УДК 004.056.55

DOI: 10.18384/2310-7251-2020-2-94-101

СОЛИТОННОЕ МОДЕЛИРОВАНИЕ РАСПРЕДЕЛЕНИЯ КВАНТОВЫХ КЛЮЧЕЙ

Чан Мья Хейн, Зар Ни Аунг, Камалов Т. Ф.

Московский физико-технический институт (национальный исследовательский университет)

141700, Московская область, г. Долгопрудный, Институтский пер., д. 9, Российская Федерация

Аннотация.

Цель работы – подтвердить, что квантовая запутанность является основным инструментом коммуникации и обработки информации.

Процедура и методы исследования. Протоколы квантового распределения ключей и вопросы их защиты изучались на примере солитонной модели запутанных фотонов. Были оценены риски взлома передачи информации между легитимными пользователями. Здесь также используется простой метод генерации дихотомического сигнала, который может быть основой вероятностного моделирования квантовых состояний. Квантовые криптографические системы могут быть частично смоделированы на классическом компьютере с помощью модели запутанных солитонов, т. к. квантовая запутанность является основным инструментом коммуникации и обработки информации.

Результаты исследования. Показано, что протокол BB84 является безусловным протоколом безопасности, использующим поляризацию фотонов между удалёнными каналами. Секретные ключи используются при передаче информации между пространственно разделёнными (удалёнными) пользователями.

Теоретическая и практическая значимость. С помощью солитонного моделирования квантовых объектов удаётся имитировать их поведение и использовать некоторые их преимущества на классическом компьютере. В значительной мере это удаётся сделать при практическом использовании такого метода моделирования в области криптографии. Хорошая имитация квантово-криптографических процессов этим методом открывает перспективы применения солитонного метода для другого использования квантовой теории на практике.

Ключевые слова: квантовый компьютер, квантовая криптография, запутанные состояния

SOLITON SIMULATION OF QUANTUM KEY DISTRIBUTION

Chan Myae Hein, Zar Ni Aung, T. Kamalov

Moscow Institute of Physics and Technology (National Research University)

9 Institutskiy pereulok, Dolgoprudny 141701, Moscow Region, Russian Federation

Abstract.

Purpose is to assert that quantum entanglement is the main tool for communication and information processing.

Methodology and Approach. Quantum key distribution protocols and problems of their protection were studied with the soliton model of entangled photons. They were evaluated hacking risks transmitting information between the legitimate users. The risks of hacking information transfer between legitimate users were assessed. There is also used a simple dichotomous signal generating method. This method can be the basis of probabilistic modeling of quantum states. Quantum Cryptographic Systems can be partially simulated on a classical computer with entangled soliton model, because quantum entanglement is the main tool for communication and information processing.

Results. It is shown that the BB84 protocol is an unconditional security protocol using photon polarization between remote channels. Secret keys are used when transmitting information between spatially separated (remote) users.

Theoretical and/or Practical implications. Using soliton modeling of quantum objects, it is possible to imitate their behavior and use some of their advantages on a classical computer. To a large extent, this can be done with the practical use of such a modeling method in the field of cryptography. A good imitation of quantum cryptographic processes by this method opens up prospects for the application of the soliton method for another use of quantum theory in practice.

Keywords: quantum computer, quantum cryptography, entangled state

Введение

Актуальной проблемой функционирования квантовых компьютеров для квантовой криптографии является разработка эффективных режимов их работы. Вопросы теоретического шифрования изучались в работе [1]. Его результат был представлен в закрытом отчёте «Математическая теория криптографии». Благодаря этому исследованию появилось чёткое и строгое понимание того, какие условия должны удовлетворять применённому стабильному коду. Шифр абсолютно не может быть взломан, когда:

- 1) секрет известен только законным пользователям;
- 2) длина ключа в битах не меньше длины сообщения;
- 3) ключ случайный;
- 4) ключ используется только один раз.

В этом случае зашифрованное сообщение статистически не зависит от исходного сообщения.

Описание протокола квантовой криптографии BB84

Появление квантовой криптографии связано с публикацией в 1984 г. замечательной работы [2], в которой был предложен первый криптографический протокол BB84, который впоследствии стал классическим [3]. Квантовая криптография определяет метод безопасного общения, основанный на принципах квантовой физики. В отличие от традиционной криптографии, которая использует математические методы для обеспечения секретности информации,

квантовая криптография рассматривает случаи, когда информация передаётся с использованием принципов квантовой механики. На практике квантовая криптография использует фотоны в качестве носителя информации. Если фотоны будут перехвачены, они не достигнут пункта назначения, что сразу же сигнализирует о шпионаже. Для передачи информации по протоколу BB84 определены следующие группы:

1. Алиса посылает последовательность фотонов со случайной (0° , 45° , 90° , 135°) поляризацией.
2. Боб измеряет поляризацию фотонов, выбирая случайным образом базис «+» (0° и 90° – линейная поляризация) или «х» (45° , 135° – диагональная линейная поляризация).
3. Боб фиксирует результаты измерений, сохраняя их в тайне (одиночные фотоны могут быть совсем не приняты, потеряны или «стёрты»).
4. Затем Боб сообщает Алисе по открытому каналу, какие направления («+» или «х») он использовал для всех полученных фотонов (но не для своих результатов). Алиса сообщает Бобу, какие направления из использованных были правильными (данные, полученные из измерения в неправильных направлениях, отбрасываются).
5. Остальные данные интерпретируются в соответствии с согласованной схемой (0° и 45° , расшифрованные как «0», и 90° 135° – как «1») как двоичная последовательность (11001).

Модель с бесконечным числом битов

Моделирование Q-бита на классическом компьютере была разработана недавно в работах [4]. Исходя из этого, предлагается классическая компьютерная модель квантовых запутанных состояний. Подход основан на контролируемой корреляции или антикорреляции типа ЭПР-Боба, где неравенства Белла не нарушаются. В этих работах утверждается, что построение виртуальных квантовых состояний возможно благодаря гипотезе о природе квантовых состояний [5]. Таким образом, можно построить коррелированные квантовые объекты с учётом стохастического фона полей и волн. В результате могут быть получены решения для двух частиц, которые совершают колебания со случайной фазой. Эта фаза определяется областью когерентности [4]. Генерация нескольких дихотомических случайных сигналов с управляемым коэффициентом взаимной корреляции была реализована из одного непрерывного случайного процесса. В работе [6] случайный сигнал генерировался на его основе с помощью следующего алгоритма.

Используя найденное решение можно вычислить интегралы движения, описывающей конфигурацию солитона, то есть физические наблюдаемые: энергия W , спин S и импульс P .

Введём функцию Ψ_N [7]:

$$\Psi_N(t, z) = (\hbar N)^{-1/2} \sum_{j=1}^N \varphi_j(t, z). \quad (1)$$

Классическая наблюдаемая A_j , j – номер частицы, которая представлена как солитон-частица:

$$A_j = \int d^3x \pi_j i \hat{M}_A \phi_j = \int d^3x \phi_j^* V \phi_j, \quad (2)$$

где π_j – обобщённый импульс и ϕ_j – обобщённые координаты.

Соответствующие значения величин [7]:

$$E(A) = \frac{1}{N} \sum_{j=1}^N A_j = \frac{1}{N} \sum_{j=1}^N \int d^3x \phi_j^* \hat{M}_A \phi_j = \int d^3x \Psi_N^* \hat{A} \Psi_N + O\left(\frac{V_0}{\Delta V}\right), \quad (3)$$

где Эрмитов оператор имеет вид $\hat{A} = \hbar \hat{M}_A$.

Двухсолитонные синглетные состояния, при условии, что спин и импульс равны нулю (индексом L описывается левая поляризация, а R правая поляризация), выражаются в виде [7]:

$$\varphi^{(12)}(t, z_1, z_2) = \frac{1}{\sqrt{2}} [\varphi_L(t, -z_1) \otimes \varphi_R(t, z_2) - \varphi_R(t, -z_1) \otimes \varphi_L(t, z_2)]. \quad (4)$$

Нормировка для (4) даёт:

$$\int dz_1 \int dz_2 \varphi^{(12)*} \varphi^{(12)} = \hbar^2. \quad (5)$$

Два солитона в синглетных запутанных состояниях имеют вид:

$$\Psi_N(t, z_1, z_2) = (\hbar^2 N)^{-1/2} \sum_{j=1}^N \varphi_j^{(12)}, \quad (6)$$

где функции $\varphi_j^{(12)}$ описывают запутанные солитоны.

Если Φ_j – случайная фаза, то вероятность нахождения центра солитона равна:

$$\left| \int d^3x \varphi_j^{*(k)}(t, \vec{r}) \varphi_j^{(k)}(t, \vec{r} - \vec{d}_j^{(k)}) \right| \rightarrow \max.$$

Квантовая механика даёт для спиновой корреляционной функции хорошо известное выражение:

$$P(a, b) = -(ab). \quad (7)$$

Рассмотрим систему с секретным ключом, называемую симметричной криптосистемой. В этих системах один секретный ключ используется как для шифрования, так и для дешифрования передаваемой информации. Пусть Алиса и Боб владеют какой-то секретной информацией. Если в текущем состоянии при передаче информации ключ Еве неизвестен, то возможны следующие случаи защиты информации: 1) ключ абсолютно случайный; 2) длина ключа в битах не меньше длины сообщения; 3) ключ используется только один раз.

Асимметричная криптосистема

Система с открытым ключом называется асимметричной криптосистемой. Эти системы используют пару ключей: открытый и секретный. Для шифрова-

ния используется открытый ключ, а для дешифрования – секретный ключ. При отправлении сообщения, оно шифруется с помощью открытого ключа. При дешифровке используется секретный ключ. Существует несколько вариантов ключей:

- 1) физическое распределение;
- 2) распределение с использованием протоколов с секретным ключом;
- 3) распространение с использованием протоколов открытых ключей;
- 4) распределение квантовых ключей.

Моделирование запутанных фотонов с помощью стохастических процессов

Моделируя квантовые запутанные состояния би-фотонов, используем простой метод генерации двух дихотомных случайных сигналов с контролируемым коэффициентом корреляции. При этом реализуется один непрерывный стохастический процесс [8]. На основе генератора случайных чисел системы компьютера была построена модель стационарного случайного процесса $\Phi(t)$ с $\langle \Phi(t) \rangle = 0$, в которой определяют случайную фазу, равномерно распределённую по интервалу $0 \div 2\pi$. Из одного стохастического процесса $\Phi(t)$ можно генерировать два (или более) стохастических дихотомических сигнала с произвольной корреляцией между ними, заключёнными в интервале -1 и $+1$. Здесь одна и та же функция $\Phi(t)$ применима для нескольких наблюдателей.

Случайная фаза может использоваться для моделирования запутанных состояний путём генерации следующих K случайных дихотомических функций:

$$f_s(\theta) = \text{sign}[\cos(\Phi(t) + \theta_s)], \quad s = 1, K \quad (8)$$

с θ_s произвольными фиксированными фазами. Теперь напомним, что бифотоны могут отождествляться с вектором состояния

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle.$$

Соответствие суперпозиции двух ортогональных состояний $|0\rangle$ и $|1\rangle$ – это две поляризации фотона, горизонтальная и вертикальная. Стоит сравнить (8) со стандартной ЭПР-корреляцией, которая имеет вид:

$$E(f_1 f_2) = 1 - \frac{2}{\pi} |\Delta\theta|, \quad (9)$$

где $\Delta\theta = \theta_1 - \theta_2$. Сходство этих двух функций (8) и (9) для угловой переменной, по-видимому, является хорошей мотивацией для моделирования К-бифотонов с помощью дихотомических случайных функций. Эта очень простая модель моделирования стохастических бифотонов может быть использована для моделирования также ЭПР состояний. Мы надеемся, что эта модель будет полезна для реализации квантовых алгоритмов Шора и Гровера.

Заключение

В работе изучены протоколы распределения квантовых ключей и вопросы их защиты. Были оценены риски передачи информации между легитимными пользователями и для любых взломщиков. Показано, что протокол BB84 является безусловным протоколом безопасности, использующим поляризацию фотонов между удалёнными каналами. Секретные ключи делятся между пространственно-разделёнными (удалёнными) пользователями. Этот метод может позволить описание вероятностных квантовых состояний. Утверждается, что квантовые криптографические системы могут быть частично смоделированы на классическом компьютере с конечными степенями свободы, квантовая запутанность является основным инструментом коммуникации и обработки информации.

Статья поступила в редакцию 22.05.2020 г.

ЛИТЕРАТУРА

1. Visualization of the birth of an optical vortex using diffraction from a triangular aperture / Mourka A., Baumgartl J., Shanor C., Dholakia K., Wright E. M. // *Optics Express*. 2011. Vol. 19. Iss. 7. P. 5760–5771.
2. Dusek M., Lutkenhaus N., Hendrych M. Quantum cryptography // *Progress in Optics*. Vol. 49 / edited by E. Wolf. New York: Elsevier, 2007. P. 381–454.
3. Bennett C. H., Brassard G. Quantum cryptography: Public key distribution and coin tossing // *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (Bangalore, India, December 10–12, 1984). New York: IEEE, 1984. P. 175–179.
4. Rybakov Yu. P., Kamalov T. F. Probabilistic Simulation of Quantum Computation // *Quantum Computers and Computing*. 2006. Vol. 6. No. 1. P. 125–136.
5. Kamalov T. F. Hidden variables and the nature of Quantum Statistics // *Journal of Russian Laser Research*. 2001. Vol. 22. No. 5. P. 475–479.
6. Rybakov Yu. P., Kamalov T. F. Bell's theorem and Entangled Solitons // *International Journal of Theoretical Physics*. 2016. Vol. 55. Iss. 9. P. 4075–4080.
7. Rybakov Yu. P., Kamalov T. F. Entangled optical solitons in non-linear Kerr dielectric // *Proceedings of SPIE*. Vol. 6729. ICONO 2007: Coherent and Nonlinear Optical Phenomena (1 June 2007, Minsk, Belarus). Bellingham, WA, United States: SPIE-The International Society for Optical Engineering, 2007. P. 67291T.
8. Неравенства Белла и корреляции ЭПР-Боба: действующая классическая радиочастотная модель / Евдокимов Н. В., Клышко Д. Н., Комолов В. П., Ярочкин В. А. // *Успехи физических наук*. 1996. № 166. С. 91–107.

REFERENCES

1. Mourka A., Baumgartl J., Shanor C., Dholakia K., Wright E. M. Visualization of the birth of an optical vortex using diffraction from a triangular aperture. In: *Optics Express*, 2011, vol. 19, iss. 7, pp. 5760–5771.
2. Dusek M., Lutkenhaus N., Hendrych M. Quantum cryptography. In: Wolf E., ed. *Progress in Optics*. Vol. 49. New York, Elsevier Publ., 2007, pp. 381–454.
3. Bennett C. H., Brassard G. Quantum cryptography: Public key distribution and coin tossing. In: *Proceedings of the IEEE International Conference on Computers, Systems and*

- Signal Processing (Bangalore, India, December 10–12, 1984)*. New York, IEEE Publ., 1984, pp. 175–179.
4. Rybakov Yu. P., Kamalov T. F. Probabilistic Simulation of Quantum Computation. In: *Quantum Computers and Computing*, 2006, vol. 6, no. 1, pp. 125–136.
 5. Kamalov T. F. Hidden variables and the nature of Quantum Statistics. In: *Journal of Russian Laser Research*, 2001, vol. 22, no. 5, pp. 475–479.
 6. Rybakov Yu. P., Kamalov T. F. Bell's theorem and Entangled Solitons. In: *International Journal of Theoretical Physics*, 2016, vol. 55, iss. 9, pp. 4075–4080.
 7. Rybakov Yu. P., Kamalov T. F. Entangled optical solitons in non-linear Kerr dielectric // *Proceedings of SPIE. Vol. 6729. ICONO 2007: Coherent and Nonlinear Optical Phenomena (1 June 2007, Minsk, Belarus)*. Bellingham, WA, United States, SPIE-The International Society for Optical Engineering Publ., 2007, p. 67291T.
 8. Evdokimov N. V., Klyshko D. N., Komolov V. P., Yarochkin V. A. [Bell's inequalities and EPR-Bohm correlations: Working classical radiofrequency model]. In: *Uspekhi fizicheskikh nauk* [Physics-Uspekhi (Advances in Physical Sciences)], 1996, no. 66, pp. 91–107.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Чан Мья Хейн – аспирант кафедры теоретической физики Московского физико-технического института (национального исследовательского университета);
e-mail: chanmyaehein3@gmail.com;

Зар Ни Аунг – аспирант кафедры теоретической физики Московского физико-технического института (национального исследовательского университета);
e-mail: zarniaung52@gmail.com;

Камалов Тимур Фянович – кандидат физико-математических наук, доцент кафедры теоретической физики Московского физико-технического института (национального исследовательского университета);
e-mail: t.kamalov@phystech.edu.

INFORMATION ABOUT THE AUTHORS

Chan Myae Hein – Postgraduate Student at the Department of Theoretical Physics, Moscow Institute of Physics and Technology (National Research University);
e-mail: chanmyaehein3@gmail.com;

Zar Ni Aung – Postgraduate Student at the Department of Theoretical Physics, Moscow Institute of Physics and Technology (National Research University);
e-mail: zarniaung52@gmail.com;

Timyr. F. Kamalov – PhD in Physical and Mathematical sciences, Associate Professor at the Department of Theoretical Physics, Moscow Institute of Physics and Technology (National Research University);
e-mail: t.kamalov@phystech.edu.

ПРАВИЛЬНАЯ ССЫЛКА НА СТАТЬЮ

Чан Мья Хейн, Зар Ни Аунг, Камалов Т. Ф. Солитонное моделирование распределения квантовых ключей // Вестник Московского государственного областного университета. Серия: Физика-Математика. 2020. № 2. С. 94–101.
DOI: 10.18384/2310-7251-2020-2-94-101

FOR CITATION

Chan Myae Hein, Zar Ni Aung, Kamalov T. F. Soliton simulation of quantum key distribution. In: *Bulletin of Moscow Region State University. Series: Physics-Mathematics*, 2020, no. 2, pp. 94–101.
DOI: 10.18384/2310-7251-2020-2-94-101