

характеризуют проективно точечные пространства линейных элементов, где $\mathcal{Z}_{bg}^a(x)$ - объект аффинной связности с кручением, зависящей только от координат точки $M(x)$, $\Gamma_{bg}^a = \mathcal{Z}_{(bg)}^a$. Из (10), (11), при $\mathcal{Z}_{bg}^a = 0$, получим связность проективно точечных пространств линейных элементов с кручениями.

Если $p^a = \mathbf{x}^a$ - опорный касательный псевдовектор, то получим уравнение геодезических

$$\Gamma : \mathbf{x}^a + \Phi_{bg}^a \mathbf{x}^b \mathbf{x}^g = x \mathbf{x}^a, \quad (12)$$

пространства линейных элементов $B_{x, \mathbf{x}}$, где

$\Phi_{bg}^a(x, \mathbf{x})$ - присоединенная аффинная связность без кручения.

Следующее преобразование

$$\bar{\Phi}_{bg}^a = \Phi_{bg}^a + 2d_{(b}^a q_{g)} + \mathbf{x}^a a_{bg} + M_{bg}^a \quad (13)$$

сохраняет форму дифференциальных уравнений аффинных Γ - путей, где $M_{bg}^a \mathbf{x}^b \mathbf{x}^g = 0$,

$$M_{bg}^a(x, l\mathbf{x}) = M_{bg}^a(x, \mathbf{x}).$$

Формула (13) через объекты связности Картана-Лаптева можно записать так

$$\bar{L}_{(bg)}^a + \bar{F} \bar{C}_{(bg)}^a = L_{(bg)}^a + F C_{(bg)}^a + 2d_{(b}^a q_{g)} + \mathbf{x}^a a_{bg} + M_{bg}^a, \quad (14)$$

где $\bar{C}_{bg}^a \mathbf{x}^g = 0$, $C_{bg}^a \mathbf{x}^g = 0$. Равенство (13), (14) являются однородными нулевого измерения относительно $\mathbf{x}^a$.

СПИСОК ЛИТЕРАТУРЫ

1. Ферзалиев А.С. О связностях, индуцированных объектами Картана - Лаптева // Publ. Math. Debrecen, 1990, Т.37. Fasc. 1-2. P.115 - 120.
2. Ферзалиев А.С. Пространство линейных элементов присоединенной связности // Изв. вузов. Сер. Математика, 1988, №10, С.55-64.

КВАНТОВАНИЕ РЕШЕНИЙ ОДНОГО ДИФФЕРЕНЦИАЛЬНОГО УРАВНЕНИЯ ВТОРОГО ПОРЯДКА

Флоринский В.В., Чеканов Н. А.

Белгородский государственный университет,
Белгород

Рассмотрим гамильтонову функцию одномерной системы

$$H(x, p) = \frac{p^2}{2} + \frac{x^2}{2} + a x^4, \quad (1)$$

где x и p - канонически сопряженные переменные, a - малый параметр ($a \ll 1$). Уравнения движения данной системы можно свести к одному дифференциальному уравнению второго порядка:

$$\ddot{x} + x + 4a x^3 = 0, \quad (2)$$

которое называется уравнением Дюффинга [1]. Методом Линдштедта-Пуанкаре [2] получаем решение уравнения (2) в первом порядке по a

$$x(t) = a \cos(wt + j_0) + \frac{1}{8} a a^3 \cos 3 \cdot (wt + j_0), \quad (3)$$

$$w = 1 + \frac{3}{2} a a^2, \quad (4)$$

j_0 и a - произвольные постоянные, зависящие от начальных условий, которые без потери общности выберем в виде $x(0) = -x_E$, $\dot{x}(0) = 0$. Через $\pm x_E$ обозначены корни уравнения

$$V(x) = E, \quad (5)$$

где $V(x) = \frac{1}{2} x^2 + a x^4$ - потенциальная функция системы (1), E - полная энергия.

$$\begin{cases} a \cos j_0 + \frac{1}{8} a a^3 \cos 3j_0 = -x_E, \\ a \sin j_0 + \frac{3}{2} a a^3 \left(\sin j_0 + \frac{1}{4} \sin 3j_0 \right) = 0, \end{cases}$$

Для определения постоянных интегрирования получаем следующую систему из которой находим,

$$\text{что } j_0 = 0 \text{ и } a = x_E \left(1 - \frac{1}{8} x_E^4 a \right).$$

Заметим, что произвольную постоянную a при таком выборе начальных условий можно выразить через полную энергию E . Второе слагаемое в скобках в последнем выражении для a является величиной пятого порядка малости по a , и в рассматриваемом приближении им можно пренебречь. Таким образом, можно считать, что $a = x_E$ и рассматривать a как корень уравнения (5). Подставив a в выражение (5), и разрешив полученное уравнение методом итераций, найдем выражение a через E

$$x(t) = a \cos wt + \frac{1}{8} a a^3 \cos 3wt.$$

$a^2 = 2E - 9aE^2$. В итоге решение (3) в первом порядке по a примет вид

$$4 \int_0^{\frac{p}{2w}} \dot{x}^2(t) dt = h \left(n + \frac{1}{2} \right), \quad n = 1, 2, \mathbf{K},$$

Произведем квантование полученных периодических решений уравнения Дюффинга, отобрав из них те, которые удовлетворяют условию где h - постоянная Планка.

$$p(2E - 9aE^2) = h \left(n + \frac{1}{2} \right)$$

Подставив частоту (4), а также выражения для $\dot{x}^2(t)$ и $a^2 = 2E - 9aE^2$ в условие квантования, получим

Квантовый аналог гамильтоновой функции (1) получится при помощи известной подстановки

$p \rightarrow \frac{ih}{2p} \cdot \frac{d}{dx}$. Тогда приближенный спектр полученного дифференциального оператора определится по формуле

$$E_n = \hbar \left(n + \frac{1}{2} \right) + \frac{3}{2} a \hbar^2 \left(n^2 + n + \frac{1}{4} \right)$$

где $\hbar = \frac{h}{2p}$. Эта формула совпадает с результа-

том стандартной теории возмущений с точностью до последнего слагаемого во второй скобке. В частности, при $a = 0$ имеем известный случай гармонического осциллятора.

СПИСОК ЛИТЕРАТУРЫ

1. Найфэ А.Х. Методы возмущений. М.:МИР, 1976, 455с.
2. Де Брёйн Н.Г. Асимптотические методы в анализе. М.: ИИЛ, 1961, 247 с.
3. Давыдов А.С. Квантовая механика. М.: Физматгиз, 1963, 748с.

АНАЛИЗ ПРОТОКОЛОВ КВАНТОВОЙ КРИПТОГРАФИИ BB84 И B92

Хайров И.Е., Троцюк Е.В.

Квантовая криптография представляет собой одно из многообещающих и уже реализованных в практических приложениях направлений в рамках квантовой теории информации. Методами квантовой криптографии удается создавать абсолютно случайные секретные ключи между пользователями квантовой линии связи. Для достижения абсолютной случайности биты ключа необходимо передавать посредством отдельных фотонов, параметры которых, в соответствии с квантовой физикой, являются неопределенными. В начале 80-х годов подобную схему предложили Чарльз Беннет (Charles Bennett) из IBM и Жиль Браскар (Gilles Brassard) из Монреальского университета. Данный протокол получил название BB84. Несколько позже, в 1992 году, была модернизирована эта схема и на свет появился новый протокол, названный B92.

В работе проводится сравнительный анализ указанных двух протоколов квантовой криптографии. Для этих целей разработана программа для ЭВМ. Данная программа позволяет визуально наблюдать работу протоколов при наличии и отсутствии несанкционированного доступа (НСД). На рис. 1 представлены примеры работы протоколов BB84 и B92 при наличии НСД методом непосредственного съема и генерации.



Рисунок 1. Пример работы протоколов BB84 и B92 при наличии НСД

В качестве выходных данных программа рассчитывает вероятность правильного приема ключевой информации легальными пользователями и вероятность попадания этой информации (или ее части) злоумышленнику, осуществляющему НСД.

Из рис. 1 видно, что наличие анализатора агента вносит существенную неопределенность в результаты измерения поляризации фотонов получателем. Действительно, в случае протокола BB84 на приемном конце квантовой линии связи регистрируется фотон с типом поляризации, ортогональным переданному фотону. В случае же протокола B92, легальным получа-

телем возможна регистрация фотона с ненулевой вероятностью, хотя его анализатор ориентирован ортогонально поляризатору отправителя, что невозможно при отсутствии НСД.

Основным отличием протоколов BB84 и B92 является то, что даже при отсутствии в канале несанкционированного съема информации вероятность правильной регистрации типа поляризации фотонов (формирование ключевой последовательности бит) в протоколе B92 в два раза меньше чем в протоколе BB84.