

ИСПОЛЬЗОВАНИЕ МЕТОДОВ ЧИСЛЕННОГО МОДЕЛИРОВАНИЯ ДЛЯ ПРЕДСКАЗАНИЯ ПОВЕДЕНИЯ КВАНТОВЫХ ТОЧЕК В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ

Ефремова А.Ю.

*Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь*

Научный руководитель: Алефиренко В.М. – к.т.н., доцент, доцент кафедры ПИКС

Аннотация. Одним из наиболее перспективных решений для защиты информации является шифрование с помощью квантовых точек. В данной статье рассматривается возможность использования численных методов моделирования для прогнозирования поведения спектров квантовых точек. Основное внимание уделяется решению двумерного стационарного уравнения Шредингера методом конечных элементов с использованием эрмитовых функций. Результатом решения данного уравнения являются энергетические уровни, позволяющие предсказать спектры поглощения, что важно для оптимизации параметров квантового шифрования и повышения его устойчивости к внешним воздействиям.

Ключевые слова: квантовое шифрование, квантовые точки, спектры поглощения, методы численного моделирования, уравнение Шредингера.

Введение. В последние десятилетия наблюдается стремительное развитие технологий, связанных с обработкой и защитой данных. В условиях постоянного роста объемов информации и увеличения числа киберугроз, вопросы безопасности данных становятся особенно актуальными. Одним из наиболее перспективных направлений в этой области является использование квантовых технологий, в частности, квантовых точек, для шифрования данных. Квантовые точки, будучи наноразмерными полупроводниковыми структурами, обладают уникальными оптическими и электронными свойствами. Благодаря этим свойствам они успешно применяются в квантовой криптографии. Численное моделирование физических процессов, связанных с квантовыми точками, играет ключевую роль в понимании их поведения и взаимодействия с окружающей средой. С помощью современных вычислительных методов и алгоритмов можно проводить детальный анализ свойств квантовых точек, что позволяет оптимизировать их использование в системах шифрования [1–3].

Основная часть. Квантовое шифрование – это метод защиты информации, основанный на использовании квантовых битов для передачи информации, что обеспечивает высокий уровень безопасности. Этот вид шифрования использует квантовую механику для выполнения криптографических задач, которые повышают безопасность передаваемых данных. В отличие от традиционных методов шифрования, таких как *AES* и *RSA*, которые опираются на сложные математические вычисления, квантовое шифрование использует физические свойства квантовых битов (кубитов) для защиты данных, делая их более сложными для взломов.

Квантовые точки – это наноразмерные полупроводниковые кристаллы, которые обладают уникальными оптическими и электронными свойствами благодаря квантовым эффектам.

Спектры поглощения квантовых точек зависят от их размера, формы и материала, из которого они изготовлены. Эти спектры могут быть использованы для шифрования информации, так как они представляют собой уникальные «отпечатки» для каждой квантовой точки. При передаче информации через квантовые точки можно манипулировать их спектрами поглощения, изменяя параметры, такие как размер или состав, что позволяет создавать различные состояния, которые могут быть использованы для шифрования данных.

При использовании спектров поглощения в квантовом шифровании информация может быть закодирована в виде различных уровней энергии, которые соответствуют различным состояниям квантовых точек.

При этом, благодаря квантовым эффектам, любое вмешательство в систему, например, попытка перехвата информации, приведет к изменению состояния квантовых точек, что будет немедленно замечено. Это свойство обеспечивает высокий уровень безопасности, так как злоумышленник не сможет получить доступ к закодированной информации без ее изменения.

Кроме того, использование квантовых точек в шифровании позволяет интегрировать эту технологию в существующие оптические системы связи, что делает ее более практичной для применения в реальных условиях. Квантовые точки могут быть использованы в качестве источников фотонов, которые передают информацию на большие расстояния, обеспечивая при этом защиту от перехвата [1].

В рамках шифрования с помощью квантовых точек, можно использовать различные численные и математические методы, а также численные модели физических процессов для прогнозирования параметров шифрования и его качества.

Численные методы – это набор алгоритмов, используемых для решения математических задач, которые не могут быть решены аналитически или требуют значительных вычислительных ресурсов.

Численные методы, такие как метод Монте-Карло, могут быть использованы для моделирования статистических свойств квантовых точек, включая распределение энергии и вероятности переходов между энергетическими уровнями. Среди подобных методов можно выделить метод функционала плотности, который позволяет исследовать электронные структуры квантовых точек с высокой точностью, демонстрируя, как электронные состояния изменяются в зависимости от размера и формы квантовой точки, что, в свою очередь, влияет на ее оптические свойства.

В результате применения численных методов исследователи могут не только предсказывать спектры поглощения, но и оптимизировать параметры квантовых точек для достижения желаемых свойств.

Математические методы – это совокупность подходов, используемых для решения математических задач и анализа различных явлений.

Численные модели физических процессов – это более сложные математические модели, которые используют численные методы для решения физических уравнений и описания различных явлений в природе. Эти модели позволяют исследовать сложные системы, для которых аналитическое решение невозможно или крайне затруднительно [2].

Численные модели физических процессов позволяют использовать методы Монте-Карло для моделирования случайных процессов и оценки вероятностей различных исходов в системах с квантовыми точками, использовать решение уравнений Максвелла для анализа взаимодействия света с квантовыми точками, а также провести симуляцию на основе конечных элементов для моделирования распределения электромагнитных полей вблизи квантовых точек.

Все эти методы и модели могут быть использованы для разработки и анализа методов шифрования, основанных на спектрах поглощения квантовых точек, а также для оценки их эффективности и безопасности. Однако в данной статье подробно будет рассмотрено предсказание поведения квантовых точек и их спектров поглощения с помощью решения уравнения Шредингера [2,3].

Уравнение Шредингера – это основное уравнение нерелятивистской квантовой механики, описывающее динамику частиц. Состояние классической частицы в любой момент времени описывается заданием ее координат и импульсов (x, y, z, p_x, p_y, p_z) . Зная эти величины в момент времени t , можно определить эволюцию системы под действием известных сил во все последующие моменты времени. В квантовой физике состояние системы описывается волновой функцией $\psi(x, y, z, t)$.

Предсказание поведения квантовых точек сводится к решению стационарного уравнения Шредингера.

Однако важно понимать, что, поскольку аналитическое решение уравнения Шредингера для сложных систем часто невозможно, необходимо использовать численные методы, такие как метод конечных разностей, метод конечных элементов или метод матричной диагонализации.

Решив уравнение Шредингера, можно получить энергетические уровни электронов в квантовой точке. Энергетические уровни могут быть использованы для предсказания спектров поглощения квантовых точек. Когда квантовая точка поглощает фотон, она может перейти с одного энергетического уровня на другой. Спектр поглощения будет зависеть от разности энергий между уровнями, что можно вычислить с помощью уравнения Шредингера.

Стационарное двумерное уравнение Шредингера, записанное под формулой 1, является теоретической основой для описания квантовых систем, многие из которых исследуются численными методами [4,5]

$$-\frac{\hbar^2}{2m} \left(\frac{d^2 \Psi}{dx^2} + \frac{d^2 \Psi}{dy^2} \right) + U(x, y) \cdot \Psi(x, y) = E \Psi(\vec{r}), -\infty < x < \infty, -\infty < y < \infty. \quad (1)$$

где $\hbar$ – постоянная Планка;

m – масса частицы;

$d^2 \Psi / dx^2, d^2 \Psi / dy^2$ – производные второго порядка волновой функции по координатам x, y соответственно;

$U(x, y)$ – потенциальная энергия частиц в данном пространстве пространства;

E – энергия состояния частицы;

r – радиус частицы.

В данном случае для решения уравнения будет использоваться метод конечных элементов. Этот метод можно использовать для нахождения энергетического спектра связанных состояний [3].

В подавляющем большинстве работ применяются конечные элементы, функции формы которых являются интерполяционными полиномами Лагранжа определенного порядка. При этом обеспечивается непрерывность функции численного решения, однако частные производные решения не являются непрерывными. Известен и другой тип конечных элементов, функции формы которых строятся на основе интерполяционных полиномов Эрмита [4]. Их применение приводит к непрерывности первой, а при необходимости, второй и более старших производных в численном решении.

В данном случае будет использоваться второй тип конечных элементов.

Численные решение задачи реализуется в конечной области $x_{min} < x < x_{max}, y_{min} < y < y_{max}$, размеры которой выбираются достаточно большими, чтобы не влиять на вычисляемые собственные значения, так что граничные условия принимают вид

$$\Psi(x_{min}, y) = 0; \Psi(x_{max}, y) = 0; \Psi(x, y_{min}) = 0; \Psi(x, y_{max}) = 0. \quad (2)$$

Для аппроксимации численного решения уравнения используется прямоугольные конечные элементы, функции формы которых получаются в виде произведения одномерных функций формы по каждой независимой переменной. В локальных координатах $-1 < \alpha < 1, -1 < \beta < 1$

$$\varphi_{i,j}(\alpha, \beta) = \varphi_i(\alpha) \cdot \varphi_j(\beta). \quad (3)$$

где $\varphi_{i,j}(\alpha, \beta)$ – двумерная функция;

$\varphi_i(\alpha), \varphi_j(\beta)$ – одномерные функции, зависящие от α и β соответственно.

Причем одномерные функции формы являются полиномами, коэффициенты которых обеспечивают выполнение непрерывности функции и ее производной в узлах. В одномерном случае при выборе U узлов на каждом элементе это означает, что искомую функцию можно представить в виде

$$f(\alpha) = \sum_{k=1}^U (f_k \varphi_k(\alpha) + f'_{U+k} \varphi_{U+k}(\alpha)). \quad (4)$$

где $f(\alpha)$ – аппроксимируемая функция.

f_k – коэффициент разложения функции $\varphi_k(\alpha)$

f'_{U+k} – коэффициент разложения функции $\varphi_{U+k}(\alpha)$

$\varphi_k(\alpha)$ – эрмитовы базисные функции.

$\varphi_{U+k}(\alpha)$ – дополнительные базисные функции.

При этом эрмитовы базисные функции должны удовлетворять следующим условиям интерполяции

$$\varphi_k(\alpha_l) = \delta_{kl}; \quad \frac{d\varphi_{U+k}}{d\alpha} \big|_{\alpha_l} = \delta_{kl}; \quad k, l = 1 \dots U. \quad (5)$$

где $\varphi_k(\alpha_l)$ – значение k -й базисной функции в узле α_l ;

$d\varphi_{U+k}(\alpha)/d\alpha$ – производная функции φ_{U+k} по α , взятая в точке α_l ;

δ_{kl} – символ Кронекера: $\delta_{kl} = \begin{cases} 1, & \text{если } k=l \\ 0, & \text{если } k \neq l \end{cases}$.

При этом базисные функции являются полиномами порядка $P=2U-1$.

Далее представим численное решение уравнения (1) в виде суперпозиции функций формы конечных элементов в глобальных координатах

$$\Psi(x, y) = \sum_a \Psi_a \varphi_a(x, y), \quad (6)$$

где a – глобальный номер узла в двумерной области.

Для получения системы расчетных соотношений необходимо подставить выражение (6) для искомой волновой функции в уравнение (1). После выполнения стандартного умножения на весовые (они же – базисные) функции (3) и перехода к слабой формулировке метода взвешенных невязок можно получить задачу, обобщенную на собственные значения

$$A \Psi = \varepsilon B \Psi. \quad (7)$$

При этом матрицы A, B вычисляются суммированием отдельных конечно-элементных матриц

$$A = \sum_{e=1}^E A^{(e)}; \quad B = \sum_{e=1}^E B^{(e)}. \quad (8)$$

Элементы матриц вычисляются по формулам (9) и (10).

$$A_{i,j}^{(e)} = \frac{\hbar^2}{2m} \iint_{(e)} \frac{d\varphi_i}{dx} \cdot \frac{d\varphi_j}{dx} dx dy + \frac{\hbar^2}{2m} \iint_{(e)} \frac{d\varphi_i}{dy} \cdot \frac{d\varphi_j}{dy} dx dy + \iint_{(e)} \varphi_i \varphi_j U(x, y) dx dy. \quad (9)$$

$$B_{i,j}^{(e)} = \iint_{(e)} \varphi_i \varphi_j dx dy. \quad (10)$$

Учет граничных условий реализуется присвоением узловым значениям заданных значений и исключением строк и столбцов с соответствующими номерами из разреженных матриц А и В, определяющих обобщенную задачу на собственные значения.

Решение задачи (7) позволяет получить собственные значения энергии ε_n и соответствующие собственные векторы $\Psi_a^{(n)}$, содержащие значения функции и ее частных производных в узлах прямоугольной сетки [4,5].

Заключение. Численное моделирование физических процессов является важным методом для исследования квантовых точек и их спектров. С помощью современных вычислительных методов можно понять взаимодействия между квантовыми точками и окружающей средой, что, в свою очередь, способствует оптимизации их использования в шифровании. Моделирование позволяет предсказывать поведение квантовых систем, что является важным шагом для разработки новых технологий и улучшения существующих.

Список литературы

1. Алефиренко В.М., Ефремова А.Ю., Асценко А.М. (2024) Анализ современных подходов к классификации методов шифрования. *SCIENCE TIME* (12), 45–50.
2. Зенков, А. В. Численные методы : учеб. пособие / А. В. Зенков. – Екатеринбург : Изд-во Урал. ун-та, 2016. – 124 с.
3. Стренг Г., Фикс Дж. Теория метода конечных элементов: Пер. с англ. – М.: Мир, 1977.
4. Shertzer J., Botero J. Finite-element analysis of electron-hydrogen scattering // *Phys.Rev.* 49A (1994) 3673-3679.
5. Pask J.E. Finite-element methods in electronic-structure theory // *Computer Physics Communications* 135 (2001) 1–34.

UDC 004.056.53–517.956.227

APPLICATION OF NUMERICAL MODELING METHODS FOR PREDICTING THE BEHAVIOR OF QUANTUM DOTS IN INFORMATION SECURITY SYSTEMS.

Yafremava A.Y.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Alefirenko V.M. – Cand. of Sci., associate professor, associate professor of the department of ICSD

Annotation. One of the most promising solutions for information security is encryption using quantum dots. This work explores the possibility of applying numerical modeling methods to predict the behavior of quantum dot absorption spectra. The focus is on solving the two-dimensional stationary Schrödinger equation using the finite element method with Hermite basis functions. The solution of this equation yields energy levels that allow for the prediction of absorption spectra, which is essential for optimizing quantum encryption parameters and enhancing its resistance to external influences.

Keywords: quantum encryption, quantum dots, absorption spectra, numerical modeling methods, Schrödinger equation.