Алгоритм симметричного шифрования с использованием «закрученного» света

С.А. Бурлов[a], А.В. Горохов[a]

[a] *Самарский национальный исследовательский университет имени академика С.П. Королёва, 443086, Московское шоссе, 34, Самара, Россия*

Аннотация

В данной работе мы описали алгоритм применения «закрученного» света для построения схемы шифрования. За основу выбраны известные классический симметричный перестановочный шифр и асимметричный алгоритм, основанный на NP-полной проблеме «укладки рюкзака», который претерпел некоторые изменения для более тесной связи с квантовой природой носителя информации.

Ключевые слова: квантовая криптография; орбитальный угловой момент фотона; «закрученный» свет; перестановочный шифр

1. Введение

Современная криптография бурно развивается в связи с активным развитием средств хранения и передачи информации. Поиски среди алгебраических структур хороших алгоритмов приводят к уже известным задачам дискретного логарифмирования и факторизации, которые имеют большую историю криптоанализа. Иначе обстоит дело с недвоичными каналами передачи информации.

Современная квантовая физика активно развивается и предлагает новые объекты и задачи как для построения защищенных систем передачи информации, так и для анализа стойкости таковых. Однако на сегодняшний день такая криптография также пока еще завязана на «битность» передачи информации: кубиты – системы с двумя ортогональными чистыми состояниями.

В данной работе мы построили схему шифрования, основанную на известном алгоритме с открытым ключом, с применением потенциально бесконечномерного гильбертова пространства, построенного на состояниях орбитального углового момента фотонов.

2. Орбитальный угловой момент фотона

Световые пучки с азимутальной фазой, зависящей от комплексного множителя $exp(-il\varphi)$, несут орбитальный угловой момент. Угол φ – это азимутальная координата в поперечном сечении пучка, а l может принимать любое целое число, положительное или отрицательное. Значение l показывает количество переплетенных спиральных фазовых фронтов. Само значение ОУМ предполагает показатель $L = l\nabla$ на единичный фотон [1].

Многие исследования данного феномена связаны с определенным видом световых пучков, а именно моды Лагерра-Гаусса. В работах приводится измененная схема квантового распределения ключа [2,3], передача информации посредством суперпозиции состояний с ненулевым ОУМ фотонов [4]. Многие работы связаны с генерацией ОУМ пучка [5-8]. Основной сложностью на пути практического применения данного феномена служит проблема детектирования показателя ОУМ фотона и поиск среды передачи такого пучка. Были разработаны некоторые методы, позволяющие измерить величину ОУМ фотона: метод детектирования порождающей голограммой [9], сортировочный метод каскадных интерферометров [10-12], метод оптического геометрического преобразования [13-14] и другие.

В данной работе предполагается использовать метод детектирования порождающими голограммами. Схема построена таким образом, что неопределенность принимаемого пучка снижена до минимума, а отсутствие фотонов на выходе детектора также является полезной однозначной информацией для процесса.

При рассмотрении ОУМ фотона как квантового состояния получается бесконечномерное гильбертово пространство, базисом которого служит ортогональный набор чистых состояний с целым показателем ОУМ фотона $\{|l\rangle\}_{l\in Z}$. Аналогом измерительного устройства является оператор

$$\hat{L}_z = i\frac{\partial}{\partial\varphi} \tag{1}$$

Потенциально можно генерировать состояния с любой величиной ОУМ. В работе [15] показана возможность непрерывной генерации пучков с различными величинами ОУМ за счет программируемого управления генерирующими голограммами.

3. Схема шифрования

Основой алгоритма являются распределенные между абонентами сети (Анна, Борис, …) сверхвозрастающая последовательность чисел

$$A = \{a_1, a_2, ..., a_k\},\ \text{где}\ a_i > \sum_{j=1}^{i-1} a_j \tag{2}$$

и пара чисел *n* и *w* такие, чтобы *НОД(n, w) = 1* и *n* больше суммы всех элементов последовательности. Из этих значений вычисляется новая последовательность

$$T = \{t_1, t_2, ..., t_k\},\ \text{где}\ t_i = a_i \cdot w (\mathrm{mod}\ n) \tag{3}$$

По вычисленной последовательности формируется перестановочную для нее последовательность

$$T' = \{t_{j_1}, t_{j_2}, ..., t_{j_k}\},\ \text{где}\ t_{j_1} < t_{j_2} < ... < t_{j_k} \tag{4}$$

применением подстановки

$$\sigma(T) = T',\ \text{где}\ \sigma = \begin{pmatrix} 1 & 2 & ... & k \\ j_1 & j_2 & ... & j_k \end{pmatrix} \tag{5}$$

Схематично конструкция отправителя и получателя процесса шифрования представлена на рис. 1.

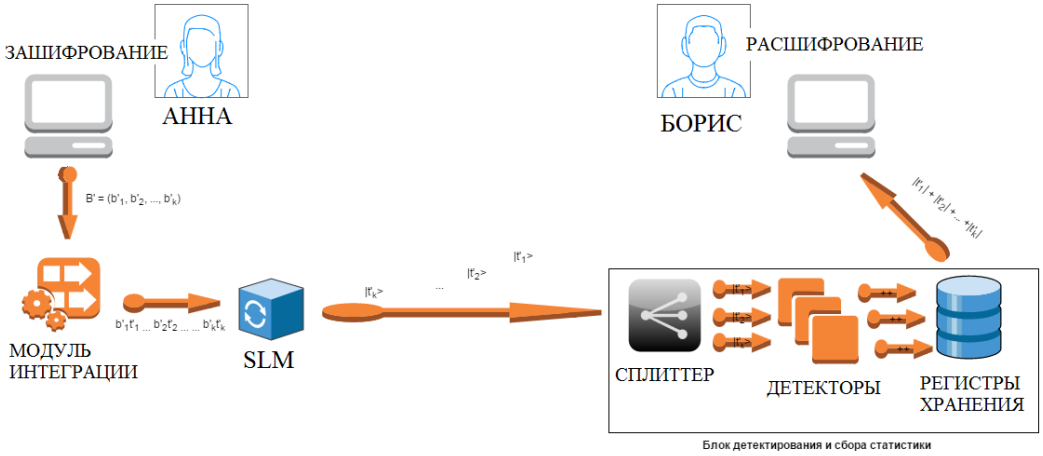

Рис. 1. Схема процесса формирования, передачи и детектирования пакетов.

Контроллер управления *SLM* (модуль интеграции) настраивается на генерацию световых пучков с проекциями ОУМ фотонов только для показателей из множества *T*. Генерация нужного пучка может быть осуществлена, к примеру, с помощью управляемых компьютером голографических дифракционных решеток [9].

Текст поданный для зашифрования переводится в битовую строку

$$B = \{b_1, b_2, ..., b_l\}, \tag{6}$$

которая делится на блоки по *k* бит

$$B_1 = \{b_1, b_2, ..., b_k\}, B_2 = \{b_{k+1}, b_{k+2}, ..., b_{2k}\}, ..., B_s = \{b_{(s-1)k+1}, b_{(s-1)k+2}, ..., b_{sk}\} \tag{7}$$

Каждый блок обрабатывается отдельно. На *i*-ом шаге выполняется следующее:

$$B'_i = \sigma(B_i) = \{b'_{i_1}, b'_{i_2}, ..., b'_{i_k}\} \tag{8}$$

Контроллер управления *SLM* до начала передачи выдает устройству генерации пучка управляющий сигнал, чтобы тот послал приемнику сигнальное состояние, нулевую гауссову моду. Приемник и передатчик должны быть синхронизованы по длительности передачи последовательности пучков итерации – υ. Модуль интеграции, получая на вход итерационную последовательность B'_i на временном промежутке $\tau = \upsilon/k$, в зависимости от 0 или 1, отправляет чистое состояние, соответствующее t'_j либо его инверсию. Набор пересылаемых за этот интервал пучков будет соответствовать итерационному блоку шифртекста.

Выход данного канала связи подключен к компоненту приемника – блоку детектирования и сбора статистики. В задачи этого блока входит детектирование получаемых состояний и учет их в соответствующих регистрах. Прием осуществляется после получения сигнального состояния, которым может быть нулевая гауссова мода, и на протяжении промежутка времени равного υ/k детектор воспринимает пучок с заранее условленным показателем ОУМ. Его «не детектирование» воспринимается как 0. Каждая итерация длится время, равное υ.

По окончании передачи пакета рассчитывается сумма показателей, которые воспринялись как 1 за время υ.

$$c''_j = \sum_{i=1}^{k} b''_i \cdot t''_i \qquad (9)$$

Далее вычисляется $d_j = c''_j \cdot w^{-1} (mod\ n)$ и получившееся число раскладывается однозначно по базису секретной сверхвозрастающей последовательности, заданной выражением (2). Таким образом получается блок открытого текста. Получив все блоки и расшифровав, получатель расшифровывает переданное сообщение.

4. Выводы

Описанная схема шифрования является симметричной в силу намеченного ранее ограничения, что для эффективного детектирования необходимо свести неопределенность для легальных абонентов касательно принимаемого сигнала к минимуму. Это можно сделать в первую очередь за счет того, что легальный абонент знает, в какой последовательности и какие физические сигналы он должен получить, а сами сообщения при этом априорно неизвестны.

Стойкость представленной схемы определяется стойкостью перестановочных соотношений, используемых для вычисления передаваемой последовательности: вероятность определения ключа 1 из *k!* вариантов, поэтому длина исходной последовательности должна быть оптимальной. Оптимальность в данном случае понимается как взвешенность между длиной шифрующей последовательности (2) и максимальным показателем ОУМ пучка, который будет детектироваться с минимальной погрешностью. Исходя из максимального «хорошо» детектируемого показателя ОУМ равного *f*, длина битовой последовательности не может превышать значения $log_2(f)$, где максимальная длина достигается у «плохой» сверхвозрастающей последовательности – стандартного двоичного разложения {1,2,4,8,16,32,…}.

Для злоумышленника получение потока без точного детектирования не дает никакой информации о передаваемом сигнале, т.к. нули в последовательности также передаются ненулевым значением ОУМ, а его отрицательный знак нужно еще выявить, на что злоумышленнику будет предоставлен очень короткий интервал времени (при этом играет немало важную роль тот факт, что носитель нельзя однозначно точно «сохранить в памяти»).

Литература

[1] Allen, L. Orbital angular momentum of light and the transformation of Lagerre-Gaussian laser modes/ L. Allen, M.W. Beijersbergen, R.J.C. Spreeuw, J.P. Woerdman// Phys. Rev. – 1992. – Vol. 45. – P. 8185-8189.

[2] Boyd Robert, W. Quantum key distribution in a high-dimensional state space: exploiting the transverse degree of freedom of the photon/ Robert W. Boyd, Anand Jha, Mehul Malik, Colin O'Sullivan, Brandon Rodenburg, Daniel J. Gauthier//Advances in Photonics of Quantum Computing, Memory, and Communication IV. – 2011. – Proc. of SPIE Vol. 7948. – P. 79480L-1 – 79480L-6. DOI:10.1117/12.873491.

[3] Mirhosseini, M. High-dimensional quantum cryptography with twisted light//M. Mirhosseini, O.S.Magana-Loaiza, M.N. O`Sullivan, B. Rodenburg, M. Malik, M.P.J. Lavery, M.J. Padgett, D.J. Gouthier, R.W. Boyd//New J. Phys. – 2015. – Vol. 17. – P. 1-11.

[4] Krenn, M. Communication with spatially modulated light through turbulent air across Vienna/M. KRenn, R. Fickler, M. Fink, J. Handsteiner, M. Malik, T. Scheidl, R. Ursin, A. Zeilinger//New Journal of Physics. – 2014. – Vol. 16. DOI:10.1088/1367-2630.

[5] Abramochkin, E. Beam transformations and nontransformed beams//E. Abramochkin, V. Volostnikov//Opt. Commun. – 1991. – Vol. 83. – P. 123-135.

[6] Beijersbergen, M. Helical-wavefront laser beams produced with a spiral phaseplate/ M. Beijersbergen, R. Coerwinkel, M. Kristensen, J. Woerdman//Optics Communications. – 1994. – Vol. 112(5-6). – P. 321–327.

[7] Yoshida, N. Nonpixellated electrically addressed spatial light modulator (SLM) combining an optically addressed SLM with a CRT/ N. Yoshida, H. Toyoda, Y. Igasaki, N. Mukohzaka, Y. Kobayashi, T. Hara//Holographic Optical Elements and Displays. – 1996. – Vol., Proc. SPIE 2885. – P. 132-136.

[8] Marrucci, L. Pancharatnam-Berry phase optical elements for wave front shaping in the visible domain: switchable helical mode generation/L. Marrucci, C. Manzo, D. Paparo// Applied Physics Letters. – 2006. – Vol. 88. DOI: 10.1063/1.2207993.

[9] Padgett, M. Light's orbital angular momentum/M. Padgett, J. Courtial, L. Allen//Phys. Today. – 2004. – Vol. 57. – P. 35-40. DOI:10.1063/1.1768672.

[10] Leach, J. Measuring the Orbital Angular Momentum of a Single Photon/ J. Leach, M.J. Padgett, S.M. Barnett, S. Franke-Arnold, J. Courtial//Phys. Rev. Lett. – 2002. – Vol. 88. – P. 257901-1-257901-4. DOI:10.1103/88.257901.

[11] Berkhout, G.C.C. Efficient Sorting of Orbital Angular Momentum States of Light/G.C.C. Berkhout, M.P.J. Lavery, J. Courtial, M.W. Beijersbergen, M.J. Padgett//Phys. Rev. Lett. – 2010. – Vol. 105. – P. 153601-1-153601-4. DOI:10.1103/105.153601.

[12] Leach, J. Interferometric methods to measure orbital and spin, or the total angular momentum of a single photon/J. Leach, J. Courtial, K. Skeldon, S.M. Barnett, S. Franke-Arnold, M.J. Padgett//Phys. Rev. Lett. – 2004. – Vol. 92. – P. 013601-1-013601-4. DOI:10.1103/92.013601.

[13] Lavery, M.P.J. Measurement of the light orbital angular momentum spectrum using an optical geometric transformation/ M.P.J. Lavery, G.C.C. Berkhout, J. Courtial and M.J. Padgett.//J. Opt. – 2011. – Vol. 13. – P. 1-4. DOI:10.1088/2040-8978/13/6/064006.

[14] Lavery, M.P.J. The efficient sorting of light's orbital angular momentum for optical communications/M.P.J. Lavery, D. Roberston, M. Malik, B. Robenburg, J. Courtial, R.W. Boyd, M.J. Padgett// Electro-Optical Remote Sensing, Photonic Technologies, and Applications VI. – 2012. – Vol. Proc. SPIE 8542. – P. 85421R-1-85421R-7. DOI:10.1117/12.979934.

[15] Arlt, J. The production of multiringed laguerre-gaussian modes by computer-generated holograms/J. Arlt, K. Dholakia,L. Allen, M.J. Padgett, M.J.//Mod. Opt. – 1998. – Vol. 45. – P. 1231-1237.

[16] Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. — М.:Триумф, 2002. – 816 с.