Раздел IV. Методы и средства криптографии и стеганографии

УДК 621.383

О.А. Кулиш, С.Р. Шарифуллин, Ф.Г. Хисамов

АНАЛИЗ ПРОБЛЕМ ПОСТРОЕНИЯ СИСТЕМ КВАНТОВОЙ КРИПТОГРАФИИ С ФАЗОВЫМ КОДИРОВАНИЕМ

Основой конструкции установок квантовой криптографии являются два разбалансированных интерферометра Маха-Цендера, соединенных волоконно-оптической линией связи. Для приемлемой видности интерференции на выходе такой системы оба интерферометра должны быть идентичны с точностью до единиц микрометров, а расщепители излучения на входах и выходах интерферометров должны разделять интенсивность волны в соотношении 50:50, что сложно выполнить существующими методами. Проведенный анализ показал, что данная проблема может быть решена только на базе использования интегрально-оптических технологий проектирования квантовых систем, исследованию которых посвящены следующие работы авторов.

Квантовая криптография; фазовое кодирование; видность интерференции; дрейф фазы; детектирование фотонов; оптический разделитель.

O.A. Culish, S.R. Sharifullin, F.G. Khisamov

ANALYSIS OF THE PROBLEMS OF CONSTRUCTING A QUANTUM CRYPTOGRAPHY SYSTEM WITH A PHASE CODING

The base of the construction of quantum cryptography units are two dis-balanced interferometers of Mah-Cender, connected with fiber-optic line. For acceptable visibility of interference at the quit of such a system the interferometers must be identical up to a few micrometers. Moreover, light splitters at the entrance and at the quit of the interferometers must divide the wave intensity in the ratio 50:50, it is difficult to perform the existing methods. The analysis has shown that this problem can only be solved on the basis of integrated optical design technology of quantum systems, which are devoted to the study of these authors' work.

Quantum cryptography; phase coding; visibility of the interference; phase drift; photons' detection; optical splitter.

Одним из наиболее интенсивно развивающихся направлений криптографии в настоящее время является квантовая криптография, современный этап развития которой характеризуется созданием оптических систем передачи квантовой информации. Безопасность информации, передаваемой по квантово-криптографическому каналу связи, обусловлена физическими принципами квантовой механики.

Для передачи случайной последовательности бит, которую используют в качестве ключа в симметричных криптосистемах, разработаны оптические квантово-криптографические установки с фазовой модуляцией и последующим интерферометрическим детектированием фотонов. Основой конструкции квантово-криптографических установок с фазовым кодированием являются два разбалансированных интерферометра Маха-Цендера, соединенных волоконно-оптической линией связи [1].

Рассмотрим основные требования, предъявляемые к оптическим элементам систем квантовой криптографии с фазовым кодированием. Элементы системы квантовой криптографии должны обладать малыми потерями мощности оптического излучения, так как в квантово-криптографических волоконно-оптических схемах нельзя использовать усилители. Из невозможности клонирования состояний квантовых систем следует, что использование усилителя оказывает такое же разрушающее воздействие при передаче по оптическому квантовому каналу, как и попытка перехвата сообщения [2]. Поэтому требованием к квантово-криптографическим системам является малость потерь в передающем оптическом волокне, а также использование для регистрации фотонов фотодетекторов, работающих в режиме счета единичных фотонов. Для всех существующих систем, основанных на инфракрасных фотонах и кварцевых световодах, минимальный уровень потерь оптического излучения составляет порядка 0,2 дБ/км.

Основная трудность в применении волоконно-оптической квантово-криптографической системы с фазовым кодированием состоит в необходимости добиться полной идентичности всех компонентов двух интерферометров системы, что само по себе довольно трудно реализуется на практике. Рассмотрим зависимость видности интерференции от рассогласования оптических путей в интерферометре. Для оптических монохроматических волн видность интерференционной картины всегда равна 1. Свет от реального физического источника никогда не бывает строго монохроматическим, так как даже самая узкая спектральная линия обладает конечной шириной. Кроме того, физический оптический источник имеет конечные размеры и состоит из огромного числа элементарных излучателей. Поэтому для адекватного описания интерференции рассматривают квазимонохроматический свет. То есть свет, состоящий из спектральных компонент, которые занимают частотный интервал $\Delta\nu$, малый по сравнению со средней частотой.

Для интерференции квазимонохроматического света интенсивность на выходе для максимумов и минимумов определяется по формулам [3]:

$$I_{макс} = I_1 + I_2 + 2\sqrt{I_1 I_2}\,\left|\gamma(\tau)\right|;$$

$$I_{мин} = I_1 + I_2 - 2\sqrt{I_1 I_2}\,\left|\gamma(\tau)\right|,$$

где I_1, I_2 – вклад каждого из плеч интерферометра, когда другое плечо заблокировано, $\gamma(\tau)$ – комплексная степень когерентности.

$$\gamma(\tau) = \frac{\Gamma(\tau)}{\sqrt{I_1 I_2}}, \quad 0 \le \left|\gamma(\tau)\right| \le 1,$$

где $\Gamma(\tau)$ – взаимная когерентность световых колебаний в двух точках, являющихся вторичными источниками света. Причем колебания в одной точке рассматриваются в момент времени, запаздывающий на величину τ по сравнению с моментом времени колебаний оптического излучения в другой точке. Когда обе точки совпадают, получим:

$$\Gamma(\tau) = \left\langle A^*(t)\, A(t+\tau) \right\rangle,$$

где скобки $\langle\ \rangle$ означают среднее по ансамблю. Тогда говорят об автокогерентности световых колебаний. Ансамбль функций $A(t)$ представляет собой световое возмущение.

На практике время задержки τ одного интерферирующего пучка относительно другого часто довольно мало. Если модуль τ так мал, что $\left|\left(\nu-\bar{\nu}\right)\tau\right|<<1$, то степень когерентности может быть выражена в форме:

$$\gamma(\tau)=|\gamma(\tau)|e^{i\varphi(\tau)}.$$

При этом формула интерференции может быть переписана в виде:

$$I=I_1+I_2+2\sqrt{I_1I_2}|\gamma(\tau)|\cos\varphi(\tau)\,.$$

Формула является основной формулой элементарной теории частичной когерентности оптического излучения. Она будет выполняться до тех пор, пока разность хода между интерферирующими оптическими пучками будет мала по сравнению с длиной когерентности.

По определению видности интерференции:

$$V=\frac{I_{\max}-I_{\min}}{I_{\max}+I_{\min}}.$$

Оценив минимум и максимум выражения интерференции, и подставив их в определение видности, мы получим:

$$V=2\frac{\sqrt{I_1I_2}}{I_1+I_2}|\gamma(\tau)|\,.$$

Эта формула связывает видность полос с интенсивностями двух оптических пучков и их степенью когерентности. Когда потери в волоконно-оптическом интерферометре сбалансированы, то есть равны в обоих плечах, измеренная видность равна модулю степени когерентности.

Аргумент $\varphi(\tau)$ комплексной степени когерентности может быть получен из пространственного положения максимумов интерференционной картины. Он связывается с положением максимумов интенсивности простым соотношением:

$$\frac{2\pi}{\bar{\lambda}}(s_2-s_1)-\varphi(\tau)=2m\pi\quad m=0,\pm1,\pm2,\ldots,$$

где s_1 , s_2 – оптические пути лучей.

Используя теорему Винера о спектральном разложении степени когерентности, можно получить нормализованную плотность степени когерентности:

$$\gamma(\tau)=\int_0^\infty g(\nu)e^{-i2\pi\nu\tau}d\nu\,,$$

где $g(\nu)$ – спектральная плотность.

По приведенным формулам можно найти связь между видностью интерференционной картины и временем разности хода интерферирующих оптических лучей τ. В идеальном случае видность должна быть равна 1. Расчеты показывают, что при рассогласовании плеч волоконно-оптического интерферометра порядка длины волны оптического излучения, видность падает до 50 %, что является очень низким показателем. Таким образом, в волоконно-оптических системах квантовой криптографии с фазовым кодированием оба интерферометра должны быть идентичны с точностью до долей длины волны.

В волоконно-оптических интерферометрах на четкость интерференции негативно влияет также дрейф фазы оптического излучения. Поэтому для нормальной работы оптической установки необходима активная система компенсации дрейфа фазы и подстройка фазы каждый раз перед циклом передачи ключа. Для того, чтобы количество ошибок в сыром ключе не превышало 11 % (максимально допустимое количество), ошибка в установке фазы должна быть менее 10 %.

Одной из основных проблем квантовой криптографии является то, что до сих пор невозможно создавать чистые однофотонные оптические импульсы. Обычно источником света для квантовой криптографии является просто ослабленный атенюатором луч лазера. Для такого типа света число фотонов в оптическом импульсе есть случайная величина с пуассоновским распределением. Это значит, что некоторые импульсы могут вообще не содержать фотонов, а в других может быть несколько фотонов. Из оптических импульсов с более чем одним фотоном информация может быть подслушана, а для очень слабых импульсов мало отношение сигнала к шуму. Для получения одиночных фотонов в современных волоконно-оптических системах используются импульсы лазерного излучения длительностью 30 пс, длиной волны 1,5 мкм и частотой импульсов 10 кГц.

При повышении скорости передачи данных в волоконно-оптических квантово-криптографических системах, появляются проблемы, связанные с детектированием единичных фотонов. На сегодняшний день многие квантово-криптографические системы работают на низкой частоте, так как повышение частоты ведет к повышению процента ошибок при детектировании.

Для волоконно-оптической системы квантовой криптографии с фазовым кодированием важно соотношение потерь и коэффициентов разделения оптического сигнала в разветвителях. Неидеальность разделителя и неравные потери оптического излучения в плечах интерферометра Маха-Цендера существенно влияют на видность интерференционной картины.

На рис. 1 показана система фазового кодирования на одном интерферометре с отражателями. Оптическое излучение лазера делится на два луча пластиной BS1, оба луча, пройдя через фазовые модуляторы $\varphi_А$ и $\varphi_Б$, интерферируют с помощью пластины BS2. В результате интерференции оптическое излучение поступает на детекторы D1 или D2 в зависимости от внесенной фазовыми модуляторами разности фаз. Согласно теории интерферометрии видность на детекторе D1 (рис. 1) выражается формулой [3]:

$$V_1 = 2\left(\frac{|r_1||t_2||t_A|}{|t_1||r_2||t_B|} + \frac{|t_1||r_2||t_B|}{|r_1||t_2||t_A|}\right)^{-1},$$

а на детекторе D2 формулой:

$$V_2 = 2\left(\frac{|r_1||r_2||t_A|}{|t_1||t_2||t_B|} + \frac{|t_1||t_2||t_B|}{|r_1||r_2||t_A|}\right)^{-1},$$

где r_1, r_2, t_1, t_2 – амплитудные коэффициенты отражения и пропускания разделителей луча BS_1 и BS_2. t_A, t_B – коэффициенты поглощения в плечах интерферометра.

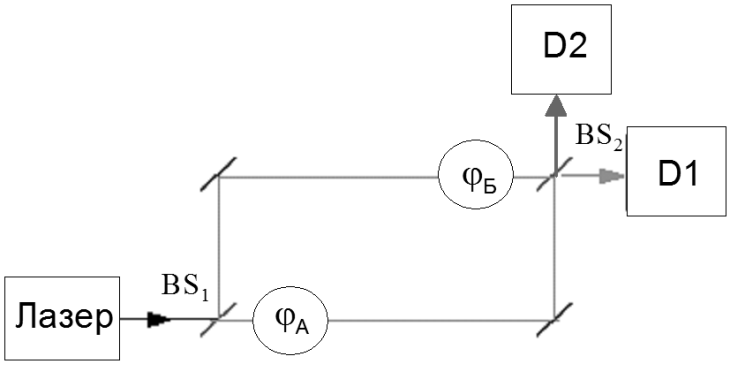

Рис. 1. Система фазового кодирования на одном интерферометре с отражателями

Видности V_1 и V_2 достигают максимума, равного 1, при условиях:

$$V_1 = 1, \text{если} \frac{|r_1||t_2||t_A|}{|t_1||r_2||t_B|} = 1$$

$$V_2 = 1, \text{если} \frac{|r_1||r_2||t_A|}{|t_1||t_2||t_B|} = 1$$

Видности V_1 и V_2 одновременно достигают единицы, когда $|r_1|^2 = |r_2|^2 = 0{,}5$. Если $|r_1|^2 = |r_2|^2 \neq 0{,}5$, то V_1 остается равной единице, а V_2 уменьшается до значения

$$V_2 = 2\left(\frac{|r_1|^2}{|t_1|^2} + \frac{|t_1|^2}{|r_1|^2}\right)^{-1}.$$

Если $|r_1|^2 = |t_2|^2$, то V_1 и V_2 меняются местами.

Из формулы для V_1 следует, что возможно достичь единичной видимости на D1 даже, когда $|r_1|^2 \neq |r_2|^2$. Это может быть достигнуто путем введения некоторых потерь оптического излучения в одном из плеч интерферометра. При этом V_2 уменьшается до значения:

$$V_2 = 2\left(\frac{|r_2|^2}{|t_2|^2} + \frac{|t_2|^2}{|r_2|^2}\right)^{-1}.$$

Делитель BS_2 в схеме на рис. 1 значительно более важен, чем делитель BS_1. Если BS_2 – идеальный делитель 50:50, то можно достичь единичной видности на обоих детекторах одновременно вне зависимости от несовершенства делителя BS_1. Условия достижения единичной видности на обоих делителях $V_1 = V_2 = 1$ имеют вид:

$$|r_2|^2 = 0{,}5 \text{ и } \frac{|r_1||t_A|}{|t_1||t_B|} = 1.$$

Если $|r_2|^2 \neq 0,5$, то единичная видность может быть достигнута только на одном из детекторов. Поэтому разделитель оптического пучка, чей коэффициент разделения близок к 50:50 должен быть использован для сведения лучей, то есть в роли BS_2. Например, если ввести потери оптического излучения на уровне 2 дБ в одно из плеч интерферометра, то видность на обоих детекторах понижается на 2,5 %. Если коэффициенты разделения BS_1 и BS_2 соотносятся как 56:44 и 53:47, то V_1 падает до 96 %, а V_2 – до 92 %. Таким образом, в системах квантовой криптографии требуется высокая точность деления мощности оптического излучения в пропорции 50:50.

Таким образом, практическая реализация схемы с фазовым кодированием на двух разбалансированных волоконно-оптических интерферометрах Маха-Цендера сталкивается с рядом серьезных проблем. Как показывают расчеты для получения четкой интерференции на выходе системы оба интерферометра должны быть идентичны с точностью до единиц микрометров. В такой системе будет возникать так же дрейф фазы, который необходимо свести к минимуму путем применения систем температурной стабилизации и компенсации набега фазы. Для приемлемой видности интерференции расщепители излучения на входах и выходах интерферометра должны разделять интенсивность волны пополам.

Решение проблем квантовой криптографии на элементной базе современной волоконной оптики является сложной задачей. Применение интегрально-оптической технологии позволяет создать оптические элементы (разветвители, интерферометры, поляризационные расщепители, фазовые модуляторы, брегговские волноводные отражатели, мультиплексоры) с требуемой точностью геометрических параметров, а также уменьшить размеры устройств, что значительно облегчает и упрощает их термостабилизацию. Хотя в интегрально-оптических волноводах потери излучения выше, чем в волокне, благодаря малым размерам интегрально-оптических устройств их применение в системах квантовой криптографии не требует значительного уменьшения длины квантовой линии связи. Кроме того, интегрально-оптические схемы с применением периодически поляризованного ниобата лития позволяют создать источники единичных фотонов и пар фотонов в перепутанных состояниях. Различные протоколы квантовой криптографии требуют построения сложных схем обработки сигналов, что также удобно реализовать на основе единой интегральной схемы. Поэтому дальнейшие исследования авторов посвящены разработке методов квантовой криптографии с применением интегрально-оптических технологий и синтезу математических моделей для оптимального их проектирования.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Баумеистер Д., Экерт А., Цайлингер А.* Физика квантовой информации. – М.: Постмаркет. – 2003. – 253 с.
2. *Bennett C., Bessette F., Brassard G., Salvail L., Smolin J.* Experimental Quantum Cryptography // J. of Cryptology. – 1992. – № 5 – P. 356-353.
3. *Tittel W., Brendel J., Gisin B., Herzog T., Zbinden H., Gisin N.* Experimental demonstration of quantum correlations over more than 10 km // Phys. Rev. A. – 1998. – Vol. 57. – P. 3229-3232.

Статью рекомендовал к опубликованию д.т.н. профессор О. Акаткин.

Кулиш Ольга Александровна – Филиал Военной академии связи г. Краснодар; e-mail: culish_olga@mail.ru; 350035, г. Краснодар, ул. Красина, 4; тел.: 89615213577; кафедра криптографических средств защиты информации и математических основ криптологии; старший преподаватель; к.ф.-м.н.; доцент.

Шарифуллин Сергей Равильевич – e-mail: SharifullinSR@mail.ru; тел.: 89054726222; кафедра криптографических средств защиты информации и математических основ криптологии; начальник; к.т.н.; доцент.

Хисамов Франгиз Гильфанетдинович – e-mail: kiiz@rambler.ru; тел.: 88612523031; кафедра специальной связи; д.т.н.; профессор.

Culish Olga Aleksandrovna – Branch of the Military Academy of Communications, Krasnodar; e-mail: culish_olga@mail.ru; 4, Krasin street, Krasnodar, 350035, Russia; phone: +79615213577; the department of cryptographic systems for information protection and mathematical foundations of cryptology; senior lecturer; cand. of phis.-math. sc; associate professor.

Sharifullin Sergey Raviljevich – e-mail: SharifullinSR@mail.ru; phone: +79054726222; the department of cryptographic systems for information protection and mathematical foundations of cryptology; cand. of eng. sc; associate professor.

Khisamov Frangiz Gilfanetdinovich – e-mail: kiiz@rambler.ru; phone: +78612523031; the department of special communications; dr. of eng. sc.; professor.

УДК 681.03.245

Л.К. Бабенко, Е.А. Ищукова

АНАЛИЗ СИММЕТРИЧНЫХ КРИПТОСИСТЕМ*

Рассматриваются основные аспекты применения современных методов криптоанализа для оценки стойкости симметричных блочных алгоритмов шифрования. В том числе, рассмотрены такие методы анализа как линейный, дифференциальный, алгебраический анализы, слайдовая атака. Также рассмотрены различные подходы к анализу стандарта AES. Дано определение Парадоксу дней рождений и объяснена его роль в решении задач защиты информации. При рассмотрении подходов к анализу современных симметричных криптосистем отдельное внимание уделено вопросам возможности применения распределенных многопроцессорных вычислений с целью сокращения времени анализа.

Криптография; крипроанализ; симметричное шифрование; секретный ключ; блочный шифр; стойкость; распределенные многопроцессорные вычисления.

L.K. Babenko, E.A. Ischukova

ANALYSIS OF SIMMETRIC CRYPTOSYSTEMS

Article considers the main aspects of application of modern methods of cryptanalysis for an assessment of strength of symmetric block algorithms of enciphering. Considering include such methods of the analysis as linear, differential, algebraic analyses and slide attack. The different variants of analysis of AES are considered. It is described what the Birthday Paradox is and what is its role in the information security. The special attention is given to questions of possibility of using of the distributed multiprocessing calculations for reduction of time of the analysis.

Cryptography; cryptanalysis; symmetric cipher; secret key; block cipher; strength; multiprocessing calculations.

Современные алгоритмы шифрования разрабатываются таким образом, чтобы аналитик имел как можно меньше шансов отыскать секретный ключ, с помощью которого были зашифрованы данные, даже если ему известен сам алгоритм шифрования и есть в наличие несколько текстов и соответствующих им шифртекстов. Приступая к задаче анализа, первым делом аналитик определяет тот набор данных, который ему изначально известен для анализа. От этого зависит тот тип

* Работа поддержана грантами РФФИ: № 12-07-00037-а, №12-07-31120-мол_а.