БЕЗОШИБОЧНОЕ РАЗЛИЧЕНИЕ СОСТОЯНИЙ В КВАНТОВОМ РАСПРЕДЕЛЕНИИ КЛЮЧЕЙ НА ОСНОВЕ КОДИРОВАНИЯ ПО ВРЕМЕНИ

М. М. Эскандери, Д. Б. Хорошко *, С. Я. Килин

УДК 535.14

Институт физики НАН Беларуси,
220072, Минск, просп. Независимости, 68-2, Беларусь; e-mail: horoshko@dragon.bas-net.by

(Поступила 10 июля 2019)

Исследована атака безошибочного различения состояний на линию квантового распределения ключей с использованием кодирования информации по времени на основе протоколов BB84 и B92. Получены вероятности различения всех сигнальных состояний в квантовом канале связи и установлены параметры соответствующего квантового измерения.

Ключевые слова: *квантовая криптография, квантовые измерения, безошибочное различение квантовых состояний.*

We explore the attack of unambiguous state discrimination on the line of quantum key distribution utilizing time coding of the information on the basis of the protocols BB84 u B92. We obtain the probability of discriminating all signal states in the quantum communication channel and establish the parameters of the corresponding quantum measurement.

Keywords: *quantum cryptography, quantum measurements, unambiguous discrimination of quantum states.*

Введение. Создание квантовых компьютеров, способных факторизовать достаточно большие числа за полиномиальное время, сделает уязвимыми протоколы с открытым ключом, широко используемые для защиты информации в настоящее время [1]. В этом случае основным средством защищенной коммуникации должна стать квантовая криптография, основанная на фундаментальной чувствительности квантовых систем к процедуре измерения [2]. Наиболее развитым направлением квантовой криптографии является квантовое распределение ключей (КРК), обеспечивающее создание у удаленных пользователей двух случайных последовательностей, которые могут использоваться в качестве криптографических ключей в симметричных протоколах шифрования, стойких к атаке квантового компьютера. Существующие системы КРК, в том числе коммерческие, основаны на кодировании информации в состояниях оптического излучения с использованием различных степеней свободы: поляризации, частоты, времени, волнового вектора и т. д. Важная часть исследования степени защищенности систем КРК — анализ возможных атак, которые противник может осуществлять, получая доступ к квантовому каналу связи (оптическому волокну). Подобные атаки неизбежно, в силу фундаментальных ограничений квантовых измерений, приведут к появлению ошибок или потерь в передаваемых данных, однако эти ошибки и потери могут быть не замечены пользователями на фоне ошибок и потерь, всегда имеющих место в волоконно-оптической линии связи высокой (10—100 км) дальности. Моделирование атак на квантовый канал связи позволяет определить предельно допустимые значения уровней ошибок и потерь в квантовой линии связи и представляет собой актуальную физическую задачу.

В настоящей работе рассмотрена одна весьма опасная атака: с безошибочным различением состояний в квантовом канале связи [3]. Данная атака вносит потери, но не ошибки, и ее основу состав-

---

UNAMBIGUOUS STATE DISCRIMINATION IN QUANTUM KEY DISTRIBUTION ON THE BASIS OF TIME CODING

M. M. Eskandari, D. B. Horoshko *, S. Ya. Kilin (*B. I. Stepanov Institute of Physics of the National Academy of Sciences of Belarus, 68-2 Nezavisimosti Prosp., Minsk, 220072, Belarus; e-mail: horoshko@dragon.bas-net.by*)

ляет безошибочное различение состояний (БРС) квантовой системы, которое может быть проведено с некоторой вероятностью успеха. В [4] показано, что вероятность успеха равновероятного БРС задается минимальным собственным значением матрицы Грама набора различаемых состояний. Данный результат открывает возможность сравнительно простого вычисления нижнего предела потерь, при котором квантовый канал связи становится уязвимым к атаке БРС. Подобное вычисление проведено в отношении двух наиболее популярных протоколов квантовой криптографии — BB84 и B92 — при использовании кодирования информации по времени прихода оптического сигнала [5—9].

Расчет. В системе КРК с кодированием по времени посылающая сторона (Алиса) отправляет на принимающую сторону оптические импульсы, представляющие собой ослабленное до однофотонного уровня лазерное излучение и занимающие определенные временные окна в каждом такте линии связи. В протоколе B92 используются два сигнальных состояния и три окна. Первое состояние занимает первое и второе окна, второе состояние — второе и третье окна. Представим поле в окне k как гармонический осциллятор и обозначим его когерентное состояние $|\alpha\rangle_k$. Тогда два сигнальных состояния протокола B92 можно записать как

$$|\varphi_1\rangle = |\alpha\rangle_1 |\alpha\rangle_2 |0\rangle_3, \quad |\varphi_2\rangle = |0\rangle_1 |\alpha\rangle_2 |\alpha\rangle_3,$$

где $|0\rangle_k$ — вакуумное состояние в окне k (когерентное состояние с амплитудой $\alpha = 0$). В протоколе BB84 используются пять временных окон и четыре сигнальных состояния, которые могут быть записаны следующим образом:

$$|\psi_1\rangle = |\alpha\rangle_1 |\alpha\rangle_2 |0\rangle_3 |0\rangle_4 |0\rangle_5, \; |\psi_2\rangle = |0\rangle_1 |\alpha\rangle_2 |\alpha\rangle_3 |0\rangle_4 |0\rangle_5,$$
$$|\psi_3\rangle = |0\rangle_1 |0\rangle_2 |\alpha\rangle_3 |\alpha\rangle_4 |0\rangle_5, \; |\psi_4\rangle = |0\rangle_1 |0\rangle_2 |0\rangle_3 |\alpha\rangle_4 |\alpha\rangle_5.$$

Принимающая сторона (Боб) проводит в каждом такте либо измерение числа фотонов в каждом окне, либо деструктивную интерференцию полей в соседних окнах. Фаза когерентной амплитуды α случайно изменяется от такта к такту, но остается одной для всех окон такта. Защита протокола от перехвата основана на принципиальной невозможности провести одновременное точное измерение числа фотонов и фазы оптического сигнала, а значит, определить сигнальное состояние.

Однако различение сигнальных состояний может быть вероятностным, если оно проводится на основе измерения БРС для совокупности всех временных окон. Квантовое измерение, относящееся к классу БРС, используется, когда известно, что система находится в одном из N линейно независимых состояний. Это измерение имеет $N+1$ исход, из которых N соответствуют обнаружению одного из возможных состояний с условными вероятностями $\{p_i, i = 1,\ldots, N\}$, а еще один исход является неопределенным, т. е. не соответствует никакому знанию о состоянии системы. При использовании в реализации КРК квантового канала с коэффициентом пропускания по интенсивности η БРС дает противнику (Еве) возможность организовать следующую атаку. Ева заменяет квантовый канал с потерями на более совершенный, имеющий пренебрежимо малые потери. После этого в одной из точек данного канала Ева подвергает импульсы, идущие от Алисы, измерению БРС с равными условными вероятностями обнаружения всех четырех состояний $p_i = P_D$. В случае успешного обнаружения состояния импульса Ева воспроизводит данный импульс и посылает его Бобу. В случае неопределенного результата измерения Ева не посылает в данном такте ничего, внося таким образом потери. При условии равенства вероятности успешной дискриминации и пропускания канала ($P_D = \eta$) потери, вносимые Евой, совпадают с ожидаемым уровнем потерь в квантовом канале связи. В случае $P_D > \eta$ Ева вносит дополнительные потери, т. е. использует канал с пропусканием $\eta' = \eta/P_D$. Таким образом, при $P_D \geq \eta$ Ева перехватывает весь ключ и остается незамеченной. Это означает, что P_D определяет нижний предел пропускания квантового канала связи системы КРК.

Как найдено в [3], вероятность успешного равновероятного БРС дается минимальным собственным значением матрицы Грама сигнальных состояний. Для протокола BB84 матрица Грама $G_{ij} = \langle\psi_i|\psi_j\rangle$ имеет вид

$$G = \begin{pmatrix} 1 & R & R^2 & R^2 \\ R & 1 & R & R^2 \\ R^2 & R & 1 & R \\ R^2 & R^2 & R & 1 \end{pmatrix},$$

где $R = \left|\langle 0|\alpha\rangle\right|^2 = e^{-\nu}$ — вероятность обнаружить вакуум в окне, поле которого приготовлено в когерентном состоянии $|\alpha\rangle$; $\nu = |\alpha|^2$ — среднее число фотонов в одном временном окне, занимаемом импульсом света. Минимальное собственное значение матрицы G может быть найдено численно. Для протокола B92 матрица Грама имеет размерность 2 и ее минимальное собственное значение можно найти аналитически как $\lambda = 1 - \langle \psi_i | \psi_j \rangle = 1 - R$.

Квантовое измерение, реализующее БРС, задается положительной операторной мерой, состоящей из N операторов $\hat{\Pi}_k = P_D |\tilde{\psi}_k\rangle\langle\tilde{\psi}_k|$, соответствующих успешному различению состояния k, и оператора неопределенного исхода $\hat{\Pi}_0 = \hat{I} - \sum_{k=1}^{N} \hat{\Pi}_k$, где $\hat{I}$ — единичный оператор в линейной оболочке сигнальных состояний [3]. Взаимные состояния $|\tilde{\psi}_k\rangle$ связаны с сигнальными состояниями $|\psi_k\rangle$ линейным преобразованием с обратной матрицей Грама

$$\left(|\tilde{\psi}_k\rangle ... |\tilde{\psi}_N\rangle\right) = \left(|\psi_k\rangle ... |\psi_N\rangle\right) G^{-1}.$$

Для протокола B92 расчет обратной матрицы дает

$$|\tilde{\varphi}_1\rangle = \frac{|\varphi_1\rangle - R|\varphi_2\rangle}{1-R^2} = \left(u|\alpha\rangle_1 |0\rangle_3 + w|0\rangle_1 |\alpha\rangle_3\right)|\alpha\rangle_2,$$

$$|\tilde{\varphi}_2\rangle = \frac{-R|\varphi_1\rangle + |\varphi_2\rangle}{1-R^2} = \left(w|\alpha\rangle_1 |0\rangle_3 + u|0\rangle_1 |\alpha\rangle_3\right)|\alpha\rangle_2,$$

где $u = 1/(1 - R^2)$, $w = -R/(1 - R^2)$. Состояния $|\tilde{\varphi}_1\rangle$ и $|\tilde{\varphi}_2\rangle$ являются перепутанными когерентными состояниями [10, 11] окон 1 и 3 и относятся к классу состояний “кота Шредингера”. Состояния данного класса очень чувствительны к декогеренции [12, 13] и могут служить источником квантовых нестабильностей при взаимодействии с атомами [14, 15]. Квантовые измерения с положительной операторной мерой в виде проекторов на состояния “кота Шредингера” вряд ли реализуемы при современном состоянии техники оптических измерений. Однако при рассмотрении защищенности системы КРК принято предполагать, что Ева обладает всеми техническими возможностями, допускаемыми законами квантовой теории.

Результаты и их обсуждение. Вероятность равновероятного БРС как функция среднего числа фотонов в одном окне сигнального импульса приведена на рис. 1. Как указано выше, данная вероятность накладывает предел на пропускание квантового канала связи и, следовательно, на дальность линии связи. Например, значение $\nu = 0.05$, используемое в экспериментальной реализации протокола BB84 [5], соответствует пропусканию $\eta = 0.02$ или уровню потерь 17 дБ. Это означает, что максимальная дистанция линии КРК составляет 85 км при использовании стандартного телекоммуникационного волокна с потерями 0.2 дБ/км. Как видно из рис. 1, для протокола B92 вероятность БРС всегда выше, чем для протокола BB84, при том же среднем числе фотонов. В частности, использование $\nu = 0.05$ в данном протоколе ограничит максимальную дальность линии КРК дистанцией 66 км.

Для борьбы с атакой БРС могут быть использованы различные методы: увеличение числа сигнальных состояний [7, 8], использование линейно зависимого набора сигнальных состояний [9]. Следует отметить, что последний метод применим только при очень малом среднем числе фотонов, так как предложенный в [9] набор сигнальных состояний линейно зависим только в однофотонном подпространстве. Интересный метод борьбы с атакой БРС предложен недавно для реализации протокола BB84 на боковых компонентах модулированного лазерного пучка [16, 17], в котором набор состояний также представляет собой когерентные состояния нескольких мод [18]. Метод состоит в добавлении вакуумного состояния к набору сигнальных состояний, что понижает вероятность БРС [19]. Однако наиболее перспективным представляется метод состояний-ловушек [20], который, с одной стороны, значительно понижает вероятность БРС [4], а с другой — позволяет работать со сравнительно большими средними числами фотонов, а значит, с более высокими скоростями генерации ключа.

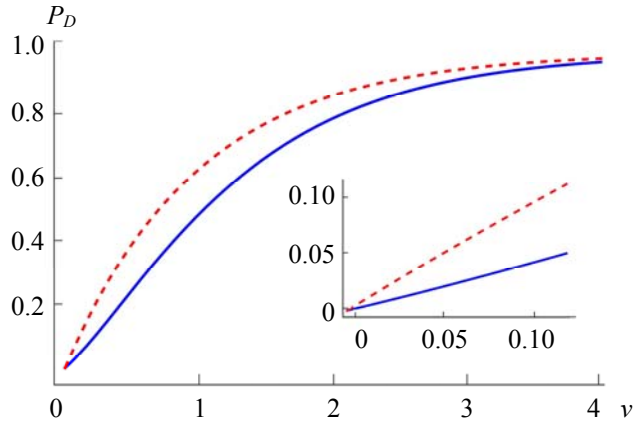

Рис. 1. Вероятность равновероятного БРС как функция среднего числа фотонов для протоколов BB84 (сплошная линия) и B92 (штриховая)

Заключение. Исследована атака безошибочного различения состояний на линию квантового распределения ключей с использованием кодирования информации по времени на основе протоколов BB84 и B92. Получены вероятности различения всех сигнальных состояний в квантовом канале связи и установлены параметры соответствующего квантового измерения. Показано, что экспериментально реализованная линия квантового распределения ключей [6] имеет ограничение дальности 85 км.

[1] **С. Я. Килин.** УФН, **169** (1999) 507
[2] Квантовая криптография: идеи и практика, под ред. С. Я. Килина, Д. Б. Хорошко, А. П. Низовцева, Беларуская навука (2007)
[3] **M. Dušek, M. Jahma, N. Lütkenhaus.** Phys. Rev. A, **62** (2000) 022306
[4] **D. B. Horoshko, M. M. Eskandari, S. Ya. Kilin.** Phys. Lett. A, **383**, N 15 (2019) 1728—1732
[5] **T. Debuisschert, W. Boucher.** Phys. Rev. A, **70** (2004) 042306
[6] **W. Boucher, T. Debuisschert.** Phys. Rev. A, **72** (2005) 062325
[7] **Д. Б. Хорошко, Д. И. Пустоход, С. Я. Килин.** Опт. и спектр., **108**, № 2 (2010) 372—379
[8] **Д. Б. Хорошко, Д. И. Пустоход, С. Я. Килин.** Опт. и спектр., **111**, № 5 (2011) 719—723
[9] **Д. Б. Хорошко, Д. И. Пустоход, С. Я. Килин.** Опт. и спектр., **112**, № 3 (2012) 373—380
[10] **B. C. Sanders.** Phys. Rev. A, **45** (1992) 6811
[11] **D. B. Horoshko, S. De Bièvre, M. I. Kolobov, G. Patera.** Phys. Rev. A, **93** (2016) 062323
[12] **D. B. Horoshko, S. Ya. Kilin.** J. Mod. Opt., **44** (1997) 2043—2047
[13] **D. B. Horoshko, S. Ya. Kilin.** Opt. Express, **2** (1998) 347—354
[14] **S. Y. Kilin, V. N. Shatokhin.** Phys. Rev. Lett., **76** (1996) 1051—1054
[15] **Д. Б. Хорошко, С. Я. Килин.** ЖЭТФ, **117** (2000) 844—852
[16] **J.-M. Mérolla, Y. Mazurenko, J.-P. Goedgebuer, W. T. Rhodes.** Phys. Rev. Lett., **82** (1999) 1656
[17] **G. P. Miroshnichenko, A. V. Kozubov, A. A. Gaidash, A. V. Gleim, D. B. Horoshko.** Opt. Express, **26** (2018) 11292—11308
[18] **D. B. Horoshko, M. M. Eskandary, S. Ya. Kilin.** J. Opt. Soc. Am. B, **35** (2018) 2744
[19] **A. Gaidash, A. Kozubov, G. Miroshnichenko.** J. Opt. Soc. Am. B, **36** (2018) B16—B19
[20] **W.-Y. Hwang.** Phys. Rev. Lett., **91** (2003) 057901