Заключение

Предложенный метод встраивания полухрупких ЦВЗ показал свою работоспособность и может исследоваться далее на предмет возможности практического использования для защиты изображений в формате JPEG 2000.

Благодарности

Работа выполнена при поддержке Минобрнауки РФ в рамках гранта президента РФ МК-1907.2017.9.

Литература

1. JPEG 2000 [Электронный ресурс]. – JPEG. – Режим доступа: https://jpeg.org/jpeg2000/, свободный. – яз. англ.

2. Гонсалес, Р. Цифровая обработка изображений в среде MATLAB [Текст] / Р. Гонсалес, Р. Вудс, С. Эддинс. – М.: Техносфера, 2006. – 616с.

3. Rabbani, M. An overview of the JPEG 2000 still image compression standart [Text] / M. Rabbani, R. Joshi // Signal Processing: Image Communication. – 2004. - № 17. – 3-38 p.

4. Chen, B. Quantization index modulation: A class of provably good methods for digital watermarking and information embedding / B. Chen and G.W. Wornell // IEEE Transactions on Information Theory. – 2001. – V. 47(4). – P. 1423–1443. – DOI: 10.1109/18.923725.

5. Egiazarian, K. New full-reference quality metrics based on HVS [Text] / K. Egiazarian, J. Astola, N. Ponomarenko et al. // Proceedings of the Second International Workshop on Video Processing and Quality Metrics, Scottsdale, USA. – 2006. – 4 p.

Д.А. Бизин, С.А. Бурлов

МОДЕЛЬ КВАНТОВОГО АЛГОРИТМА ШИФРОВАНИЯ НА СОСТОЯНИЯХ ОРБИТАЛЬНОГО УГЛОВОГО МОМЕНТА ФОТОНОВ

(Самарский университет)

Орбитальный угловой момент (ОУМ) фотона – самая перспективная и исследуемая на сегодняшний момент физическая величина для передачи информации по квантовому каналу связи. В данной работе описана система шифрования на состояниях ОУМ фотонов.

В качестве измерительного прибора ОУМ рассматривается каскад интерферометров, рассмотренный в работе [1]. Каскад интерферометров формально будет не измерять состояния ОУМ фотонов, а сортировать их в зависимости от величин ОУМ по определенному модулю. В качестве алгоритма шифрования используется адаптированная схема Меркли, описанная в работе [2], использующая в качестве шифртекста смешанное состояние фотонов.

Каждый фотон имеет азимутальную фазовую зависимость вида $e^{il\varphi}$, на которую будет ориентироваться каскад интерферометров. Такие фотоны несут

ОУМ, равный $l\hbar$. При повороте пучка на угол α, фазовая зависимость принимает вид $e^{il(\varphi+\alpha)}$[1]. После поворота на угол π, пучок с четным значением l не изменится, в то время как с нечетным значением l будет отличаться по фазе на π по сравнению с не вращающимся пучком. Интерференция луча с повернутой копией себя приводит к конструктивной интерференции для четного значения l и к деструктивной интерференции для нечетного значения l. Такая концепция может быть реализована при помощи интерферометра Маха-Цендера с призмами Дове, вставленными в каждый рукав (рис. 1). Призма Дове переворачивает поперечное сечение любого проходящего пучка. Две призмы Дове, повернутые относительно друг друга на угол $\alpha/2$, поворачивают проходящий пучок на угол α.

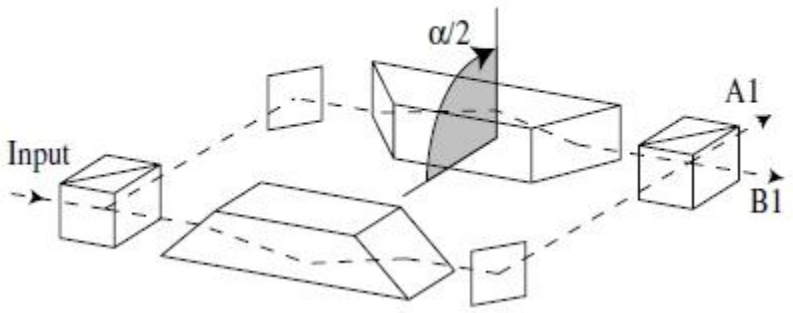

Рис. 1. Первый этап "сортировщика" ОУМ фотонов

В примере, представленном на рисунке 1, $\alpha/2 = \pi/2$, разность фаз между двумя рукавами интерферометра равна $\Delta\psi = l\pi$. Путем правильной настройки длины рукавов интерферометра можно гарантировать, что фотоны с четным значением l появляются на выходе $A1$, а фотоны с нечетным значением l появляются на выходе $B1$.

Такой принцип может быть продолжен и далее, чтобы можно было проверить сколь угодно большое число состояний ОУМ фотонов. Это можно достигнуть путем каскадирования дополнительных интерферометров Маха-Цендера с разными углами поворота (рис. 2). Первый интерферометр (первый этап) разделяет фотоны с четным и нечетным значением l на порты $A1$ и $B1$ соответственно. Фотоны с четным значением l затем проходят на второй этап, где они разделяются дальше. Угол между призмами Дове на втором этапе равен $\alpha/2 = \pi/4$, что соответствует $\Delta\psi = l\pi/2$. Поэтому пучки с $l = 4n$, где n — целое, пойдут на порт $A2$, а пучки с $l = 4n + 2$ пойдут на порт $B2$. К сожалению, угол поворота не позволяет однозначно сортировать фотоны с нечетным значением l (по модулю 4) таким же образом. Эта проблема решается путем размещения голограммы впереди одного интерферометра на втором этапе, которая увеличивает азимутальную фазу фотонов с нечетным значением l (по модулю 4) на единицу, тем самым делая значение l четным (по модулю 4). Дополнительный интерферометр с $\alpha = \pi/2$ теперь будет отделять оригинальные фотоны с нечетным значением l (по модулю 4) так же, как он отделяет фотоны с четным значением l

(по модулю 4). На рисунке 2 показаны первые три сортировочных этапа, которые позволяют определять 8 различных значений l.

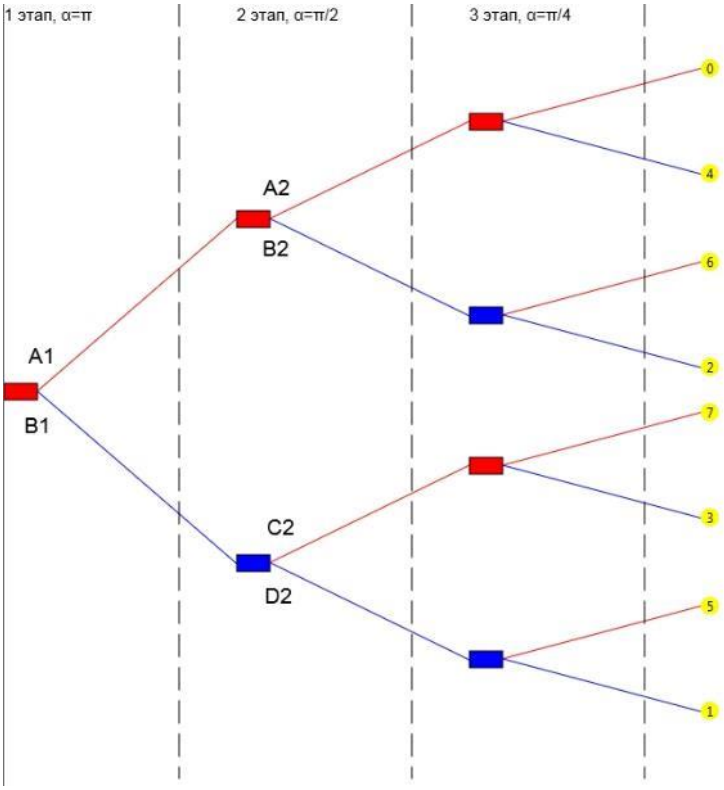

Рис. 2. Первые три этапа схемы сортировки ОУМ фотонов (перед синими интерферометрами размещены голограммы с разными значениями спиральных фазовых фронтов)

В работе [2] описана адаптированная схема шифрования Меркли-Хеллмана. Для начала нужно сгенерировать сверхвозрастающую последовательность $w_1, w_2, \dots, w_n$, удовлетворяющую условию:

$$w_{k+1} > \sum_{i=1}^{k} w_i \quad (1)$$

Затем выбираются числа q и r такие, что

$$q > \sum_{i=1}^{n} w_i \text{ и НОД}(r, q) = 1 \quad (2)$$

и строится последовательность $b_1, b_2, \dots, b_n$ по формуле:

$$b_i = r \cdot w_i \, mod(q) \quad (3)$$

Последовательность $b_1, b_2, \dots, b_n$ является открытым ключом. Открытый текст разбивается на битовые блоки, равные по длине открытому ключу.

Затем формируется лазерный пучок для каждого блока, описываемый смешанным квантовым состоянием ОУМ с матрицей плотности:

$$\rho = \begin{pmatrix} \alpha_1^2 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \alpha_n^2 \end{pmatrix} \quad (4)$$

Получается *n*-мерное гильбертово пространство с базисными векторами из (3). Коэффициенты в матрице плотности (4) рассчитываются по формуле:

$$\alpha_i = \frac{x_i}{\sqrt{\sum_{j=1}^{n} x_j}} \quad (5)$$

где $i = 1..n$; x_i— i-ый бит блока открытого текста.

Далее формируется представление смешанного состояния в виде:

$$|\psi\rangle = \sum_{i=1}^{n} \alpha_i \cdot |b_i\rangle = \sum_{i=1}^{n} \frac{x_i}{\sqrt{\sum_{j=1}^{n} x_j}} \cdot |b_i\rangle \quad (6)$$

По данному представлению генерируется лазерный пучок, который будет шифртекстом. Состояния $|b_i\rangle$ являются состояниями фотонов с ОУМ, а α_i^2 – вероятность того, что у фотонов в лазерном пучке будет ОУМ, равный $|b_i\rangle$.

Для того чтобы расшифровать блок шифртекста, необходимо собрать статистику с тех выходов каскада интерферометров, которые отвечают за состояния из (3). Затем эти состояния суммируются и получается шифртекст согласно классической схеме Меркли.

Для моделирования процесса была написана программа, которая шифрует сообщение, анимирует прохождение фотонов по каскаду интерферометров, накапливает статистику на выходах каскада и по набранной статистике расшифровывает исходное сообщение. В программе происходит разбиение сообщения на блоки, состоящие из четырех бит, генерация тысячи фотонов со смешанными состояниями и анимированное прохождение фотонов по каскаду для каждого блока сообщения. Темно-зеленый цвет на выходе каскада говорит о том, что на данном выходе вышло небольшое число фотонов, а светло-зеленый цвет показывает, что большая часть фотонов вышла на данном выходе. Также в программе моделируются случайные помехи, поэтому на все выходы каскада случайно попадают фотоны. Затем программа находит выходы, на которых фотоны окрашены в максимально светло-зеленый цвет и принимает состояния, ассоциированные с данными выходами, за передаваемые. После чего происходит расшифрование блока сообщения и вывод его в правой части окна (рис. 3).

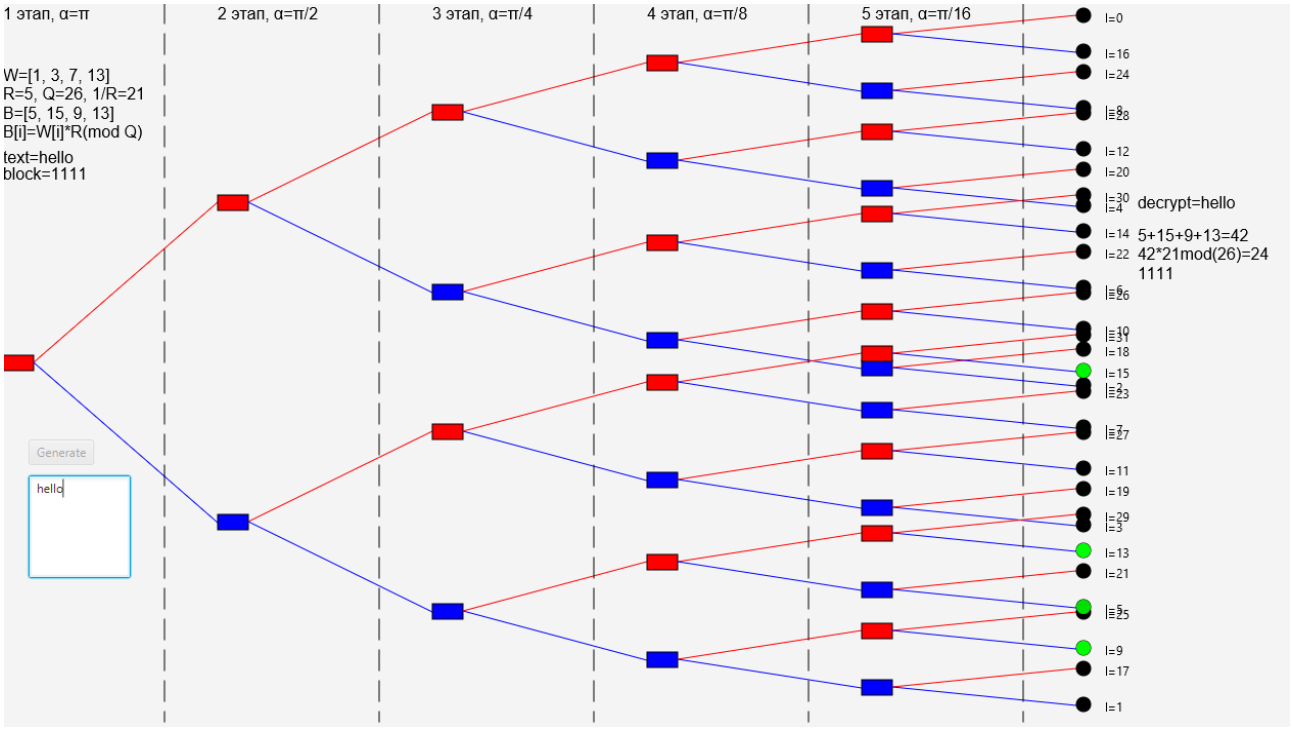

Рис. 3. Программная реализация схемы

Литература

1. Jonathan Leach, MilesJ. Padgett, Stephen M. Barnett, Sonja Franke-Arnold, and Johannes Courtial. Measuring the Orbital Angular Momentum of a Single Photon. — PHYSICAL REVIEW LETTERS, 2002, v. 88, N 25. — Яз. англ.

2. Бурлов С.А., Горохов А.В. Симметричный алгоритм шифрования с использованием "закрученного" света // Сборник трудов ИТНТ-2017, Самара: Самара: НОВАЯ ТЕХНИКА, 2017. С. 1-3.

С.А. Бурлов, Н.В. Егоров

РЕАЛИЗАЦИЯ МОДЕЛИ КВАНТОВОГО КОДИРОВАНИЯ И ДЕКОДИРОВАНИЯ НА СОСТОЯНИЯХ ОРБИТАЛЬНОГО УГЛОВОГО МОМЕНТА ФОТОНОВ

(Самарский национальный исследовательский университет
имени академика С.П. Королёва)

Введение. Для передачи квантовой информации с помощью фотонов обычно используется поляризация света. Однако очень заманчивые перспективы откроются, если для той же цели приручить другую характеристику фотонов — их «закрученность». До сих пор считалось, что передача фотонов на километровые расстояния через реальную турбулентную атмосферу сильно исказит сигнал и приведет к потере информации о закрученности. Новые и довольно простые эксперименты австрийской группы физиков под руководством Ан-