УДК 535.513.1

**С.А. Бурлов, А.В. Горохов**

Самарский национальный исследовательский университет
имени академика С.П. Королева

# О ВОЗМОЖНОСТИ ЗАЩИТЫ КВАНТОВОГО КАНАЛА СВЯЗИ НА СОСТОЯНИЯХ ОРБИТАЛЬНОГО УГЛОВОГО МОМЕНТА ФОТОНОВ

В данной работе описаны технологии и техники, предложенные на сегодняшний момент для использования в целях информационной безопасности квантовые состояния потенциально бесконечномерных квантовых систем, построенные на орбитальном угловом моменте, представляющем дополнительную степень свободы фотона.

Ключевые слова: квантовая криптография, квантовая информация, орбитальный угловой момент фотона

## Введение

На сегодняшний день идея использования «закрученного» света для быстрой и ёмкой передачи информации активно исследуется в различных областях знаний. Это и квантовая механика, как источник данного физического явления, и теория информации, и квантовая криптография, и биофотоника. Формирование отдельных квантовых состояний орбитальной составляющей представляет собой довольно трудоемкую задачу, однако уже существуют модели, позволяющие выделить описание данных состояний.

В работах [1-2] описывается возможность использования таких состояний для емкой и быстрой передачи информации. В связи с этим возникает необходимость обеспечения защищенности канала от различного рода помех, в том числе для безопасной, личной передачи информации. Вопросы квантового кодирования поднимаются в связи с принципиально новыми структурами, имеющими более двух уровней значений, а не просто 0 или 1, как в битовом случае. Параллельно криптография поднимает вопросы, о возможности использования нового квантового канала связи в рамках своей предметной области.

В данной работе приводится некоторый обзор уже сформированных техник и алгоритмов, некоторые из них реализованы на практике, некоторые существуют исключительно в теоретическом описании. Однако можно с уверен-

ностью сказать, что первые шаги в направлении формирования безопасного квантового канала «закрученного» света уже сделаны.

## 1. Квантовые состояния орбитального углового момента (ОУМ) фотона

Орбитальный угловой момент изначально был открыт для массивных частиц. До сих пор ведутся споры в научных кругах о возможности выделения конкретной орбитальной составляющей общего углового момента, поскольку фотон является безмассовой частицей. Однако исследования соотечественников [3-4] и западных ученых [5-7] показывают возможность реализации выделения данной составляющей на практике.

Световой пучок, имеющий в своей структуре фазовый множитель $e^{-il\varphi}$, несет орбитальный угловой момент [8]. Принципиально, за квантовое состояние ОУМ фотона принимают выражение, записанное в угловом базисе [9]:

$$A_l(\varphi) = \frac{1}{\sqrt{2\pi}} e^{-il\varphi}, \quad (1)$$

математической моделью измерительного прибора которого является оператор проекции в цилиндрических координатах

$$\widehat{L_z} = -i\frac{\partial}{\partial\varphi} \quad (2)$$

## 2. Квантовое кодирование

В работе [10], определяется возможность встраивания дополнительной информации для обеспечения примитивного отслеживания проверки на четность. Описанные методы имеют хорошие механизмы генерации пучка, однако возникают существенные проблемы измерения состояний. В частности, предложенная схема с добавлением внутреннего светового кольца пучка практически реализуема на данный момент лишь с графическим измерением – детектирование профиля интенсивности.

Применение уже зарекомендовавших себя алгоритмов квантового кодирования систем кубитов [11] не дает выигрыша использования систем состояний ОУМ фотонов перед теми же самыми системами кубит, поэтому здесь существует большая область для разработки специфического кодирования или адаптации уже известных алгеброгеометрических кодов, использующих многоуровневые небитовые структуры, основанные на алгебраических 70нновпах [например, см. 12].

## 3. Квантовая криптография

В работах исследователей [13-14] приводится модифицированный алгоритм квантового распределения ключа, основанный на протоколе *BB-84*. В данной схеме используется вместо двух «оригинальных» базисов поляризации, два базиса, использующие состояния ОУМ фотонов (рис. 1): множество чистых состояний ОУМ пучков и множество смешанных состояний ОУМ пучков (3):

$$|a_n\rangle = \frac{1}{\sqrt{2d+1}} \sum_{k=-d}^{d} |l = k\rangle \exp(\frac{i2\pi nk}{2d+1}), \quad (3)$$

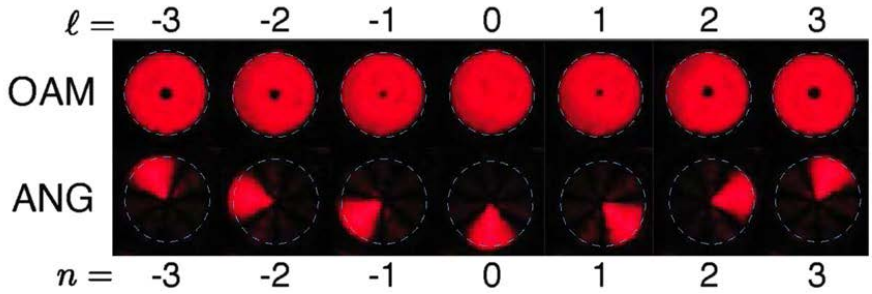


Рисунок 1 – Множества передаваемых состояний
в модифицированном протоколе *BB-84*

С квантовым шифрованием ситуация обстоит немного иначе. Шифрование – это процесс предобработки сообщений. А сообщения в начальном виде не являются квантовым состоянием.

Однако в работе [15] авторы представили алгоритм стойкого квантового шифрования, опирающегося на свойства шифра Вернама. Данная схема использует «одноразовый блокнот» для формирования наборов начальных состояний установок, генерирующих световые пучки. Утверждается, что представленный алгоритм является абсолютно стойким, и при этом длина ключа может быть сделана меньше длины сообщения, что теоретически обходит требование, поставленное Клодом Шенноном для абсолютной стойкости шифрования.

В работах [16-17] спроектированы на основе известного алгоритма Меркли (алгоритм на основе задачи «укладки рюкзака») две схемы применения квантовых состояний ОУМ фотона для квантового шифрования. Методы измерений и формирования квантовых состояний интегрированы в схемы обработки сообщений, поэтому в данном случае речь идет действительно о квантовом шифровании.

Основная идея заключается в формировании смешанного состояния, который будет аналогом суммы, которую необходимо «положить в рюкзак» и засекреченности сверхвозрастающей последовательности с коэффициентами, образующими систему.

$$\{e_1, e_2, \dots, e_k\} \xrightarrow{*w(mod\ n)} \{g_1, g_2, \dots, g_k\}, \quad (4)$$

$$S = \{b_1, b_2, \dots, b_k\}, b_i \in \{0,1\}, \quad (5)$$

$$|a\rangle = \frac{1}{\sqrt{k - |\text{кол-во 0 в } S|}} \sum_{i=1}^{k} b_i |l = g_i\rangle, \quad (6)$$

## Заключение

Несмотря на огромное количество работ по исследованию ОУМ фотона, его применению для передачи информации, применение в криптографических целях пока ограничено зарекомендовавшей себя схемой секретного распространения ключа. Практическое шифрование во многом затруднено слабо реализуемыми схемами измерений, малой разрядностью и сложностью аппаратной реализации. К тому же шифрование является для передачи информации этапом обработки, который пока выполняется на двухуровневых (битовых) структурах. С развитием квантовых вычислений, а соответственно и квантовых компьютеров, после перехода от двоичной информации к более высокоуровневым структурам физических данных, способных адаптировать генерацию, обработку и измерение в заложенном виде, квантовую криптографию ожидает принципиально новый виток развития, при котором будут ставиться нетривиальные задачи поиска принципиально новых 72нновационноческих примитивов.

## Литература

1. Bozinovic N., Yue Y., Tur M., Kristensen P., Huang H., Willner AE., Ramachandran S. Terabit-scale orbital angular momentum mode division multiplexing in fibers // Science, 2013, 340, 6140, P. 1545-1548.

2. Wang J., Yang J.Y., Fazal I.M., Ahmed N., Yan Y., Huang H., Ren Y.,Yue Y., Dolinar S., Tur M., Willner A.E. Terabit free-space data transmission employing orbital angular momentum multiplexing // Nature Photonics, 2012, 6, P. 488-296.

3. Abramochkin E., Volostnikov V. Beam transformations and nontransformed beams // Opt. Commun., 1991, 83, P. 123-135.

4. Abramochkin E.G., Volostnikov V.G. Generalized Gaussian beams // J. Opt. A, 2004, 6, P. 157-161.

5. Padgett M., Courtial J., Allen L. Light’s orbital angular momentum // Phys. Today, 2004, 57, P. 35-40.

6. Krenn M., Fickler R., Fink M., Handsteiner J., Malik M., Scheidl T., Ursin R., Zeilinger A. Communication with spatially modulated light through turbulent air across Vienna // New Journal of Physics, 2014, 16.

7. Berkhout G.C.C., Lavery M.P.J., Courtial J., Beijersbergen M.W., Padgett M.J. Efficient Sorting of Orbital Angular Momentum States of Light // Phys. Rev. Lett, 2010, 105, P. 153601-1-153601-4.

8. Allen L., Beijersbergen M.W., Spreeuw R.J.C., Woerdman J.P. Orbital angular momentum of light and the transformation of Laguerre-Gaussian laser mode // Physical Review A, 1992, 45, 11, 8185-8189.

9. Nagali E, Sciarrino F. Manipulation of photonic orbital angular momentum for quantum information processing // Advanced Photonic Sciences, 2012, 4, 1, P. 75-103.

10. Бурлов С.А. Кодирование с проверкой на четность светового пучка Лагерра-Гаусса, несущего орбитальный угловой момент //Самара: Издательство Самарского научного центра РАН, 2016. С. 416-418.

11. Прескилл Дж. Квантовая информация и квантовые вычисления // М.-Ижевск: НИЦ «Регулярная и хаотическая динамика»; Институт компьютерных исследований, 2008. С. 464.

12. Влэдуц С.Г., Ногин Д.Ю., Цфасман М.А. Алгеброгеометрические коды: основные понятия // Москва: МЦНМО, 2003. С. 504.

13. Robert W. Boyd, Anand Jha, Mehul Malik. Quantum key distribution in a high-dimensional stats space: exploiting the transverse degree of freedom of the photon // Advances in Photonics of Quantum Computing Memory and Communications, 2011, 7948, P. 79480L1-79480L6.

14. Mirhosseini M., Magana-Loaiza O.S., O`Sullivan M.N., Rodenburg B., Malik M., Lavery M.P.J., Padgett M.J., Gauthier D.J., Boyd R.W. High-dimensional quantum cryptography with twisted light // New Journal of Physics, 2015, 17, P. 033033-033043.

15. Lum D.J., Allman M.S., Gerrits T., Lupo C., Verma V.B., Lloyd S., Nam S.W., Howell J.C. A quantum enigma machine: experimentally demonstrating quantum data locking // Phisical Review A, 2016, 94, P. 022315-022324.

16. Бурлов С.А., Горохов А.В. Алгоритм симметричного шифрования с использованием «закрученного света» // (отосланы для печати)

17. Бурлов С.А. Квантовый алгоритм шифрования на состояниях орбитального углового момента фотонов // (отосланы для печати)