a contact potential in one-dimensional space. The Hamiltonian is given by

$$H = -\frac{1}{2}\sum_{i=1}^{s}\Delta_i + 2c\sum_{1\le i<j\le s}\delta(x_i - x_j).$$

It is well known [8] that solving the stationary Schrödinger equation

$$H\psi = E\psi$$

is equivalent to solving the free Schrödinger equation

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

in each ordered sector

$$\mathscr{R}_1: \quad 0 < x_1 < x_2 < \cdots < x_s < L,$$

subject to the contact boundary conditions

$$\left(\frac{\partial}{\partial x_{j+1}} - \frac{\partial}{\partial x_j}\right)\psi\Big|_{x_{j+1}=x_j} = c\,\psi\big|_{x_{j+1}=x_j},$$

together with periodicity conditions.

3.1 General Bethe Ansatz

In each ordered sector, the eigenfunctions admit the Bethe ansatz representation

$$\psi(x_1,\ldots,x_s) = \sum_{P\in S_s} a(P)P\exp\left(i\sum_{j=1}^{s} k_{P(j)}x_j\right),$$

where the sum is taken over all permutations of the symmetric group S_s. The corresponding energy eigenvalue is

$$E = \sum_{j=1}^{s} k_j^2.$$

For an elementary exchange of two momenta $k_i \leftrightarrow k_j$, the coefficients satisfy [19]

$$a(\cdots j,i\cdots) = S(k_j,k_i)\,a(\cdots i,j\cdots),$$

where the two-particle scattering matrix is

$$S(k_j,k_i) = -\frac{c-i(k_j-k_i)}{c+i(k_j-k_i)} = -e^{i\theta(k_i,k_j)},$$

with $|S(k_i,k_j)| = 1$.

As a consequence of integrability, the amplitude corresponding to an arbitrary permutation factorizes as [20]

$$a(P) = \prod_{i<j} S\left(k_{P(i)},k_{P(j)}\right).$$

3.2 Explicit Three-Particle Bethe Ansatz

For $s = 3$ and in the region $x_1 < x_2 < x_3$, the wave function consists of six plane-wave terms:

$$\begin{aligned}\psi(x_1,x_2,x_3) = {}& e^{i(k_1x_1+k_2x_2+k_3x_3)}\\ &+S(k_2,k_1)\,e^{i(k_2x_1+k_1x_2+k_3x_3)}\\ &+S(k_3,k_2)\,e^{i(k_1x_1+k_3x_2+k_2x_3)}\\ &+S(k_3,k_1)S(k_2,k_1)\,e^{i(k_2x_1+k_3x_2+k_1x_3)}\\ &+S(k_3,k_1)S(k_3,k_2)\,e^{i(k_3x_1+k_1x_2+k_2x_3)}\\ &+S(k_3,k_2)S(k_3,k_1)S(k_2,k_1)\\ &\times e^{i(k_3x_1+k_2x_2+k_1x_3)}.\end{aligned}$$

4 Application of Bethe Ansatz in Information Technology

We demonstrate a three-stage information transfer protocol based on the three-particle Bethe ansatz.

Let the information M be encoded in the three-particle Bethe wave function

$$\begin{aligned}M = \psi(x_1,x_2,x_3) = {}& e^{i(k_1x_1+k_2x_2+k_3x_3)}\\ &+a(k_3,k_2)\,e^{i(k_1x_1+k_3x_2+k_2x_3)}+\ldots\\ &+a(k_1,k_3;k_2,k_3)\,e^{i(k_3x_1+k_2x_2+k_1x_3)} =\\ &e^{i(k_1x_1+k_2x_2+k_3x_3)}\\ &+(S_{3,2})\,e^{i(k_1x_1+k_3x_2+k_2x_3)}+\ldots\\ &+(S_{3,2}S_{3,1}S_{2,1})\,e^{i(k_3x_1+k_2x_2+k_1x_3)},\end{aligned}$$

where the amplitudes $a(P)$ are constructed from two-body scattering matrices $S_{ij} \equiv S(k_i,k_j)$. We consider a three-stage information transfer scheme based on the Bethe ansatz.

Let Alice encrypt information M using the collision operator

$$E_1 = S_{2,1}S_{3,2}S_{1,3},$$

sending the encrypted message to Bob:

$$\begin{aligned}E_1M = {}& S_{2,1}S_{3,2}S_{1,3}\,e^{i(k_1n_1+k_2n_2+k_3n_3)}+\\ &(S_{3,2})S_{2,1}S_{3,2}S_{1,3}\,e^{i(k_1x_1+k_3x_2+k_2x_3)}+\ldots+\\ &(S_{3,2}S_{3,1}S_{2,1})S_{2,1}S_{3,2}S_{1,3}\,e^{i(k_3x_1+k_2x_2+k_1x_3)})\\ &= e^{i(k_3x_1+k_1x_2+k_2x_3)}+\\ &(S_{3,2})\,e^{i(k_3x_1+k_2x_2+k_1x_3)}+\ldots+\\ &(S_{3,2}S_{3,1}S_{2,1})\,e^{i(k_2x_1+k_1x_2+k_3x_3)}.\end{aligned}$$

Bob applies his collision operator

$$E_2 = S_{3,1}S_{1,2}S_{2,3}$$

and sends the double-encrypted message back to Alice:

$$\begin{aligned}E_2(E_1M) = {}& S_{3,1}S_{1,2}S_{2,3}\,e^{i(k_3x_1+k_1x_2+k_2x_3)}+\\ &(S_{3,2})S_{3,1}S_{1,2}S_{2,3}\,e^{i(k_3x_1+k_2x_2+k_1x_3)}+\ldots+\\ &(S_{3,2}S_{3,1}S_{2,1})S_{3,1}S_{1,2}S_{2,3}\,e^{i(k_2x_1+k_1x_2+k_3x_3)} =\\ &e^{i(k_1x_1+k_2x_2+k_3x_3)}+\\ &(S_{3,2})\,e^{i(k_1x_1+k_3x_2+k_2x_3)}+\ldots+\\ &(S_{3,2}S_{3,1}S_{2,1})\,e^{i(k_3x_1+k_2x_2+k_1x_3)}.\end{aligned}$$

Alice decrypts with her inverse operator

$$D_1 = S_{2,1}S_{3,2}S_{1,3}$$

to obtain

$$\begin{aligned} D_1(E_2(E_1M)) = S_{2,1}S_{3,2}S_{1,3}\, e^{i(k_1x_1+k_2x_2+k_3x_3)} &+ \\ (S_{3,2})S_{2,1}S_{3,2}S_{1,3}\, e^{i(k_1x_1+k_3x_2+k_2x_3)} &+ \ldots + \\ (S_{3,2}S_{3,1}S_{2,1})S_{2,1}S_{3,2}S_{1,3}\, e^{i(k_3x_1+k_2x_2+k_1x_3)} &= \\ e^{i(k_3x_1+k_1x_2+k_2x_3)} &+ \\ (S_{3,2})\, e^{i(k_3x_1+k_2x_2+k_1x_3)} &+ \ldots + \\ (S_{3,2}S_{3,1}S_{2,1})\, e^{i(k_2x_1+k_1x_2+k_3x_3)} & \end{aligned}$$

and sends it back to Bob.

Finally, Bob applies his inverse

$$D_2 = S_{3,1}S_{1,2}S_{2,3}$$

to recover the original message:

$$\begin{aligned} D_2(D_1(E_2(E_1M))) = S_{3,1}S_{1,2}S_{2,3}\, e^{i(k_3x_1+k_1x_2+k_2x_3)} &+ \\ (S_{3,2})S_{3,1}S_{1,2}S_{2,3}\, e^{i(k_3x_1+k_2x_2+k_1x_3)} &+ \ldots + \\ (S_{3,2}S_{3,1}S_{2,1})S_{3,1}S_{1,2}S_{2,3}\, e^{i(k_2x_1+k_1x_2+k_3x_3)} &= \\ e^{i(k_1n_1+k_2n_2+k_3n_3)} &+ \\ (S_{3,2})\, e^{i(k_1x_1+k_3x_2+k_2x_3)} &+ \ldots + \\ (S_{3,2}S_{3,1}S_{2,1})\, e^{i(k_3x_1+k_2x_2+k_1x_3)} &= M. \end{aligned}$$

Since the collision operators $S_{i,j}$ satisfy the **Yang–Baxter relations**, and the coefficients $a(\cdot)$ can be expressed via S-operators, the order of applying the S-operators does not affect the outcome. This commutativity, used in the equations for the sequential encryption and decryption operations between Alice and Bob, ensures that the original information is reproduced exactly.

Adaptation for Information Transfer

To adapt the results obtained in Chapter 3 for modern computers based on matrix coding, we introduce the permutation operator P, defined as:

$$e^{i(k_2x_1+k_1x_2)} = \sum_{n=0}^{\infty} \frac{i^n}{n!} \left(\begin{bmatrix} x_1 & x_2 \end{bmatrix} \times P \times \begin{bmatrix} k_1 \\ k_2 \end{bmatrix} \right)^n ,$$

where

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

From this we obtain the matrix form of the encryption and decryption operators.

5 Matrix Form of Encryption and Decryption Operators

We introduce permutation operators in matrix form:

$$E_1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \quad E_2 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix},$$

$$D_1 = E_1^{-1} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad D_2 = E_2^{-1} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

They satisfy the commutation and inversion relations:

$$E_1E_2 = E_2E_1 = I_3, \quad D_1E_1 = D_2E_2 = I_3,$$

where I_3 is the 3×3 identity matrix.

6 Double Encryption and Decryption (Column-Fit)

Let the message be .

$$M = \begin{bmatrix} k_1 \\ k_2 \\ k_3 \end{bmatrix} + (S_{3,2}) \begin{bmatrix} k_1 \\ k_3 \\ k_2 \end{bmatrix} + \cdots + (S_{3,2}S_{3,1}S_{2,1}) \begin{bmatrix} k_3 \\ k_2 \\ k_1 \end{bmatrix} .$$

6.1 First Encryption (E_1)

$$\begin{aligned} E_1M = S_{2,1}S_{3,2}S_{1,3} \begin{bmatrix} k_1 \\ k_2 \\ k_3 \end{bmatrix} + (S_{3,2})S_{2,1}S_{3,2}S_{1,3} \begin{bmatrix} k_1 \\ k_3 \\ k_2 \end{bmatrix} \\ + \cdots + (S_{3,2}S_{3,1}S_{2,1})S_{2,1}S_{3,2}S_{1,3} \begin{bmatrix} k_3 \\ k_2 \\ k_1 \end{bmatrix} = \begin{bmatrix} k_3 \\ k_1 \\ k_2 \end{bmatrix} \\ +(S_{3,2}) \begin{bmatrix} k_3 \\ k_2 \\ k_1 \end{bmatrix} + \cdots + (S_{3,2}S_{3,1}S_{2,1}) \begin{bmatrix} k_2 \\ k_1 \\ k_3 \end{bmatrix} . \end{aligned} \tag{1}$$

6.2 Second Encryption (E_2)

$$\begin{aligned} E_2E_1M = S_{3,1}S_{1,2}S_{2,3} \begin{bmatrix} k_3 \\ k_1 \\ k_2 \end{bmatrix} + (S_{3,2})S_{3,1}S_{1,2}S_{2,3} \begin{bmatrix} k_3 \\ k_2 \\ k_1 \end{bmatrix} \\ + \cdots + (S_{3,2}S_{3,1}S_{2,1})S_{3,1}S_{1,2}S_{2,3} \begin{bmatrix} k_2 \\ k_1 \\ k_3 \end{bmatrix} = \begin{bmatrix} k_1 \\ k_2 \\ k_3 \end{bmatrix} \\ +(S_{3,2}) \begin{bmatrix} k_1 \\ k_3 \\ k_2 \end{bmatrix} + \cdots + (S_{3,2}S_{3,1}S_{2,1}) \begin{bmatrix} k_3 \\ k_2 \\ k_1 \end{bmatrix} . \end{aligned}$$

6.3 First Decryption (D_1)

$$D_1E_2E_1M = S_{2,1}S_{3,2}S_{1,3}\begin{bmatrix}k_1\\k_2\\k_3\end{bmatrix} + (S_{3,2})S_{2,1}S_{3,2}S_{1,3}\begin{bmatrix}k_1\\k_3\\k_2\end{bmatrix}$$

$$+\cdots+(S_{3,2}S_{3,1}S_{2,1})S_{2,1}S_{3,2}S_{1,3}\begin{bmatrix}k_3\\k_2\\k_1\end{bmatrix} = \begin{bmatrix}k_3\\k_1\\k_2\end{bmatrix}$$

$$+(S_{3,2})\begin{bmatrix}k_3\\k_2\\k_1\end{bmatrix}+\cdots+(S_{3,2}S_{3,1}S_{2,1})\begin{bmatrix}k_2\\k_1\\k_3\end{bmatrix}.$$

6.4 Second Decryption (D_2)

$$D_2D_1E_2E_1M = S_{3,1}S_{1,2}S_{2,3}\begin{bmatrix}k_3\\k_1\\k_2\end{bmatrix} + (S_{3,2})S_{3,1}S_{1,2}S_{2,3}\begin{bmatrix}k_3\\k_2\\k_1\end{bmatrix}$$

$$+\cdots+(S_{3,2}S_{3,1}S_{2,1})S_{3,1}S_{1,2}S_{2,3}\begin{bmatrix}k_2\\k_1\\k_3\end{bmatrix} = \begin{bmatrix}k_1\\k_2\\k_3\end{bmatrix}$$

$$+(S_{3,2})\begin{bmatrix}k_1\\k_3\\k_2\end{bmatrix}+\cdots+(S_{3,2}S_{3,1}S_{2,1})\begin{bmatrix}k_3\\k_2\\k_1\end{bmatrix} = M.$$

6.5 Term-by-Term Commutation Relations

In (1) the commutation of E_1 with the coefficients $a(\cdot)$ is verified term by term:

$$E_1\,a(k_3,k_2)\,M = a(k_3,k_2)\,E_1M,$$

Using the swap operators $S(\cdot)$, the term-by-term commutation can be written compactly:

$$E_1\,S(k_3,k_2)M = S(k_3,k_2)\,E_1M:$$

Proof of commutation relations:

$$\begin{bmatrix}0&1&0\\0&0&1\\1&0&0\end{bmatrix}(\begin{bmatrix}1&0&0\\0&0&1\\0&1&0\end{bmatrix}\begin{bmatrix}k_1\\k_3\\k_2\end{bmatrix} = \begin{bmatrix}k_1\\k_2\\k_3\end{bmatrix}) = \begin{bmatrix}k_2\\k_3\\k_1\end{bmatrix} =$$

$$\begin{bmatrix}0&1&0\\1&0&0\\0&0&0\end{bmatrix}(\begin{bmatrix}0&1&0\\0&0&1\\1&0&0\end{bmatrix}\begin{bmatrix}k_1\\k_3\\k_2\end{bmatrix} = \begin{bmatrix}k_3\\k_2\\k_1\end{bmatrix}) = \begin{bmatrix}k_2\\k_3\\k_1\end{bmatrix}.$$

and

$$E_1\,a(k_1,k_3;k_2,k_3)\,M = a(k_1,k_3;k_2,k_3)\,E_1M.$$

$$E_1\,S(k_1,k_2)S(k_1,k_3)S(k_2,k_3)M$$

$$= S(k_1,k_2)S(k_1,k_3)S(k_2,k_3)\,E_1M:$$

$$\begin{bmatrix}0&1&0\\0&0&1\\1&0&0\end{bmatrix}(\begin{bmatrix}0&1&0\\1&0&0\\0&0&1\end{bmatrix}(\begin{bmatrix}1&0&0\\0&0&1\\0&1&0\end{bmatrix}(\begin{bmatrix}0&1&0\\1&0&0\\0&0&1\end{bmatrix}\begin{bmatrix}k_3\\k_2\\k_1\end{bmatrix} = \begin{bmatrix}k_2\\k_3\\k_1\end{bmatrix}) =$$

$$\begin{bmatrix}k_2\\k_1\\k_3\end{bmatrix}) = \begin{bmatrix}k_1\\k_2\\k_3\end{bmatrix}) = \begin{bmatrix}k_2\\k_3\\k_1\end{bmatrix} =$$

$$\begin{bmatrix}0&0&1\\0&1&0\\1&0&0\end{bmatrix}(\begin{bmatrix}1&0&0\\0&0&1\\0&1&0\end{bmatrix}(\begin{bmatrix}0&0&1\\0&1&0\\1&0&0\end{bmatrix}(\begin{bmatrix}0&1&0\\0&0&1\\1&0&0\end{bmatrix}\begin{bmatrix}k_3\\k_2\\k_1\end{bmatrix} = \begin{bmatrix}k_2\\k_1\\k_3\end{bmatrix}) =$$

$$\begin{bmatrix}k_3\\k_1\\k_2\end{bmatrix}) = \begin{bmatrix}k_1\\k_3\\k_2\end{bmatrix}) = \begin{bmatrix}k_2\\k_3\\k_1\end{bmatrix}.$$

Similarly, all encryption and decryption operations E_2, D_1 and D_2 commute term by term.

7 Shannon's Perfect Secrecy Cryptosystem

The proposed permutations in Chapter 6 (4) provide ”perfect secrecy” of information.

As is known, the necessary and sufficient conditions for a cryptosystem to be perfectly secret can be formulated using Bayes' theorem:

Theorem. *A necessary and sufficient condition for perfect secrecy is that*

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

for all messages M and cryptograms C, i.e., $p_M(C)$ should not depend on M.

Indeed, according to Shannon's formula [21], [22]:

$$p_C(M) = \frac{p(M)\,p_M(C)}{p(C)}, \tag{2}$$

where

- $p(M)$ — prior probability of the message M;
- $p_M(C)$ — conditional probability of the cryptogram C given that the message M was selected; equivalently, it is the sum of the probabilities of all keys that transform M into C;
- $p(C)$ — probability of receiving the cryptogram C;
- $p_C(M)$ — posterior probability of the message M given that the cryptogram C has been intercepted.

For the system to achieve perfect secrecy [23,24], the posterior and prior probabilities must be equal for all C and M:

$$p_C(M) = p(M), \quad \forall M,C.$$

Equivalently, one of the following must hold: either $p(M) = 0$ (which is excluded, since the condition must hold for any $p(M)$) or

$$p_M(C) = p(C), \quad \forall M,C.$$

Conversely, if $p_M(C) = p(C)$, then $p_C(M) = p(M)$, and the system achieves perfect secrecy.

To illustrate, consider a plaintext M consisting of $s = 3$ letters, $k_i \in M$, each with equal probability $p(k_i) = \frac{1}{3}$. Suppose we have a plaintext cell k_i ($1 \le i \le 3$), and these cells appear in the text with frequencies $p(k_i) = \frac{1}{3}$, so that $p(M) = \sum_{i=1}^{3} p(k_i) = 1$.

In our system, for each plaintext cell k_i and ciphertext cell $k_j \in C$, there is exactly one key $K(k_{i,j})$ such that

$$K(k_{i,j})k_i = k_j.$$

The probabilities of these keys are equal, $p_K(k_{i,j}) = \frac{1}{3}$, so that

$$p_M(C) = \sum_{i=1}^{3} K(k_{i,j}) = 1.$$

Given the probabilities $p(k_i)$ and the key probabilities $p_K(k_{i,j}) = \frac{1}{3}$, the probability of a ciphertext cell k_j can be computed as

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

When all keys are independent, each key has an equal probability of $1/3$, so we can set

$$p_K(k_{i,j}) = \frac{1}{3}.$$

Accordingly, the probability of a ciphertext cell k_j is

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

In our system, for each plaintext cell k_i and ciphertext cell k_j there is exactly one key $K(k_{i,j})$. Therefore, each key occurs exactly once in the sum above, so the probability of each ciphertext cell is

$$p(k_j) = \frac{1}{3}.$$

The sum of the probabilities of all possible plaintext cells is

$$\sum_{j=1}^{3} p(k_j) = 1.$$

Hence, every ciphertext occurs with equal probability, and

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

Therefore, from Shannon's equality (2), when $p(M) = p(C) = 1$, we get

$$p_C(M) = p(M) \quad \text{and} \quad p_M(C) = p(C),$$

which confirms that the system provides perfect secrecy.

Conclusion

In this paper, we have proposed a novel approach to quantum cryptography based on the complete set of Bethe states of the Lieb–Liniger model, tailored to systems in which the information carriers are trapped ions.

We have rigorously demonstrated that the use of permutation and collision operators, together with coefficients expressed in terms of S-operators, leads to encryption schemes with provable perfect secrecy in the Shannon sense. In particular, all intermediate message states remain completely uninformative to an eavesdropper lacking access to the corresponding decryption operations, thereby satisfying Shannon's necessary and sufficient conditions for perfect secrecy.

Our analysis further shows that reconstructing the system parameters from the Bethe roots is computationally nontrivial, especially as the number of particles and the boundary complexity increase. This property provides structural protection of the cryptographic keys and offers a promising route toward the design of quantum-resistant cryptographic protocols for trapped-ion quantum computers.

Future work will focus on developing formal cryptographic security proofs and extending the proposed protocols to other quantum platforms, further exploiting integrability and fundamental symmetries as intrinsic security mechanisms.

Acknowledgments

The author thanks the Academy of Sciences of Uzbekistan and the Ministry of Higher Education, Science, and Innovation for their support through grant funding.

References

[1] J.I. Cirac, P. Zoller, "New Frontiers in Quantum Information With Atoms and Ions", *Physics Today*, **57**(3), 38–44 (2004), doi:10.1063/1.1712500.

[2] D.P. DiVincenzo, "The Physical Implementation of Quantum Computation", *Fortschr. Phys.*, **48**, 771–783 (2000).

[3] A.M. Steane, "Quantum computing with trapped ions, atoms and light", arXiv:quant-ph/0004053 (2000).

[4] M.A. Nielsen, I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.

[5] D. Kielpinski, C. Monroe, D.J. Wineland, "Architecture for a large-scale ion-based quantum computer", *Nature*, **417**(6890), 709–711 (2002), doi:10.1038/nature00784.

[6] C. Monroe, D.J. Wineland, "Quantum Computing with Ions", *Scientific American*, 64–71 (2008).

[7] R. Blatt, D.J. Wineland, "Entangled states of atomic ions", *Nature*, **453**(7198), 1008–1015 (2008), doi:10.1038/nature07125.

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

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

[10] M. Brokate, M.Yu. Rasulova, "The Solution of the Hierarchy of Quantum Kinetic Equations with Delta Potential", In: Siddiqi A.H., Manchanda P. (eds), *Industrial Mathematics and Complex Systems*, Springer, Singapore, 165–170 (2017).

[11] M.Yu. Rasulova, "The Solution of Quantum Kinetic Equation with Delta Potential and its Application for Information Technology", *Appl. Math. Inf. Sci.*, **12**(4), 685–688 (2018).

[12] 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).

[13] M. Yu. Rasulova, J. Yunusov, ”Definition of a three-pass protocol using the Lieb-Liniger Model”, *Appl. Math. Inf. Sci.*, **15**(6), 677–680 (2021).

[14] M.Yu. Rasulova, ”Approach to Cryptography from the Lieb-Liniger Model”, *Appl. Math. Inf. Sci.*, **7**(3), 431–436 (2023).

[15] M.Yu. Rasulova, ”Creation of a crypto system that satisfies Shannon’s perfect secrecy condition based on the Lieb-Liniger Model”, *Appl. Math. Inf. Sci.*, **7**(4), 631–637 (2023).

[16] M.Yu. Rasulova, ”Using Bethe Ansatz in the Lieb-Liniger Model for Cryptographic Applications”, *Appl. Math. Inf. Sci.*, **19**(5), 989–996 (2025), doi:10.18576/amis/190502.

[17] M.Yu. Rasulova, ”A New Method of Cryptography Providing Perfect Confidentiality of Information”, In: *Mathematical Modeling, Applied Analysis and Computational Methods ICAIM-2023*, Springer, 2025.

[18] M. Olshanii, ”Atomic Scattering in the Presence of an External Confinement and a Gas of Impenetrable Bosons”, *Phys. Rev. Lett.*, **81**, 938 (1998).

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

[20] A. Craig, I. Tracy, J.H. Widom, ”The dynamics of the one-dimensional delta-function Bose gas”, *Phys. A: Math. Theor.*, **41**, 485204 (2008).

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

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

[23] D. Stinson, *Cryptography: Theory and Practice*, 2nd Edition, Chapman and Hall/CRC Press, 2002.

[24] 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.