ФИЗИКА ЭЛЕМЕНТАРНЫХ ЧАСТИЦ И АТОМНОГО ЯДРА
2020. Т. 51. ВЫП. 4. С. 912–922

ЦЕПОЧКА КВАНТОВЫХ КИНЕТИЧЕСКИХ УРАВНЕНИЙ ББГКИ И ЕЕ ПРИМЕНЕНИЕ В КРИПТОГРАФИИ

М. Ю. Расулова *

Институт ядерной физики АН РУ, Улугбек, Узбекистан

Предлагается новый, основанный на статистической механике метод шифрования, позволяющий передавать информацию без процесса передачи ключа шифрования после отправления информации, а также определять для каждой ячейки информации свое собственное преобразование. С этой целью используются решения уравнения Шредингера (модель Либа–Линигера) и цепочки квантовых кинетических уравнений ББГКИ с потенциалом в форме дельта-функции.

The paper proposes a new encryption method based on statistical mechanics, which allows the transfer of encrypted information without the process of transmitting the encryption key after its sending, as well as the definition of its own transformation for each information cell. For this purpose, solutions of the Schrödinger equation (Lieb–Liniger model) and a chain of quantum kinetic equations of BBGKY are used with a delta function potential.

PACS: 03.67.Dd

ВВЕДЕНИЕ

Одной из актуальнейших проблем современности является обеспечение безопасности передачи информации. Состояние этой проблемы в настоящее время далеко от идеального решения. Это видно даже из того, как много спама мы получаем каждый день по электронной почте. Известно, что «Advanced Encryption Standard» [1], являющийся основой западного шифрования информации, основан на таких хаотичных действиях, как перестановка ячеек, столбцов и строк матрицы, представляющих собой преобразование открытого текста в шифротекст. Эти действия имеют случайный характер и поэтому не обеспечивают полную закрытость информации. Полную закрытость информации можно обеспечить, если закрыть каждую ячейку информации своим собственным преобразованием. Такое полное множество преобразований можно получить, если решить уравнения для функции N переменных,

*E-mail: rasulova@live.com

где N — число ячеек. Как известно, имеется очень мало точно решаемых уравнений для функций N переменных. Одной из самых надежных является модель Либа–Линигера для описания систем бозонов, взаимодействующих посредством потенциалов в виде дельта-функции. Данная задача впервые была решена Либом и Линигером [2] и известна в научной литературе как модель Либа–Линигера. Другим уязвимым моментом, приводящим к потере информационной безопасности, является процесс передачи ключа шифрования после отправления шифрованной информации от отправителя (Алиса) к получателю (Бобу). Эту уязвимость можно устранить, если Алиса и Боб будут иметь свои собственные ключи шифрования. Исследователи обратили внимание на проблему наличия собственных ключей шифрования еще задолго до развития информационных технологий современности. Еще в начале 30-х гг. XX в. попытка игры в покер на расстоянии профессора Нильса Бора с сыном, Гейзенбергом и другими коллегами была безуспешной, и возникла проблема наличия у игроков своих собственных ключей шифрования. Только в 80-е гг. XX в. Ади Шамир [3] указал на путь решения этой проблемы. Его метод часто называют трехступенчатым протоколом. Он состоит из следующих шагов. Алиса зашифровывает своим ключом шифрования информацию и отправляет ее Бобу. Боб полученную информацию зашифровывает своим собственным ключом шифрования и возвращает находящуюся теперь под двумя ключами шифрования информацию обратно Алисе. Алиса, получив эту информацию, дешифрует ее своим ключом дешифрования и отправляет информацию, находящуюся теперь под одним ключом, обратно Бобу. Информация теперь находится под одним ключом шифрования Боба. Боб, получив эту информацию от Алисы, дешифрует ее своим ключом дешифрования. Теперь информация находится без ключа шифрования и Боб может ознакомиться с информацией, которую Алиса хотела передать Бобу. Эту задачу можно сформулировать следующим образом:

$$(D_2(D_1(E_2(E_1P)))) = (D_2(D_1(E_1(E_2P)))) = (D_2(E_2P)) = P, \qquad (1)$$

где E_1, E_2 — ключи шифрования Алисы и Боба соответственно и D_1, D_2 — ключи дешифрования Алисы и Боба соответственно. Ключи шифрования имеют свойство

$$E_2E_1 = E_1E_2,$$

т. е. матрицы, представляющие ключи E_1, E_2, должны быть коммутативными.

В настоящей работе рассмотрена возможность использования выражений, определенных на основе работы Либа–Линигера, в качестве коммутативных ключей шифрования Алисы и Боба для передачи информации на основе трехступенчатого протокола. Показано, что для определения количества информации, зависящего от времени, можно использовать реше-

ние цепочки квантовых кинетических уравнений Боголюбова–Борна–Грина–Кирквуда–Ивона (ББГКИ), когда равновесная матрица плотности определяется через анзац Бете.

1. ЦЕПОЧКА КВАНТОВЫХ КИНЕТИЧЕСКИХ УРАВНЕНИЙ БОГОЛЮБОВА–БОРНА–ГРИНА–КИРКВУДА–ИВОНА И ЕЕ РЕШЕНИЕ

Рассмотрим цепочку квантовых кинетических уравнений Боголюбова–Борна–Грина–Кирквуда–Ивона в трехмерной ограниченной области Λ [4, 5]:

$$i\frac{\partial\rho_s^\Lambda(t,x_1,\ldots,x_s;x_1',\ldots,x_s')}{\partial t} = [H_s^\Lambda,\rho_s^\Lambda](t,x_1,\ldots,x_s;x_1',\ldots,x_s') + \\ + \frac{N}{V}\left(1-\frac{s}{N}\right)\mathrm{Tr}_{x_{s+1}}\sum_{1\leqslant i\leqslant s}(\phi_{i,s+1}(|x_i-x_{s+1}|) - \\ - \phi_{i,s+1}(|x_i'-x_{s+1}|))\rho_{s+1}^\Lambda(t,x_1,\ldots,x_s,x_{s+1};x_1',\ldots,x_s',x_{s+1}) \quad (2)$$

с начальным условием

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

В (2) ρ — матрица плотности; x — трехмерная координата частицы; t — время; m — масса частицы; $\hbar = 1$ — постоянная Планка; H — гамильтониан системы частиц; s — число частиц в рассматриваемой области; $\phi_{i,j}(|x_i - x_j|)$ — потенциал взаимодействия между частицами. Гамильтониан системы частиц имеет вид

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

где $\triangle_{x_i}$ — лапласиан.

Предполагается, что операторы ρ_N^L и гамильтониан H_N^L действуют в пространстве H с нулевым граничным условием [6].

Для определения решения цепочки (2) введем согласно [6, 7] пространство ядерных операторов B^Λ, которое является банаховым пространством последовательностей положительно определенных самосопряженных ядерных операторов $\rho_s^\Lambda(x_1,\ldots,x_s;x_1',\ldots,x_s')$:

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

где ρ_0^Λ — комплексное число, $\rho_s^\Lambda \subset B_s^\Lambda$,

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

s_0 — ограниченное число и норма определена как

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

и

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

а верхняя граница берется по всем ортонормированным системам финитных, дважды дифференцируемых функций с компактным носителем $\{\psi_i^s\}$ и $\{\varphi_i^s\}$ в $L_2^s(\Lambda)$, $s \geqslant 1$ и $\left|\rho_0^\Lambda\right|_1 = \left|\rho_0^\Lambda\right|$. Введя оператор

$$\left(\Omega(\Lambda)\rho^\Lambda\right)_s (x_1, \ldots, x_s; x_1', \ldots, x_s') = \frac{N}{V}\left(1 - \frac{s}{N}\right) \times$$
$$\times \int_\Lambda \sum_i \rho_{s+1}^\Lambda (x_1, \ldots, x_s, x_{s+1}; x_1', \ldots, x_s', x_{s+1}) g_i^1(x_{s+1}) \tilde{g}_i^1(x_{s+1})\, dx_{s+1}$$

и используя метод полугруппы, на основе теоремы Стоуна в рассматриваемом пространстве можно определить единственное решение цепочки квантовых кинетических уравнений ББГКИ в виде

$$\rho_s^\Lambda(t, x_1, \ldots, x_s; x_1', \ldots, x_s') = U^\Lambda(t)\rho_s^\Lambda(x_1, \ldots, x_s; x_1', \ldots, x_s') =$$
$$= (\mathrm{e}^{\Omega(\Lambda)} \mathrm{e}^{-iH^\Lambda t}\, \mathrm{e}^{-\Omega(\Lambda)} \rho^\Lambda\, \mathrm{e}^{iH^\Lambda t})_s (x_1, \ldots, x_s; x_1', \ldots, x_s'), \quad (3)$$

где

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

2. АНЗАЦ БЕТЕ ДЛЯ БОЗЕ-ГАЗА

Следуя [2], рассмотрим решение уравнения Шредингера для частиц s, взаимодействующих с потенциалом в виде дельта-функции

$$\delta(|x_i - x_j|) = \begin{cases} \infty, & \text{если } x_i = x_j, \\ 0, & \text{если } x_i \neq x_j. \end{cases}$$

В одномерном пространстве

$$\left(-\sum_1^s \frac{1}{2m} \triangle_{x_i} + 2c \sum_{1 \leqslant i < j \leqslant s} \delta(|x_i - x_j|) \right) \psi = E\psi, \quad (4)$$

где $2c \geqslant 0$ — амплитуда дельта-функции, область рассмотрения задачи определяется как R: все $0 \leqslant x_i \leqslant L$ и волновая функция ψ удовлетворяет условию периодичности по всем переменным. В работе [2] доказано, что определение решения ψ в R эквивалентно определению решения уравнения

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

с граничным условием

$$\left(\frac{\partial\psi}{\partial x_j} - \frac{\partial\psi}{\partial x_k}\right)\Big|_{x_j=x_{k+0}} - \left(\frac{\partial\psi}{\partial x_j} - \frac{\partial\psi}{\partial x_k}\right)\Big|_{x_j=x_{k-0}} = 2c\psi|_{x_j=x_k} \tag{5}$$

для ψ в области R_1 и начальное условие периодичности эквивалентно условиям периодичности в R_1:

$$\psi(0, x_1, \ldots, x_s) = \psi(x_1, \ldots, x_s, L), \quad \psi|_{x_j=x_{k+0}} = \psi|_{x_j=x_{k-0}}.$$

Используя уравнение (5), можно определить решение уравнения (4) в форме анзаца Бете [2, 8]:

$$\psi(x_1, \ldots, x_s) = \sum_{P} a(P) P \exp\left(i \sum_{j=1}^{s} x_j k_j\right) \tag{6}$$

в области R_1: $0 \leqslant x_1 \leqslant x_2 \leqslant \ldots \leqslant x_s \leqslant L$ с собственным значением $E_s = \sum\limits_{i=1}^{s} k^2$, где суммирование проводится по всем перестановкам P чисел k и $a(P)$ является определенным коэффициентом, зависящим от P:

$$a(P) = -\frac{c - i(k_\alpha - k_\beta)}{c + i(k_\alpha - k_\beta)} = -\exp\left(i\theta_{\alpha_1,\alpha_2}\right),$$

где

$$\theta_{i,j} = \theta(k_i - k_j), \quad \theta(r) = -2\tan^{-1}(r/c)$$

и r — реальная величина:

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

Для гамильтониана с потенциалом в виде дельта-функции

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

цепочка квантовых кинетических уравнений ББГКИ для одномерной области имеет вид

$$i\frac{\partial\rho_s^L(t,x_1,\ldots,x_s;x_1',\ldots,x_s')}{\partial t}=[H_s^L,\rho_s^L](t,x_1,\ldots,x_s;x_1',\ldots,x_s')+$$
$$+2c\frac{N}{|L|}\left(1-\frac{s}{N}\right)\mathrm{Tr}_{x_{s+1}}\sum_{1\leqslant i\leqslant s}(\delta_{i,s+1}(|x_i-x_{s+1}|)-$$
$$-\delta_{i,s+1}(|x_i'-x_{s+1}|))\rho_s^L(t,x_1,\ldots,x_s,x_{s+1};x_1',\ldots,x_s',x_{s+1}) \quad (7)$$

для $1\leqslant s<N$ и

$$i\frac{\partial\rho_s^L(t,x_1,\ldots,x_s;x_1',\ldots,x_s')}{\partial t}=[H_s^L,\rho_s^L](t,x_1,\ldots,x_s;x_1',\ldots,x_s') \quad (8)$$

для $s=N$. Здесь рассматриваем систему бозонов в одномерной области L, где $\Lambda=L^3$ объемом $V=|\Lambda=L^3|$. Предполагается, что операторы ρ_N^L и гамильтониан H_N^L действуют в пространстве H с нулевым граничным условием [7].

Согласно формуле (3) решения уравнений (7) и (8) будут иметь вид соответственно [7]:

$$\rho_s^L(t,x_1,\ldots,x_s;x_1',\ldots,x_s')=U^L(t)\rho_s^L(x_1,\ldots,x_s;x_1',\ldots,x_s')=$$
$$=(\mathrm{e}^{\Omega(L)}\,\mathrm{e}^{-iH^Lt}\,\mathrm{e}^{-\Omega(L)}\rho^L\,\mathrm{e}^{iH^Lt})_s(x_1,\ldots,x_s;x_1',\ldots,x_s') \quad (9)$$

и

$$\rho_s^L(t,x_1,\ldots,x_s;x_1',\ldots,x_s')=U^L(t)\rho_s^L(x_1,\ldots,x_s;x_1',\ldots,x_s')=$$
$$=(\mathrm{e}^{-iTt}\,\rho^L\,\mathrm{e}^{iTt})_s(x_1,\ldots,x_s;x_1',\ldots,x_s'), \quad (10)$$

где

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

$$\psi(x_1,\ldots x_s)=\sum_P a(P)P\,\exp\left(i\sum_{j=1}^s x_jk_j\right),$$

$\psi(x_1,\ldots,x_s)$ — анзац Бете (6) и $T=-\sum\limits_i^s\triangle_{x_i}$ — кинетическая энергия системы. Для формул (9) и (10) можно определить энтропию фон Неймана (количество информации) с помощью формулы

$$S=-\mathrm{Tr}\,\rho_s^L(t)\ln\rho_s^L(t),$$

где ln — (натуральный) матричный логарифм.

Для случая $s = 2$ из уравнений (5), (4) при $t = 0$ можно получить [2, 9, 10]:

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

и

$$ik_2a_{1,2} + ik_1a_{2,1} - ik_1a_{1,2} - ik_2a_{2,1} = c(a_{1,2} + a_{2,1})$$

или

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

Если выберем

$$a_{1,2} = \mathrm{e}^{i(k_1x_1+k_2x_2)},$$

получим

$$\mathrm{e}^{i(k_2y_1+k_1y_2)} = -\frac{c - i(k_2 - k_1)}{c - i(k_2 - k_1)}\,\mathrm{e}^{i(k_1y_1+k_2y_2)} = -\mathrm{e}^{i\theta_{2,1}}\,\mathrm{e}^{i(k_1y_1+k_2y_2)}.$$

3. ПРИМЕНЕНИЕ АНЗАЦА БЕТЕ В ИНФОРМАЦИОННОЙ ТЕХНОЛОГИИ

Рассмотрим, как последнее уравнение может быть использовано для трехступенчатой передачи информации. Пусть Алиса шифрует информацию $P = \mathrm{e}^{i(k_1x_1+k_2x_2+k_3x_3+k_4x_4)}$ с помощью ключа шифрования $E_1 = \mathrm{e}^{i\theta_{1,4}}\,\mathrm{e}^{i\theta_{4,3}}\,\mathrm{e}^{i\theta_{3,2}} \times \mathrm{e}^{i\theta_{2,1}}$ и отправляет ее Бобу:

$$E_1P = \mathrm{e}^{i\theta_{1,4}}\,\mathrm{e}^{i\theta_{4,3}}\,\mathrm{e}^{i\theta_{3,2}}\,\mathrm{e}^{i\theta_{2,1}}\,\mathrm{e}^{i(k_1x_1+k_2x_2+k_3x_3+k_4x_4)} = \\ = \mathrm{e}^{i(k_2x_1+k_3x_2+k_4x_3+k_1x_4)}.$$

Боб, получив эту информацию, шифрует ее своим ключом $E_2 = \mathrm{e}^{i\theta_{2,4}}\,\mathrm{e}^{i\theta_{1,3}} \times \mathrm{e}^{i\theta_{4,2}}\,\mathrm{e}^{i\theta_{3,1}}$ и отправляет дважды зашифрованную информацию обратно Алисе:

$$E_2E_1P = \mathrm{e}^{i\theta_{2,4}}\,\mathrm{e}^{i\theta_{1,3}}\,\mathrm{e}^{i\theta_{4,2}}e^{i\theta_{3,1}}\,\mathrm{e}^{i(k_2x_1+k_3x_2+k_4x_3+k_1x_4)} = \\ = \mathrm{e}^{i(k_4x_1+k_1x_2+k_2x_3+k_3x_4)}.$$

Получив последнюю информацию от Боба, Алиса дешифрует ее своим ключом $D_1 = \mathrm{e}^{i\theta_{3,4}}\,\mathrm{e}^{i\theta_{2,3}}\,\mathrm{e}^{i\theta_{1,2}}\,\mathrm{e}^{i\theta_{4,1}}$:

$$D_1E_2E_1P = \mathrm{e}^{i\theta_{3,4}}\,\mathrm{e}^{i\theta_{2,3}}\,\mathrm{e}^{i\theta_{1,2}}\,\mathrm{e}^{i\theta_{4,1}}\,\mathrm{e}^{i(k_4x_1+k_1x_2+k_2x_3+k_3x_4)} = \\ = \mathrm{e}^{i(k_3x_1+k_4x_2+k_1x_3+k_2x_4)}$$

и отправляет обратно Бобу. Теперь информация зашифрована только одним ключом Боба. Боб, получив эту информацию, дешифрует ее своим ключом дешифрования $D_2 = \mathrm{e}^{i\theta_{2,4}}\,\mathrm{e}^{i\theta_{1,3}}\,\mathrm{e}^{i\theta_{4,2}}\,\mathrm{e}^{i\theta_{3,1}}$:

$$D_2 D_1 E_2 E_1 P = \mathrm{e}^{i\theta_{2,4}}\,\mathrm{e}^{i\theta_{1,3}}\,\mathrm{e}^{i\theta_{4,2}}\,\mathrm{e}^{i\theta_{3,1}}\,\mathrm{e}^{i(k_3x_1+k_4x_2+k_1x_3+k_2x_4)} = \\ = \mathrm{e}^{i(k_1x_1+k_2x_2+k_3x_3+k_4x_4)}.$$

Последняя информация совпадает с информацией, которую Алиса хотела отправить Бобу. Разлагая в ряд ключи шифрования E_1, E_2 и дешифрования D_1, D_2 в матричной форме, можно убедиться, что процесс шифрования и E_1, E_2, D_1, D_2 эквивалентны процессу шифрования и дешифрования в матричной форме:

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

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

Матрицы E_1 и E_2 являются коммутативными:

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

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

Также можно показать, что E_1^{-1} является обратной E_1:

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

Аналогично

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

Приведем пример трехступенчатой передачи информации вышеуказанными матрицами.

Пусть начальная информация имеет вид

$$X = \begin{array}{|c|}\hline 1 \\ \hline 2 \\ \hline 3 \\ \hline 4 \\ \hline \end{array}.$$

Тогда

$$E_1 X = \begin{array}{|c|c|c|c|}\hline & 1 & & \\ \hline & & 1 & \\ \hline & & & 1 \\ \hline 1 & & & \\ \hline \end{array} \times \begin{array}{|c|}\hline 1 \\ \hline 2 \\ \hline 3 \\ \hline 4 \\ \hline \end{array} = \begin{array}{|c|}\hline 2 \\ \hline 3 \\ \hline 4 \\ \hline 1 \\ \hline \end{array},$$

$$E_2 E_1 X = \begin{array}{|c|c|c|c|}\hline & & 1 & \\ \hline & & & 1 \\ \hline 1 & & & \\ \hline & 1 & & \\ \hline \end{array} \times \begin{array}{|c|}\hline 2 \\ \hline 3 \\ \hline 4 \\ \hline 1 \\ \hline \end{array} = \begin{array}{|c|}\hline 4 \\ \hline 1 \\ \hline 2 \\ \hline 3 \\ \hline \end{array},$$

$$D_1 E_2 E_1 X = \begin{array}{|c|c|c|c|}\hline & & & 1 \\ \hline 1 & & & \\ \hline & 1 & & \\ \hline & & 1 & \\ \hline \end{array} \times \begin{array}{|c|}\hline 4 \\ \hline 1 \\ \hline 2 \\ \hline 3 \\ \hline \end{array} = \begin{array}{|c|}\hline 3 \\ \hline 4 \\ \hline 1 \\ \hline 2 \\ \hline \end{array},$$

$$D_2 D_1 E_2 E_1 X = \begin{array}{|c|c|c|c|}\hline & & 1 & \\ \hline & & & 1 \\ \hline 1 & & & \\ \hline & 1 & & \\ \hline \end{array} \times \begin{array}{|c|}\hline 3 \\ \hline 4 \\ \hline 1 \\ \hline 2 \\ \hline \end{array} = \begin{array}{|c|}\hline 1 \\ \hline 2 \\ \hline 3 \\ \hline 4 \\ \hline \end{array} = X.$$

В бинарном представлении пусть начальная информация имеет вид

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

Тогда

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

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

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

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

ЗАКЛЮЧЕНИЕ

В работе предлагается новый, основанный на статистической механике метод шифрования, позволяющий передавать информацию без процесса передачи ключа шифрования после отправления информации, а также определять для каждой ячейки информации свое собственное преобразование. С этой целью используются решения уравнения Шредингера (модель Либа–Линигера) и цепочки квантовых кинетических уравнений ББГКИ с потенциалом в форме дельта-функции.

Преимущества предлагаемых алгоритма и метода передачи информации:

— наличие полной системы преобразований обеспечивает полную диффузию битов на каждом этапе передачи информации в трехступенчатом протоколе;

— алгоритм экономически эффективен, поскольку хорошая диффузия обеспечивает использование небольшого количества бит (если в современных программах для выражения букв требуется пять ячеек, то в предлагаемом подходе можно выразить букву одной ячейкой);

— имеется возможность установления нулевой корреляции между открытым и шифрованным текстами, что является условием идеального шифрования;

— предлагаемый метод обеспечивает исключение передачи ключей шифрования между партнерами, что является самой опасной частью передачи информации;

— данный подход даст возможность использовать программы, составленные по предлагаемой методике, как на современных, так и на квантовых компьютерах;

— данный подход даст возможность программировать распространение бозонов, в том числе фотонов (света), в одномерное пространство и во времени.

СПИСОК ЛИТЕРАТУРЫ

1. *Daemen J., Rijmen V.* The Design of Rijndael: AES — The Advanced Encryption Standard. Berlin; Heidelberg; New York; Barcelona; Hong Kong; London; Milan; Paris; Tokyo: Springer, 2002.
2. *Lieb E. H., Liniger W.* Exact Analysis of an Interacting Bose Gas. I: The General Solution and the Ground State // Phys. Rev. 1963. V. 130. P. 1605–1616.
3. *Shamir A., Rivest R. L., Adleman L. M.* Mental Poker // The Mathematical Gardner / Ed. by D. A. Klarner. Wadsworth, 1981. P. 37–43.
4. *Bogolyubov N. N.* Lectures on Quantum Statistics. New York: Gordon and Breach, 1967; Избранные труды. Т. 2. Киев: Наук. думка, 1970.
5. *Bogolyubov N. N., Bogolyubov N. N., Jr.* Introduction to Quantum Statistical Mechanics. M.: Nauka, 1984.
6. *Petrina D. Ya.* Mathematical Foundation of Quantum Statistical Mechanics, Continuous Systems. Dordrecht; Boston; London: Kluwer Acad. Publ., 1995.
7. *Расулова М. Ю.* Задача Коши для кинетических уравнений Боголюбова. Квантовый случай // Изв. АН УзССР. 1976. № 2. С. 6–9.
8. *Bethe H. A.* On the Theory of Metals. I. Eigenvalues and Eigenfunctions of a Linear Chain of Atoms // Z. Phys. 1931. P. 205–226 (in German).
9. *Craig A., Tracy I., Harold Widom J.* The Dynamics of the One-Dimensional Delta-Function Bose Gas // Phys. A: Math. Theor. 2008. V. 41 P. 485204-1–485204-6.
10. *Rasulova M. Yu.* The Solution of Quantum Kinetic Equation with Delta Potential and Its Application for Information Technology // Appl. Math. Inf. Sci. 2018. V. 12, No. 4. P. 685–688.