На правах рукописи

Курочкин Юрий Владимирович

МЕТОДЫ ПОВЫШЕНИЯ ПРОПУСКНОЙ СПОСОБНОСТИ КВАНТОВОЙ КРИПТОГРАФИИ

01.04.21 – лазерная физика

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата физико-математических наук

Новосибирск − 2011

Работа выполнена в Московском Физико-Техническом Институте (государственном университете)

Научный руководитель:	академик Багаев Сергей Николаевич
Официальные оппоненты:	д. ф. м. н. Задков Виктор Николаевич
	д. ф. м. н. Орлов Валерий Александрович
Ведущая организация:	Учреждение Российской академии наук Физический институт им. П. Н. Лебедева РАН (г. Москва)

Защита состоится «___»_____ 2012 г. в ___ часов на заседании диссертационного совета Д 003.024.01 при Институте лазерной физики СО РАН по адресу: 630090, г. Новосибирск, просп. Ак. Лаврентьева,13/3

С диссертацией можно ознакомиться в библиотеке Института лазерной физики СО РАН.

Автореферат разослан «____» _____ 2012 г.

Учёный секретарь диссертационного совета,
кандидат физико-математических наук Н. Г. Никулин

1. Общая характеристика работы

1.1. Актуальность темы

Развитие фундаментальных идей квантовой информатики, возникшей на стыке квантовой механики и теории информации, положили начало исследований по созданию квантовых компьютеров и квантовых линий связи. Наиболее экспериментально развитая область квантовой информатики – квантовая криптография - позволяет реализовать абсолютно секретную передачу данных. В качестве физического носителя информации в ней используются квантовые состояния отдельных частиц – фотонов. Основополагающими принципами защиты данных в квантовых линиях связи являются невозможность копирования заранее неизвестного состояния отдельного квантового объекта и невозможность получения любой информации о квантовых состояниях этого объекта без их возмущения. Таким образом, гарантией защиты передаваемой информации выступают фундаментальные законы квантовой механики. Многими экспертами квантовая криптография рассматривается как единственный метод, способный обеспечить реальную защиту системам коммуникаций, как на данный момент, так и в обозримом будущем. Идеи и перспективы этого направления исследований оказались настолько привлекательными, что многие исследовательские группы сразу же начали активную работу по созданию реально работающих установок и устройств. На данный момент проблемы создания квантовых систем связи являются актуальными, и эта область динамично развивается.

Эксперименты выявили ряд основных проблем, стоящих перед квантовыми криптографическими системами, такие как задача детектирования единичных фотонов с высокой вероятностью в заданном квантовом состоянии при низком уровне ложных срабатываний, отсутствие управляемых источников одиночных фотонов, проблема увеличения дальности передачи и малая скорость генерации квантового ключа. Проведение теоретических и экспериментальных исследований по поиску решения этих задач представляет большой научный интерес и послужит мощным средством обеспечения информационной безопасности.

Для увеличения дальности и скорости передачи необходим поиск новых теоретических подходов модификаций протоколов квантовой криптографии, позволяющих эффективнее использовать ослабленные лазерные импульсы в качестве источников квантовых состояний и снижать ограничение на соотношение сигнал/шум.

1.2.Цели диссертации

Целью диссертации являлась теоретическая разработка и экспериментальная демонстрация новых методов увеличения скорости генерации квантового ключа на основе протоколов с увеличенным и бесконечным количеством состояний. Также выполнялась задача создания высокоскоростной оптоволоконной установки для квантовой криптографии, включающая исследование параметров детекторов одиночных фотонов.

1.3.Научная новизна диссертации

Научная новизна полученных результатов заключается во впервые использованном подходе отказа от фиксированного набора базисов и переход к произвольному положению базисов в пространстве состояний кубит без падения скорости передачи до нуля. По сравнению с другими работами данный подход имеет принципиальное отличие в способе обеспечения секретности. Данный протокол не чувствителен к количеству ошибок, вносимых детектором одиночных фотонов, что снимает ряд фундаментальных ограничений по сравнению с ранее существовавшими протоколами квантовой криптографии.

Впервые для протоколов с конечным количеством базисов более двух теоретически рассчитан и экспериментально продемонстрирован эффект от анализа информации, отброшенной в процессе сверки базисов. Данный результат позволяет увеличивать объем передаваемой информации за счет дополнительных данных, позволяющих делать выводы о вмешательстве перехватчика.

Была создана установка для квантовой криптографии, работающая на автокомпенсационной оптической схеме. Созданы оригинальные детекторы одиночных фотонов, демонстрирующие характеристики по квантовой эффективности и шумам на уровне лучших мировых аналогов.

Практическая значимость полученных результатов заключается в разработке и демонстрации метода, позволяющего снять ряд принципиальных ограничений квантовой криптографии. В результате становится возможным достигать большей дальности передачи и скорости генерации ключа. Созданная экспериментальная установка на основе автокомпенсационной схемы является прототипом коммерческого устройства по распределению квантового ключа (безусловной защите передаваемых данных).

Все результаты, вошедшие в диссертацию, получены при личном определяющем участии автора в разработке методов решения поставленных задач, подготовке и проведении экспериментов.

1.4. Положения, выносимые на защиту

1. Предложен протокол квантовой криптографии, впервые использующий информацию, исключаемую при процедуре сверки базисов в протоколах квантовой криптографии с увеличенным количеством базисов, что позволяет повышать точность определения вероятного перехвата и, как следствие, повышать объем передаваемого секретного ключа на объем, раскрываемый для определения уровня ошибок.
2. Выполнена экспериментальная демонстрация протокола, использующего информацию, исключаемую при сверке базисов. Поставлен эксперимент по перехвату данных в квантовом канале, что позволило в экспериментально подтвердить теоретические выводы о вносимых возмущениях в результате перехвата.
3. Разработан протокол квантовой криптографии без фиксированных положений базиса, позволяющий преодолеть ряд принципиальных ограничений дальности передачи квантового ключа. Предложенный подход отказа от фиксированного набора базисов в пользу произвольного положения базиса в пространстве состояний кубит снимает зависимость объема перехваченной информации от соотношения сигнал/шум, что позволяет увеличивать предельную дальность и скорость генерации секретного ключа.
4. Впервые в России создана оптоволоконная установка для квантовой криптографии, получена передача секретного квантового ключа на расстояние 25 км. со скоростью 700 бит/сек.
5. Экспериментально продемонстрирована возможность практического применения протокола квантовой криптографии без фиксированных положений базиса.

1.5. Апробация работы и публикации

Основные результаты по теме диссертации докладывались и обсуждались на научных школах и международных конференциях, в том числе International Symposium on Modern Problem of Laser Physics (Novosibirsk 2004, 2008), ERATO Conference on Quantum Information Science (Tokyo, Japan, 2004), Asian Conference on Quantum Information Science (Beijing, China, 2006), International symposium “Quantum informatics” (Moscow, 2004, 2005),

International conference on quantum optics (Minsk, Belarus, 2006), Международной конференции студентов, аспирантов и молодых ученых «Ломоносов» (Москва, 2006,2007, 2009), Internationa Conference for Wave Electronics and Its Applications in the Information and Telecommunication Systems (St. Petersburg, 2007), International Workshop «Quantum Physics and Communication" (Dubna, 2007), Third Russian-French Laser Physics Workshop.(St. Petersburg, 2008), International Conference Mathematical Modeling and Computational Physics (Dubna, 2009), Second Nanotechnology International Forum (Moscow, 2009), XII международной школе-семинаре по люминесценции и лазерной физике. (Иркутск, 2010), 11 international conference Micro/Nanotechnologies EDM2010 (Erlagol, Russia, 2010), International Conference on Quantum Technologies (Moscow, 2011), Российской конференции по актуальным проблемам полупроводниковой нанофотоэлектроники «ФОТОНИКА 2011» (Новосибирск, 2011)..

По материалам диссертации опубликовано 27 научных работ, в том числе 7 статей, включающих 4 статьи в рецензируемых журналах и 3 статьи в трудах международных конференции.

1.6.Структура и объем диссертации.

Диссертация состоит из введения, двух глав и заключения. Ее объем составляет 113 страниц, включая 36 рисунков и 14 таблиц. Список цитируемой литературы состоит из 112 наименований.

1. Содержание работы

Во введении приводятся основные положения квантовой криптографии совместно с обоснованием актуальности диссертации. Проанализировано современное состояние квантовой криптографии, сформулированы цель и научная новизна работы, изложены основные положения, выносимые на защиту.

Во второй главе диссертации рассматривается новый протокол квантовой криптографии, впервые использующий информацию, исключаемую при процедуре сверки базисов в протоколах квантовой криптографии с увеличенным количеством базисов, что позволяет повышать точность определения вероятного перехвата и, как следствие, повышать объем передаваемого секретного ключа на объем, раскрываемый для определения уровня ошибок. Так же представлен протокол квантовой криптографии без фиксированных положений базиса, позволяющий преодолеть ряд принципиальных ограничений дальности передачи квантового ключа.

Протокол с увеличенным количеством базисов:

Одной из задач в квантовой криптографии является разработка протоколов, позволяющих при современном экспериментальном уровне источников одиночных фотонов и детекторов увеличивать предельную дальность передачи ключа. Исходя из этого, был разработан новый протокол квантовой криптографии, более эффективно использующий принцип запрета клонирования квантовых состояний. Данный протокол снижает объем теоретически возможной для перехвата информации за счет увеличения количества базисов. При увеличении количества базисов до трех без увеличения размерности пространства состояний кубитов, базисы располагаются под углами 0°, 30° и 60° соответственно. Алиса (передатчик) случайным образом выбирает один из трех базисов и квантовое состояние передаваемого бита. Боб (приемник) случайно выбирает базис измерения и производит измерение переданного кубита. С вероятностью $\frac{1}{3}$ базисы Алиса и Боба совпадут. После объявления по публичному каналу связи в конечный ключ включаются только те события, в которых базисы совпали.

Увеличение количества базисов ведет к повышению секретности за счет уменьшения взаимной информации I_{AE} и повышения количества вносимых перехватчиком (Евой) ошибок.

$$I(\alpha,\varepsilon)=\frac{1}{n}\sum_{i=0}^{n-1} I\left(\alpha,\varepsilon\middle|\Delta=\frac{i}{2n}\pi\right) \qquad (1)$$

$$I\left(\alpha,\varepsilon\middle|\Delta=\frac{i}{2n}\pi\right)=1+\cos^2\left(\frac{i}{2n}\pi\right)\log_2\left[\cos^2\left(\frac{i}{2n}\pi\right)\right]+\sin^2\left(\frac{i}{2n}\pi\right)\log_2\left[\sin^2\left(\frac{i}{2n}\pi\right)\right]$$

Где n – число базисов, $\cos^2\left(\frac{i}{2n}\pi\right)$ и $\sin^2\left(\frac{i}{2n}\pi\right)$ – вероятности измерить 1 и 0 в базисах повернутых относительно базиса Алисы.

Таблица 1. Результаты вычисления информации прямого перехвата Евы при увеличении числа базисов.

Число базисов	**Информация, перехватчика I_E, бит**
2	0.500
3	0.459
4	0.450
6	0.445

При переходе от 2х базисов к 3-6 объем перехваченной информации снижается приблизительно на 10% (Таблица 1). Таким образом, данный протокол дает дополнительный метод обнаружения

возможного перехвата данных в квантовом канале за счет анализа исключенной из ключа информации при объявлении базисов, что является впервые использованной методикой.

Впервые предложено анализировать дополнительную информацию, объявив приготовленное состояние и результат измерения для не совпавших базисов. В других протоколах информация о событиях с не совпавшими базисами исключается из анализа о квантовом ключе.

В случае не совпадения базисов информация об отдельном событии не даст ни какого конструктивного результата. В данном протоколе после объявления всех данных о не совпавших базисах так же объявляются значения приготовленных и измеренных битов. По полученным результатам статистически восстанавливается угол между базисами с одинаковой разностью положений и анализируется отличие от фактического угла. Наличие перехватчика вносит искажения в результаты измерений разности угловых положений базисов. Анализируя полученную информацию, Боб восстанавливает эффективный угол между его базисом и базисом, в котором был отправлен фотон.

$$\Delta_{Effective} = \arctan\left(\sqrt{\frac{P(Alice\_bit \neq Bob\_bit)}{P(Alice\_bit = Bob\_bit)}}\right) \quad (2)$$

По разности восстановленного угла с фактическим $\Delta_{Effective} - \Delta_{Real}$ рассчитывается эффективный квантовый уровень ошибок.

$$QBER_{Effective} = \sin^2\left(\Delta_{Effective} - \Delta_{Real}\right) \quad (3)$$

Для того, чтобы определить уровень ошибок QBER в качестве входных данных для процедуры повышения секретности необходимо открыть статистически значимое количество бит секретного ключа, что уменьшает скорость генерации квантового ключа. Анализ результатов измерений в не совпавших базисах позволяет уменьшить долю раскрываемого ключа при процедуре определения уровня ошибок.

Протокол с увеличенным числом базисов обладает повышенной устойчивостью к атакам разделения фотонов без квантовой памяти. Так как количество базисов увеличено, снижается вероятность совпадения базиса, использованного для измерения перехваченного фотона, и базиса передаваемого фотона обратно пропорционально числу базисов. Протокол может быть исключительно полезным в тех случаях, когда ввиду шумов детекторов и потерь в квантовом канале протокол, например BB84, находится на грани критического уровня ошибок в квантовом ключе и требуется дополнительная информация о возможности соблюдения условий безопасной передачи.

Теоретические выводы были экспериментально подтверждены на модифицированной установке квантовой криптографии с воздушным каналом связи. Также была проведена

демонстрация перехвата одиночных фотонов Евой методом измерения их квантового состояния и повторной пересылки фотонов от Евы к Бобу. Полученные экспериментальные результаты показывают повышение эффективности выявления перехвата ключа при увеличении количества базисов и рассмотрении отброшенной информации.

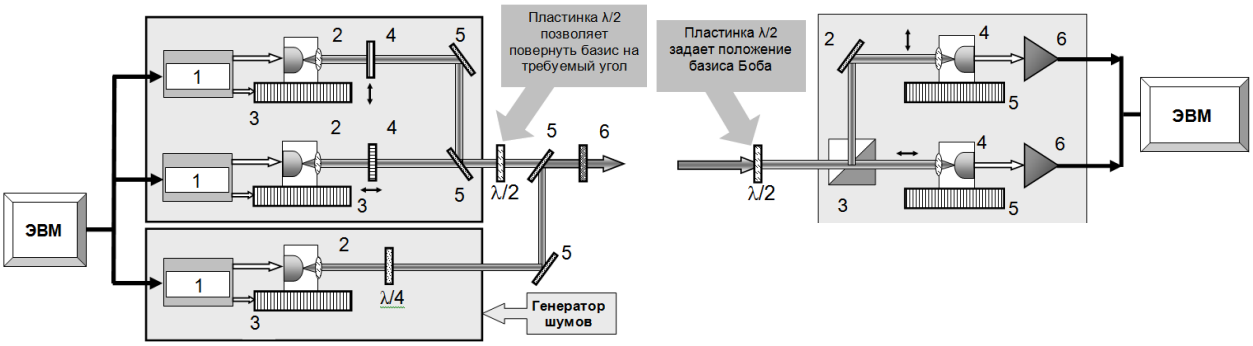

Рис. 1. Экспериментальная установка для демонстрации протокола с увеличенным количеством базисов. В установке **Алисы (слева)** для передачи фотонов использовались два лазера, которые формировали один базис. Положение этого базиса задавалось полуволновой пластинкой. Лазер с круговой поляризацией устанавливает необходимый уровень шумов. 1 – источник питания полупроводникового лазера. 2 – полупроводниковый лазер. 3 – микрохолодильник на основе элемента Пельтье. 4 – поляризатор (призма Глана). 5 – зеркало. 6 – поглощающий фильтр. λ/2 – полуволновая пластинка. λ/4 – четвертьволновая пластинка. На стороне **Боба (справа)** использовались два детектора одиночных фотонов, которые образовывали один базис. Положение базиса могло меняться на необходимый угол при помощи полуволновой пластинки. λ/2 – полуволновая пластинка. 2 – зеркало. 3 – поляризатор (призма Глана). 4 – лавинный фотодиод с собирающей линзой. 5 - микрохолодильник на основе элемента Пельтье. 6 – усилитель.

Эксперименты были проведены для случая с 3, 4 и 6 базисами. В данном эксперименте впервые в мире было продемонстрирована возможность эффективного использования отброшенных событий для выявления нелегитимного пользователя в квантовой линии.

Для этого была модифицирована существующая установка для квантовой криптографии (Рис. 1). В оптическую систему передающего узла была добавлена пластинка λ/2, которая поворачивала передаваемое состояние на определенный угол. Таким образом, поворачивая пластину можно получить базис, повернутый на произвольный угол. Для измерений при различных уровнях шумов использовались импульсы с круговой поляризацией, которые равномерно поступали на все детекторы, что эквивалентно собственным шумам квантовой линии.

Далее была проведена экспериментальная демонстрация перехвата одиночных фотонов Евой методом измерения их квантового состояния и повторной пересылки фотонов от Евы к Бобу. В данном случае процесс передачи ключа разбивался на два этапа. На первом этапе принимающая часть установка исполняла роль приемного узла

перехватчика и проводила измерение. На втором этапе передающая часть установки исполняла роль передатчика Евы (перехватчика), в то время, как принимающая часть установки исполняла свою обычную роль. Таким образом экспериментально осуществлен случай прямого перехвата данных в квантовом канале связи. Измерялись вносимые статистические отклонения в углы между базисами отброшенных событий. Данный подход показал практическую применимость и целесообразность новой идеи анализа не использовавшейся ранее информации о не совпавших базисах Алисы и Боба. На основании отклонения измеренного угла от фактического, рассчитывался эквивалентный уровень квантового шума $QBER_{Effective}$ (3) в результате перехвата, уровень которого является критерием степени вмешательства перехватчика. Эксперимент показал простоту практической реализации протокола с количеством базисов более 2х. В таблице 2 представлены результаты измерений эквивалентных уровней шумов $QBER_{Effective}$ в результате присутствия перехватчика, что в зависимости от затухания в квантовом канале может увеличивать скорость генерации ключа до 2х раз.

Таблица 2. Эквивалентный уровень квантового шума $QBER_{Effective}$, соответствующий результатам измерения восстановленной разницы положения базиса и восстановленного угла $\Delta_{Effective} - \Delta_{Real}$.

Количество базисов и разность положений базисов Алисы и Боба	**< 1% шумов**	**5% шумов**	**9% шумов**	**13% шумов**
3 базиса, 30°	2%	2%	3%	3%
3 базиса, 60°	2%	2%	2%	3%
4 базиса, 22.5°	5%	5%	6%	6%
4 базиса, 45°	0%	0%	0%	0%
4 базиса, 67.5°	4%	5%	6%	6%
6 базиса, 15°	10%	11%	12%	13%
6 базиса, 30°	2%	2%	3%	3%
6 базиса, 45°	0%	0%	0%	0%
6 базиса, 60°	2%	2%	2%	3%
6 базиса, 75°	10%	10%	12%	12%

Протокол с плавающим базисом:

Как продолжение идеи увеличения количества базисов был разработан авторский метод распределения квантового ключа (протокол с плавающим базисом) в котором базис

может занимать произвольное положение в пространстве состояний кубитов. Этот протокол является синтезом идей снижения информации, получаемой перехватчиком за счет увеличения количества базисов и необходимости совпадения базисов для предотвращения падения скорости генерации ключа по причине увеличения количества базисов. Расчет показал увеличение предельной дальности передачи без нарушения условий секретности распределяемого ключа и увеличение скорости генерации ключа на всех расстояниях по сравнению со всеми ранее предложенными протоколами.

В предлагаемом методе происходит полный отказ от фиксированных положений базисов для случая одномерного Гильбертова пространства. Это производится за счет того, что секретная информация для авторизации классического канала используется для определения секретного положения каждого базиса посредством математической псевдослучайной функции с высокой степенью равномерности. Алиса и Боб, имея некоторый объем общей секретной информации (вспомогательный ключ) применяют к ней псевдослучайную функцию $\varphi(K,i)$, определяющую последовательность сдвигов исходного положения базисов (Рис. 2) в процессе передачи, где K – вспомогательный ключ, i – порядковый номер кубита в передаче. Последовательность положений базисов значительно изменяется при изменении любого бита входных данных, а именно вспомогательного ключа, что позволяет говорить о секретности положений базиса даже при частичном раскрытии вспомогательного ключа.

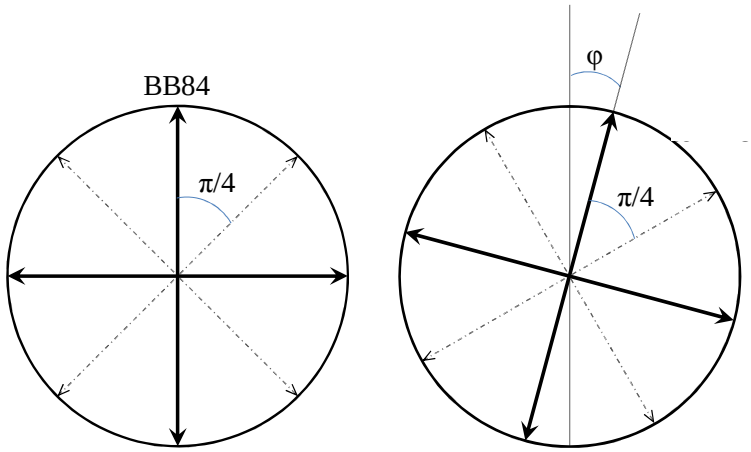

Рис. 2. Протокол с плавающим базисом. Кодирование кубит ослабленными лазерными импульсами получается из протокола BB84 добавлением секретного поворота $\varphi(K,i)$, индивидуального для каждого кубита. В результате для перехватчика возможный базис кубита может быть не в одном из двух положений, а в значительно большем наборе.

Алиса готовит и передает состояния одиночных фотонов, а Боб измеряет их в базисах, заданных последовательностью $\varphi(K,i)$. В результате для каждого кубита базисы приготовления и измерения будут совпадать в 50% случаев. Для перехватчика же базис не

известен и может принимать не 4 избранных положения, как в BB84, а произвольное состояние в Гильбертовом пространстве состояний кубит.

Показано, что в классическом случае данный подход не позволяет генерировать ключ по размерам превосходящий объем исходной секретной информации. Квантовый анализ возможного перехвата состояний показал, что невозможность полного измерения одиночного кванта позволяет генерировать секретный ключ более, чем вдвое превосходящий по объему исходную секретную информацию.

Был произведен теоретический анализ секретности протокола при использовании сильно ослабленного лазерного импульса для кодирования квантовых состояний. Доказательство секретности разбивается на две части:

1. Доказательство секретности передаваемого квантового ключа при не полностью перехваченном вспомогательном ключе (исходной секретной информации Алисы и Боба)
2. Доказательство невозможности полного перехвата вспомогательного ключа даже в случае, когда используется квантовая память и передаваемая с помощью этого ключа информация известна, этот вид атаки известен литературе под названием known cipher attack.

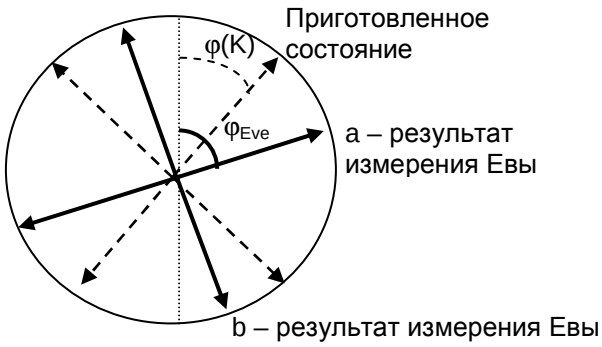

Рис. 3. Для каждого вероятного значения вспомогательного ключа K Ева рассчитывает вероятное положение базиса $\varphi(K)$ и рассматривает вероятность фактически полученного исхода измерения $p(ab\,|\,K)$ – «a» фотонов на одну ось и «b» фотонов на вторую ось, при условии, что K – значение вспомогательного ключа.

Оценка количества перехваченных бит вспомогательного ключа производилась следующим образом. На основе своих измерений перехватчик приписывает каждому вспомогательному ключу К свой вес $p_i(K)$. Предположим, что при измерении перехватчик выбрал базис, угол которого равен φ_{Eve}, при этом на одной оси было измерено «a» фотонов, на второй – «b» фотонов. Сумма «$a+b$» равна количеству фотонов, перехваченному в результате атаки с разделением фотонов, так как в качестве источника

кубит используется ослабленный лазерный импульс, «$a+b$» может быть больше единицы. Для каждого возможного K перехватчик рассчитывает возможное положение базиса $\varphi(K)$ (рис. 3) и рассчитывает вероятность полученного результата измерения при условии использования каждого возможного вспомогательного ключа $p(ab \mid K)$.

В общем случае при известном передаваемом ключе и произвольном количестве фотонов в импульсе вероятность измерить «a» фотонов на оси (1) и «b» фотонов на оси (0) составляет:

$$p(ab \mid K) = C_{a+b}^{a} \cos^{2a}(\varphi(K) - \varphi_{Eve}) \sin^{2b}(\varphi(K) - \varphi_{Eve}) \qquad (4)$$

В результате произведенных измерений перехватчик рассчитывает уточненное распределение вероятности значения вспомогательного ключа K – $p(K)$.

$$p_{i+1}(K) = \frac{p(ab \mid K) * p_i(K)}{\sum_K p(ab \mid K) p_i(K)} \qquad (5)$$

Где i – номер импульса, а $p(ab)$ – вероятность получить результат измерения ab.

Таким образом, в результате каждого измерения перехватчик получает дополнительную информацию и меняет свое представление о распределении базисов. По мере передачи квантового ключа можно производить верхнюю оценку количества информации, известной Еве о вспомогательном ключе. Передача квантового ключа возможна, пока вспомогательный ключ не известен Еве полностью.

Рассмотрим лазерный импульс, содержащий два фотона. Ева разделяет его на два одиночных фотона. Один передается Бобу и используется для формирования ключа, которым передавался известный перехватчику отрывок информации, а второй сохраняется в квантовой памяти и затем измеряется для атаки на вспомогательный ключ. Пусть например, результат измерений Евы – $a = 1; b = 0$, используя (4) и (5) получаем:

$$p(ab = \{1,0\}) = \sum_K p(ab = 10 \mid K) p_i(K) = \sum_K \cos^2(\varphi(K) - \varphi_{Eve}) p_i(K) = \frac{1}{\pi}\int_0^{\pi} \cos^2(\theta) d\theta = \frac{1}{2}$$

Так как $p_{i+1}(K) = \dfrac{p(ab \mid K) * p_i(K)}{\sum_K p(ab \mid K) p_i(K)} = 2p(ab \mid K) * p_i(K) = 2\cos^2(\varphi(K) - \varphi_{Eve}) p_i(K)$

Из чего можем рассчитать количество секретных бит во вспомогательном ключе:

$$N_{secret}(i+1) = -\sum_K p_{i+1}(K)\log_2(p_{i+1}(K)) = -\sum_K 2\cos^2(\Delta\varphi)p_i(K)\log_2(2\cos^2(\Delta\varphi)p_i(K)) =$$
$$= -2\sum_K \cos^2(\Delta\varphi)p_i(K)\left[\log_2(2\cos^2(\Delta\varphi) + \log_2(p_i(K))\right] =$$
$$-2\sum_K \cos^2(\Delta\varphi)\log_2(2\cos^2(\Delta\varphi)p_i(K) - 2\sum_k \cos^2(\Delta\varphi)p_i(K)\log_2(p_i(K))$$
$$\approx -\frac{2}{\pi}\int_0^\pi \cos^2(\theta)\left(1 + \frac{2}{\ln(2)}\ln(\cos(\theta)\right)d\theta - \frac{2}{\pi}\int_0^\pi \cos^2(\theta)d\theta * \sum_k p_i(K)\log_2(p_i(K))$$

Учитывая, что $-\sum_k p_i(K)\log_2(p_i(K)) = N_{secret}(i)$, $\frac{2}{\pi}\int_0^\pi \cos^2(\theta)d\theta = 1$

$$N_{secret}(i+1) \approx N_{secret}(i) - \frac{2}{\pi}\int_0^\pi \cos^2(\theta)\left(1 + \frac{2}{\ln(2)}\ln(\cos(\theta)\right)d\theta = N_{secret}(i) + \left(1 - \frac{1}{\ln(2)}\right) =$$
$$= N_{secret}(i) - 0{,}44\,бит$$

Оценка объема перехваченной информации при этом будет 0,44 бит на один переданный бит ключа, из чего можно заключить, что генерируемый секретный ключ может в два раза превосходить объем вспомогательного ключа. Подобным образом рассчитывается количество перехваченных бит для других результатов измерений при различном количестве фотонов в импульсе.

Секретная передача данных возможна, когда объем генерируемого квантового ключа, превосходит объем вспомогательного ключа. В этом случае возможен непрерывный процесс, когда предыдущая передача генерирует вспомогательный ключ для следующей.

Результат расчета скорости генерации квантового ключа для кодирования секретных данных приведен на рис. 4. На расстояниях более 60 км для одинаковых физических параметров установки абсолютная секретность с использованием протокола BB84 не возможна, но может быть выполнена на протоколе с плавающим базисом.

Описанный подход позволил доказать секретность протокола при атаках с квантовой памятью, частично известной передаваемой информации (known cipher). Отдельно следует подчеркнуть, что структура протокола позволяет говорить о значительно более надежной системе авторизации через квантовый канал за счет кодирования положений базисов, нежели авторизация классического канала. Это делает данный протокол более стойким к одновременным атакам на квантовый и классический каналы (men in the middle attack).

Анализ работы протокола при использовании сильно ослабленных лазерных импульсов показал, что в данном протоколе возможно повысить среднее число фотонов до 0,5-1 фотон/импульс вместо 0,1-0,2, стандартно используемых в протоколе BB84.

Повышение среднего числа фотонов в импульсе неизбежно ведет к улучшению соотношения сигнал/шум на стороне приемника и, как следствие, повышению скорости генерации ключа и предельной дальности работы протокола.

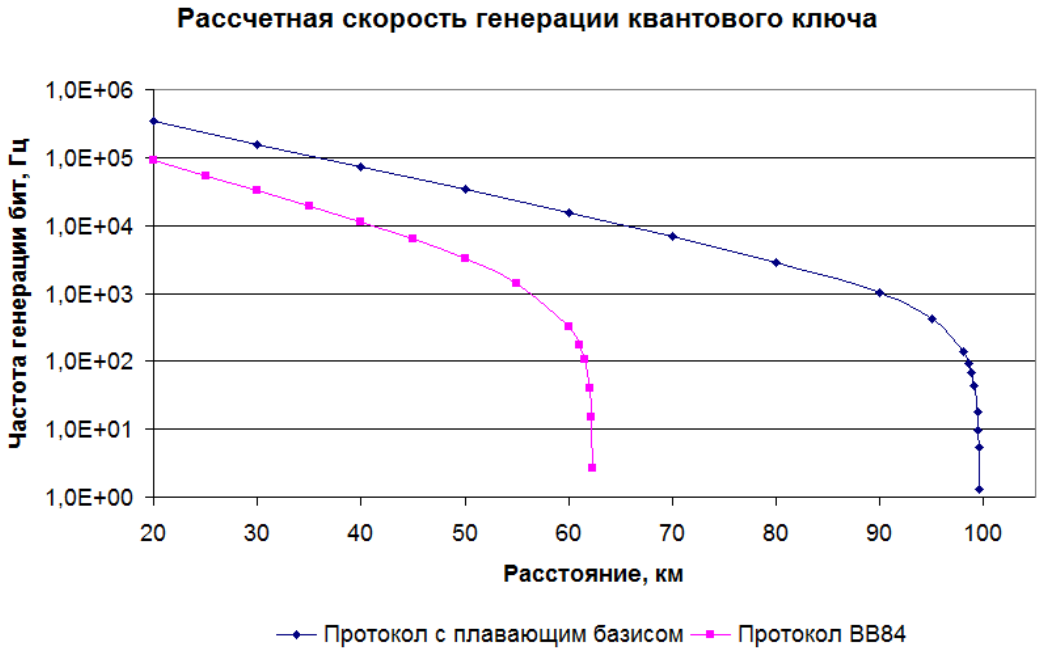

Рис. 4. Использование протокола с плавающим базисом дает преимущество по сравнению с протоколом BB84 при одинаковых параметрах установки для всех расстояний. Для расчета использовались следующие физические параметры установки: потери в оптоволоконной линии – 0,2 дБ/км, эффективность детектирования – 14%, вероятность шумового срабатывания 10^{-5}, ошибки синхронизации оптики – 1%, частота повторения импульсов – 30 МГц, число фотонов в импульсе оптимизируется для каждой точки.

Протокол с плавающим базисом имеет значительный потенциал для применения в квантовых системах связи. Также следует особо подчеркнуть, что данный протокол может внедряться на существующих установках квантовой криптографии для протокола BB84 без значительных конструкционных изменений, что делает его особенно перспективным в практическом плане.

В третьей главе рассматривается экспериментальная часть работы. Детально описаны две установки квантовой криптографии для реализации протоколов с увеличенным числом базисов и с плавающим базисом. В данных установках использовались фазовый и частотный методы кодирования одиночных фотонов.

Впервые в России осуществлено распределение квантового ключа на созданной полностью оптоволоконной процессорной системе для квантовой криптографии, работающей на телекоммуникационной длине волны 1,5 мкм. Оптическая часть собрана из оптоволоконных элементов по схеме автокомпенсационного интерферометра Маха-Цандера с двойным проходом луча. Основное достоинство выбранной нами схемы -

стабильность работы интерферометра и независимость регистрируемого оптического сигнала от внешних изменений оптоволоконной линии связи, длина которой может быть на уровне 100 км. Носителем квантового ключа является один фотон с фазовым кодированием в двух не ортогональных друг другу базисах.

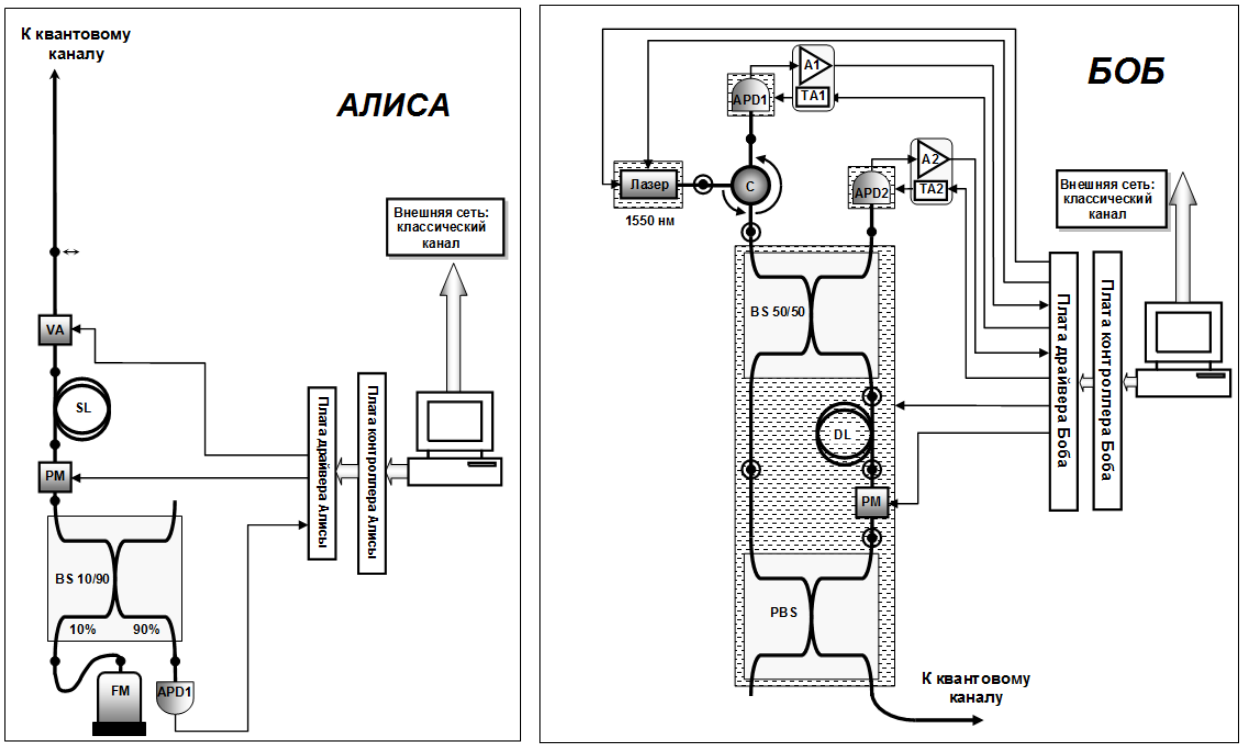

Рис. 5. Установка Алисы (слева). VA – переключаемый аттенюатор, SL – 25 км линия хранения, PM – фазовый модулятор, BS – разделитель, FM – Зеркало Фарадея, APD1 – фотодиод. Установка Боба (справа). C – циркулятор, APD1, APD2 – лавинные фотодиоды для счета фотонов, A1, A2 – усилители, BS – разделитель, DL – линия задержки 10 метров, PM – фазовый модулятор, PBS – поляризационный разделитель.

В рамках данной работы были изучены методы фазового кодирования и декодирования квантовых состояний одиночных фотонов с применением фазовых модуляторов и интерферометров Маха-Цандера и последующим детектированием их с высокой вероятностью. Получена генерация квантового ключа со скоростью 700 бит/сек. на длине квантовой линии 25 км, при частоте повторения лазерных импульсов 5 МГц. Созданы новые детекторы одиночных фотонов для длины волны излучения 1,5 мкм на основе специально отобранных AsInGa/InP лавинных фотодиодов ETX 40 и ERM547. Изучены методы регистрации одиночных фотонов с длиной волны 1,5 мкм при работе фотодиодов в режиме Гейгеровской моды. Для секретности передачи требуется присутствие не более одного фотона в каждом лазерном импульсе, поэтому были детально изучены характеристики детекторов – квантовая эффективность, уровень темновых шумов и вероятность появления послеимпульсов. На основании проведенных

исследований найдены рабочие области фотодиодов. Используемые детекторы позволили регистрировать одиночные фотоны с вероятностью 10-15%, при уровне шумов менее 10^{-4} на строб напряжения длительностью 3. Уровень ошибок в ключе при длине линии 25 км находится на уровне 2-3%. Распределение квантового ключа между Алисой и Бобом происходит по протоколу BB84.

Отдельно следует подчеркнуть исследование детекторов одиночных фотонов на основе коммерчески доступных InGaAs-InP лавинных диодов ETX 40 APD END BA (JDS Uniphase). Тестирование производилось в Гейгеровской моде, в режиме строба, когда напряжение на диоде поднимается выше порога рождения лавины только на короткий (3 нс), строго определенный период времени, в который ожидается приход фотона.

Основным параметром для квантовой криптографии является соотношение сигнал/шум. Для поиска рабочей точки однофотонных детекторов используется график зависимости квантовой эффективности от логарифма темнового счета (Рис. 6).

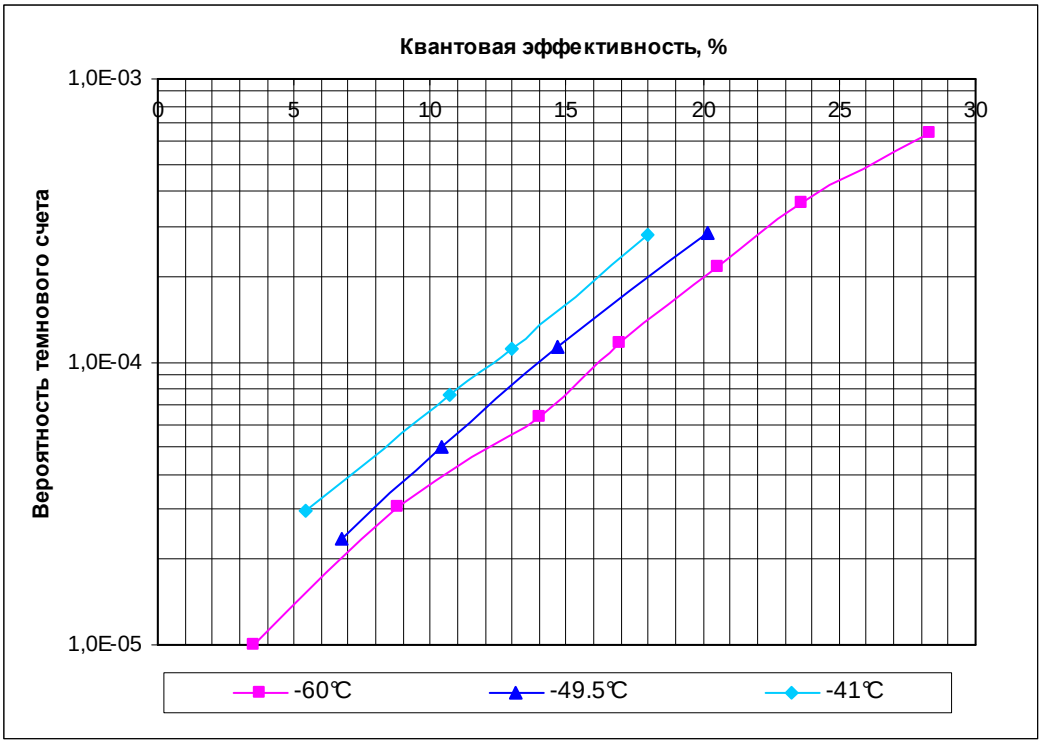

Рис. 6. Зависимость квантовой эффективности от логарифма уровня темновых шумов при различных температурах.

Вероятность послеимпульсов ограничивает частоту работы детектора. Чем меньше время между импульсами, тем больше вероятность измерить шумовой импульс, связанный со срабатыванием детектора в предыдущий период. Этот счет не связан с измерением реальных фотонов, что дает ложные срабатывания детектора. Так как вероятность послеимпульсов возрастает при снижении температуры, что обратно

поведению тепловых шумов, то для выбора рабочей температуры были произведены измерения вероятности послеимпульсов от времени при различных температурах.

Измерение параметров детекторов одиночных фотонов дает возможность выбрать рабочую точку для регистрации фотонов при работе установки для квантовой криптографии, например:

- Исходя из графика на Рис. 6, квантовая эффективность 10% при вероятности шумового срабатывания детектора $5*10^{-5}$ подходит для целей генерации ключа.
- На основе результатов измерения темнового счета и вероятности послеимпульсов оптимальной температурой является -50 -60°C
- При значительном снижении температуры вероятность послеимульсов негативно влияет на предельную скорость генерации ключа, так при температуре -60°C после каждого срабатывания детектора необходимо выдерживать мертвое время не менее ~1-3 мкс.

Установка с использованием **частотного кодирования** сконструирована специально для демонстрации протокола с плавающим базисом. Основной принцип частотного кодирования заключается в том, чтобы получить интерференцию между импульсами с различной частотой, при помощи амплитудной модуляции. На практике передатчик Алиса модулирует амплитуду лазерного излучения с помощью электрического сигнала с частотой порядка нескольких гигагерц и передает сигнал с интенсивным центральным пиком и слабыми боковыми. Принимающая сторона – Боб модулирует сигнал с помошью интерферометра Маха – Цандера. В случае совпадения фаз модуляции у Алсы и Боба происходит интерференция между боковыми пиками, созданными первой и второй модуляциями, которая измеряется Бобом при помощи фильтра Фабри-Перо.

На данной установке в многофотонном режиме был продемонстрирован протокол с плавающим базисом.

В заключении перечислены основные результаты, полученные в диссертации.

1. Предложен метод повышения уровня секретности путем увеличения количества базисов. Впервые в мире предложено использовать информацию, исключаемую при сверке базисов для детектирования перехвата. Данный подход эффективен для трех и более базисов. Теоретическая разработка была экспериментально реализована автором на установке для воздушной линии связи. Экспериментальное измерение влияния перехвата показало перспективность использования этого протокола.

2. Разработан и проведен анализ секретности оригинального протокола квантовой криптографии. Данный протокол позволяет достичь более высоких, по сравнению с используемыми методами, скоростей генерации квантового ключа. За счет того, что в

данном протоколе не существует фиксированного набора базисов, среднее число фотонов может быть увеличено, что влечет за собой дополнительное увеличение эффективности протокола.

3. Создана первая в России оптоволоконная установка для квантовой криптографии, на которой продемонстрировано распределение квантового ключа. Данная разработка находится на мировом уровне. В установке используются передовые технологии и методы, так, например, управление всей установкой происходит с помощью специализированного процессора, что позволяет достигать высокой степени автоматизации и, как следствие, высокой скорости работы.

4. Созданы детекторы одиночных фотонов для длины волны излучения 1,5 мкм. Изучены методы регистрации одиночных фотонов с длиной волны 1,5 мкм при работе фотодиодов в режиме Гейгеровской моды. Исследованы параметры детекторов - квантовая эффективность, вероятность появления послеимпульсов и уровень шумов для различных режимов работы InGaAs-InP лавинных фотодиодов.

5. В рамках Российско-Французского сотрудничества для реализации протокола с плавающим базисом была создана специальная экспериментальная установка на основе частотного кодирования кубит. Была произведена экспериментальная демонстрация протокола с плавающим базисом в многофотонном режиме.

Публикации автора по теме диссертации:

1. Kurochkin Y., Kurochkin V. Quantum key distribution and eavesdropping in multi bases protocols // Digest IV International Symposium on Modern Problem of Laser Physics. Novosibirsk, Russia. August 22-27, 2004. – P. 265-266.

2. Kurochkin Y. Multi Basis Quantum Cryptography // Abstract of EQIS’04 Conf., Tokyo, Japan, September 1-5, 2004. – P. 118-119.

3. Kurochkin Y., Kurochkin V. Quantum key distribution and eavesdropping in multi bases protocols // Proceedings of IV International Symposium on Modern Problem of Laser Physics. Novosibirsk, Russia. August 22-27, Novosibirsk 2005. – P. 461-466.

4. Kurochkin Y. Quantum cryptography with floating basis protocol // Abstract International symposium “Quantum informatics – 2004”, Moscow, Russia Oct. 5-8, 2004. – P. 8.

5. Yury Kurochkin Quantum cryptography with floating basis protocol. // Proc. SPIE. 2005. – Vol. 5833. – P. 213-221.

6. V.L. Kurochkin, I.I. Ryabtsev, A.V. Zverev, V.K. Ovchar, I.G. Neizvestny, S. Moon, B.S. Bae, H.J. Shin, J.B. Park, C.W. Park Experimental setup for long-distance quantum cryptography via optical fiber lines // Abstract International symposium “Quantum informatics – 2005”. Moscow, Russia Oct. 3-7, 2005. – P. O20.

7. V.L. Kurochkin, A.V. Zverev, Y.V. Kurochkin, I.I. Ryabtsev, I.G. Neizvestny, S. Moon, B.S. Bae, H.J. Shin, J.B. Park, C.W. Park Experimental quantum cryptography for standart fibers and free space // Abstract of XI international conference on quantum optics'2006, Minsk, Belarus, May 26-31, 2006. – P. 57.

8. Kurochkin Y., Kurochkin V. Problems of security in quantum key distribution with floating basis protocol // Abstract of AQIS'06 Conference, Beijing, China, September 1-4, 2006. – P. 134-135.

9. V.L. Kurochkin, A.V. Zverev, Y.V. Kurochkin, I.I. Ryabtsev, I.G. Neizvestny, S. Moon, B.S. Bae, H.J. Shin, J.B. Park, C.W. Park Fiber quantum cryptography setup with auto-compensating scheme // Abstract of AQIS'06 Conference, Beijing, China, September 1-4, 2006. – P. 191-192.

10. Kurochkin Yury, Donnet Stéphane, Cussey Johann, Kurochkin Vladimir, Merolla Jean-Marc Setup for quantum cryptography with floating basis protocol in frequency coding // Abstract of XIV International Scientific Conference forundergraduate and postgraduate students, and young scientists"Lomonossov" 11-14 april 2007, http:// http://lomonosov-msu.ru/archive/Lomonosov_2007/18.htm

11. В.Л. Курочкин, А.В Зверев, И.И. Рябцев, Ю.В. Курочкин, Р.А. Лавров, И.Г. Неизвестный Квантовая оптоволоконная линия связи // Фотон-экспресс. – 2007. – №6(62). – С. 187.

12. R.A. Lavrov, V.L. Kurochkin, Y.V.Kurochkin Yury Quantum Key Distribution Based On Two-Way Optical Scheme // Abstract of X Internationa Conference for Wave Electronics and Its Applications in the Information and Telecommunication Systems St. Petersburg, Russia 2-6 July 2007. – P. 29-30.

13. V. Kurochkin, Yu. Kurochkin Building of the quantum cryptography protocol using no-cloning theorem // Abstract of The 4th International Workshop "Quantum Physics and Communication' Dubna, 15 - 19 October, 2007. – P. 50-51.

14. V. Kurochkin Y. Kurochkin InGaAs-InP single photon detectors for the quantum cryptography best operation // Digest V International Symposium on Modern Problem of Laser Physics. Novosibirsk, Russia. August 24-30, 2008. – P. 189-190.

15. V. Kurochkin, Y. Kurochkin Single photon detector for fiber quantum key distribution // Abstract Third Russian-French Laser Physics Workshop. St. Petersburg, Russia, September 22-27, 2008. – P. 45-46.

16. V. Kurochkin, Y. Kurochkin Quantum communication speed improvement with the use of realistic parallel detectors considering the privacy amplification algorithms // Abstracts of International Conference Mathematical Modeling And Computational Physics, Dubna, Russia, 7-11 July 2009. – P. 194-195.

17. V. Kurochkin, Yu. Kurochkin Principles of the New Quantum Cryptography Protocols Building // Physics of Particles and Nuclei Letters. – 2009. – Vol. 6, N. 7. – P. 605-607.

18. Курочкин В.Л., Зверев А.В., Курочкин Ю.В., Рябцев И.И., Неизвестный И.Г. Применение детекторов одиночных фотонов для генерации квантового ключа в экспериментальной оптоволоконной системе связи // Автометрия. – 2009. – Т.45, №4. – С. 110-119.

19. Курочкин Ю.В. Анализ секретности протокола квантовой криптографии с неограниченным числом базисов // Материалы докладов XVI Международной конференции студентов, аспирантов и молодых ученых «Ломоносов» http://www.lomonosov-msu.ru/2009/

20. S. Bagaev,Y. Kurochkin, V. Kurochkin. Quantum cryptography protocol based on physical limitations of the photon quantum state measurement precision // Abstracts of Second Nanotechnology International Forum, Moscow, Russia, October 6 – 8, 2009. – P. 24-25.

21. Курочкин В.Л., Зверев А.В, Курочкин Ю.В., Рябцев И.И., Неизвестный И.Г. Экспериментальная установка для квантовой криптографии на основе автокомпенсационной оптической схемы // Фотон-экспресс. – 2009. – №6. – С. 172-173.

22. Ю.В.Курочкин, В.Л.Курочкин Детекторы одиночных фотонов на основе лавинных фотодиодов // Тез докладов XII международной школы-семинара по люминесценции и лазерной физике. Россия, Иркутск, 26 – 31 июля 2010. – С. 133-134.

23. V. Kurochkin, Yu. Kurochkin Quantum Cryptography Security Improvement With Additional States // Procceedings 11 international conference Micro/Nanotechnologies EDM2010, Erlagol, Russia, June 30 –July 4, 2010. – P. 231-233.

24. В.Л. Курочкин, А.В. Зверев, Ю.В. Курочкин, И.И. Рябцев, И.Г. Неизвестный Экспериментальные исследования в области квантовой криптографии // Микроэлектроника. – 2011. – Т. 40, №. 4. – С. 245–253.

25. Y. Kurochkin, V. Kurochkin Quantum cryptography efficiency increase using secret basis shift // Abstract International Conference on Quantum Technologies, Moscow, July 13-17, 2011. – P. 55.

26. В. Л. Курочкин, А. В. Зверев, И. И. Рябцев, И. Г. Неизвестный, А. А. Вольф, Ю. В. Курочкин, А. Г. Черевко Регистрация одиночных фотонов на длине волны 1,5 мкм. // Тез. докладов Российской конференции по актуальным проблемам полупроводниковой нанофотоэлектроники "ФОТОНИКА 2011", Новосибирск, 22 - 26 августа 2011. – С. 124.

27. Ю.В.Курочкин, В.Л.Курочкин Детекторы одиночных фотонов на основе лавинных фотодиодов // Известия вузов. Физика. – 2011. – Т. 54, № 2. – С. 202-205.