Московский государственный университет
имени М. В. Ломоносова

На правах рукописи

Кронберг Дмитрий Анатольевич

Криптографическая стойкость систем квантовой криптографии с фазово-временным кодированием

01.01.05 — Теория вероятностей и математическая статистика

Автореферат диссертации на соискание учёной степени
кандидата физико-математических наук

Москва — 2010

Работа выполнена на кафедре квантовой информатики факультета вычислительной математики и кибернетики Московского государственного университета имени М. В. Ломоносова.

Научный руководитель:	доктор физико-математических наук, профессор Молотков Сергей Николаевич
Официальные оппоненты:	доктор физико-математических наук, профессор Кузьмин Алексей Сергеевич, Академия криптографии Российской Федерации
	доктор физико-математических наук, ведущий научный сотрудник Математического института имени В. А. Стеклова РАН Широков Максим Евгеньевич,
Ведущая организация:	Институт информатики АН Республики Татарстан

Защита диссертации состоится «___» декабря 2010 г. в 11:00 на заседании диссертационного совета Д 501.001.44 при Московском государственном университете имени М. В. Ломоносова по адресу: 119991, ГСП-1, Москва, Ленинские горы, МГУ, 2-й учебный корпус, факультет ВМК, аудитория 685.

С диссертацией можно ознакомиться в библиотеке факультета ВМК МГУ. С текстом автореферата можно ознакомиться на официальном сайте факультета ВМК МГУ http://cs.msu.su в разделе «Наука» — «Работа диссертационных советов» — «Д 501.001.44».

Автореферат разослан «___» ноября 2010 г.

Ученый секретарь
диссертационного совета
профессор Н.П.Трифонов

Общая характеристика работы

Диссертационная работа посвящена исследованию криптографической стойкости протоколов квантового распределения ключей с фазово-временным кодированием против различных видов атак, включая атаку с разделением по числу фотонов.

Актуальность темы.

Квантовая криптография как наука зародилась в 1984 году, когда был разработан первый протокол квантового распределения ключей, названный BB84 (Bennett, Brassard). Главным преимуществом квантовых криптографических протоколов распределения ключей перед классическими является тот факт, что секретность передаваемых ключей гаранируется фундаментальными законами Природы — квантовой механики, а не предположениями об ограниченных технических или вычислительных возможностях подслушивателя.

Секретность ключей в квантовой криптографии основана на двух фундаментальных запретах квантовой механики: 1) запрете на копирование (клонирование) неизвестного квантового состояния (no cloning теорема); 2) невозможности достоверного (с вероятностью единица) различения неортогональных квантовых состояний. Любые попытки вторжения в канал связи с целью получения информации о передаваемых неортогональных квантовых состояниях неизбежно приводят к ошибкам на приемной стороне, в результате чего любые попытки подслушивания обнаруживаются по дополнительным помехам. Решение о возможности секретного распространения ключей достигается легитимными пользователями на основе величины наблюдаемой ошибки на приёмной стороне. Секретное распределение ключей возможно, если ошибка не превышает некоторой критической величины.

Это означает, что важнейшей характеристикой протоколов квантовой криптографии является допустимая критическая ошибка на приёмной стороне, до которой возможно секретное распространение ключей. Чем допустимая ошибка больше, тем более устойчивой является система квантовой криптографии по отношению к собственным шумам и попыткам подслушивания. Одной из главных задач при анализе стойкости протоколов квантового распределения ключей является нахождение точной величины критической ошибки.

Экспериментальная реализация квантовой криптографии натолкнулась на ряд технологических трудностей, наиболее важной из которых является сложность генерации строго однофотонных квантовых

состояний. На практике обычно используются ослабленные лазерные импульсы, которые описываются когерентными квантовыми состояниями. Когерентное состояние имеет пуассоновскую статистику по числу фотонов. Оказывается, что использование когерентных состояний в сочетании с неизбежным затуханием в реальных каналах связи даёт перехватчику возможность задержать часть фотонов у себя, а после получения некоторых сведений от легитимных пользователей, передаваемых по открытому каналу, извлечь из них всю необходимую информацию. В результате схемы квантовой криптографии теряют свою секретность, если длина линии связи превышает некоторую критическую величину. Подобные действия перехватчика получили название атаки с разделением по числу фотонов, или PNS-атаки (Photon number splitting attack). Поэтому следующей принципиально важной задачей при анализе криптографической стойкости реальных систем квантовой криптографии является определение критической длины линии связи, до которой гарантируется секретность распределения ключей.

Разработки в области противодействия PNS-атаке привели к появлению протокола с изменённой (по сравнению с BB84) конфигурацией состояний, используемых легитимными пользователями. Наиболее известным протоколом, устойчивым к PNS-атаке, является протокол SARG04, предложенный в 2004 году (Scarani, Acin, Ribordy, Gisin). Как показал анализ, протокол перестаёт быть секретным только в том случае, когда перехватчик имеет возможность блокировать все одно-, двух- и трёхфотонные посылки. А это значит, что можно говорить о понятии критической дистанции секретного распределения ключей, на которой доля импульсов с большим числом фотонов достаточно мала. Устойчивость протокола против PNS-атаки определяется именно этой критической длиной линии связи.

Другая часть усилий исследователей направлена на модификацию протоколов кватового распределения ключей с целью увеличения критической величины ошибки, и на сегодняший день разработаны технологии, позволяющие довести её примерно до 30%. Одним из методов увеличения критической ошибки является использование *классической предварительной обработки данных*, сводящейся к специальным согласованным действиям легитимных пользователей после оценки количества ошибок на приёмной стороне.

В то же время теоретический предел вероятности ошибки, до которой вообще можно безошибочно передавать информацию в асимптотическом пределе длинных последовательностей, составляет, согласно теореме Шеннона, 50%. Возникает принципиально важный вопрос — существуют ли протоколы квантовой криптографии, которые позволяют

не только безошибочно передавать информацию, но и гарантировать секретность ключей, вплоть до вероятности ошибки на приемной стороне не превышающей 50%. Оказывается, что возможна конфигурация сигнальных состояний, которая даёт в определённых случаях возможность распространения ключа при ошибке на приёмной стороне вплоть до 50%, и это оказывается возможным при использовании *двухпараметрических протоколов квантовой криптографии*, к которым относится протокол с фазово-временным кодированием.

Существует модификация протокола с фазово-временным кодированием, которая использует конфигурацию базисных векторов, схожую с их расположением в протоколе SARG04, позволяет сделать этот протокол также устойчивым против PNS-атаки. Более того, благодаря тому, что протокол с фазово временным кодированием использует большее количество базисов по сравнению с SARG04, его устойчивость к PNS-атаке оказывается существенно больше: теперь уже для полного взлома перехватчику нужно иметь возможность блокировать все посылки, содержащие от одного до пяти фотонов (а не от одного до трёх, как в случае SARG04). Результат этого — наибольшая критическая длина линии связи среди всех изветных на сегодняшний день протоколов квантового распределения ключей.

Другой интересной и практически важной задачей является построение явной квантовой схемы оптимальной однофотонной атаки перехватчика на известные протоколы квантового распределения ключей. Работа данной квантовой схемы может рассматриваться как одношаговое квантовое вычисление. Такая схема должна сводить все действия перехватчика к использованию реализуемых на сегодняшний день элементов, преобразующих квантовые состояния. Такими элементами являются однокубитовые элементы (реализуемые с помощью асимметричных светоделителей и фазовых модуляторов) и элемент «контролируемое НЕ» (CNOT), действующий на двухчастичные состояния. Строго говоря, элемент CNOT на сегодняшний день является ещё слишком сложным для построения, и вместо него в экспериментах используются его вероятностные модификации, выполняющие нужное действие лишь с некоторой вероятностью. Однако так как произвольное квантовое преобразование невозможно без реализации двухчастичных вентилей, то будем предполагать, что элемент CNOT, как наиболее простую двухчастичную операцию, можно реализовать с применением сегодняшних технологий. Задача построения схемы оптимальной атаки важна, в частности, тем, что с её помощью можно

оценить сравнительную сложность атаки на разные криптографические протоколы.

Разработка новых протоколов квантового распределения ключей и исследование их криптографической стойкости является на сегодняшний день важной научной и практической задачей, что определяет **актуальность** темы диссертационной работы.

Целью диссертационной работы являлось:

1. Нахождение критической величины ошибки для протокола SARG04 в случае использования строго однофотонных состояний для передачи информации.

2. Исследование стойкости протокола с фазово-временным кодированием при использовании строго однофотонных импульсов, нахождение области секретности протокола как функции двух параметров — битовой ошибки на приёмной стороне и количества отсчётов в контрольных временных окнах.

3. Исследование стойкости модификации протокола с фазово-временным кодированием с неортогональными состояниями внутри базисов против атаки с разделением по числу фотонов, а также определение критической длины линии связи, до которой гарантируется секретность распространения ключей.

4. Построение квантовой схемы для оптимального подслушивания протокола с фазово-временным кодированием при использовании строго однофотонных состояний для передачи данных.

5. Получение оценок стойкости протокола с фазово-временным кодированием с классической предвартельной обработкой данных.

Научная новизна диссертационной работы заключается в следующих положениях:

1. Для протокола SARG04 впервые получены значения критической ошибки на приёмной стороне Q_c при каждом значении параметра протокола — угла между сигнальными состояниями внутри базиса.

2. Найдена область секретности протокола с фазово-временным кодированием на плоскости (Q, q) параметров, наблюдаемых на приёмной стороне: битовой ошибки и количества отсчётов в контрольных временных окнах. Показано, что при отсутствии отсчётов в контрольных временных окнах секретная передача информации возможна при битовой ошибке, меньшей 50%, что является теоретическим пределом.

3. Получена зависимость критической длины линии связи от среднего числа фотонов в лазерном импульсе для неортогональной модификации протокола с фазово-временным кодированием.

4. Построена квантовая схема оптимальной однофотонной атаки на протокол с фазово-временным кодированием и даны принципы физической реализации подобной атаки.

Научная и практическая значимость диссертации состоит в возможности использования её результатов при построении системы квантового распространения ключей с использованием ослабленных лазерных импульсов и оптоволоконных линий связи:

- для оценки информации подслушивателя о ключе из наблюдаемых на приёмной стороне параметров.
- для оценки критической длины линии связи, до которой перехватчик не имеет возможность применить PNS-атаку.
- для оценки изменения информации перехватчика при применении метода предварительной блочной обработки данных.

Основные положения, выносимые на защиту:

1. Для протокола SARG04 получены значения критической ошибки на приёмной стороне, до которой возможно секретное распределение ключей, при произвольном значении угла между сигнальными состояниями внутри базиса.

2. Найдена область секретности протокола с фазово-временным кодированием на плоскости параметров, наблюдаемых на приёмной стороне: битовой ошибки и количества отсчётов в контрольных временных окнах. Также исследован способ увеличения области секретности с помощью классической предварительной обработки сигналов.

3. Получена зависимость критической длины линии связи от среднего числа фотонов в лазерном импульсе для неортогональной модификации протокола с фазово-временным кодированием.

4. Построена квантовая схема оптимальной атаки на протокол с фазово-временным кодированием в случае строго однофотонного источника.

Апробация работы

Основные результаты работы докладывались на следующих конференциях:

- Международная конференция «Quantum Informatics — QI-2007», Москва, Россия, 2007 г.;
- Международная конференция «Quantum Cryptography and Computing: Theory and Implementation», Гданьск, Польша, 2009 г.;
- Международная конференция «Quantum Informatics — QI-2009», Москва, Россия, 2009 г.;
- Международная конференция «19th International Laser Physics Workshop», Фос-ду-Игуасу, Бразилия, 2010 г.

Личный вклад автора

Все результаты, представленные в диссертационной работе, получены автором лично либо при его непосредственном участии.

Публикации

По теме диссертации опубликовано 6 научных работ в рецензируемых журналах из списка ВАК России, список которых приведен в конце автореферата.

Объем и структура работы.

Диссертация состоит из введения, четырех глав и заключения. Полный объем диссертации составляет **208** страниц текста с **30** рисунками. Список литературы содержит **95** наименований.

Содержание работы

Во **Введении** обосновывается актуальность исследований, проводимых в рамках данной диссертационной работы, ставятся задачи работы, сформулированы научная новизна и практическая значимость представляемой работы. Помимо этого во введении даются основные факты и понятия из близких к теме диссертации областей науки: криптографии, квантовой теории информации и квантовой криптографии.

В первой части введения даются основные факты классической криптографии. Криптографическая система называется *симметричной*, если для зашифрования и расшифрования сообщения используется один и тот же секретный ключ, в противном случае система называется *асимметричной*. Преимуществом симметричных систем шифрования является гарантия их абсолютной стойкости при выполнении условий, сформулированных в работе Шеннона в 1945 г. и опубликованной в 1949 г. Здесь же нужно отметить ради исторической справедливости, что критерий абсолютной стойкости

был сформулирован Владимиром Александровичем Котельниковым в отчете, датированном 18 июня 1941 г.

Эта теорема предъявляет следующие требования к криптографической системе для абсолютной стойкости: ключ должен выбираться случайно, использоваться только один раз, и его длина должна быть не меньше длины исходного сообщения. Эта теорема сводит задачу секретной передачи данных к задаче распространения случайных секретных ключей нужной длины. Так как эта задача является технически сложной, особенно в условиях большого количества абонентов, в последнее время всё более популярны становятся асимметричные системы шифрования, или системы с открытым ключом. Они уже не требуют наличия секретного ключа между каждой парой обменивающихся информацией абонентов: при использовании криптосистем с открытым ключом каждый может зашифровать сообщение для данного абонента, используя его открытый ключ. В то же время для расшифрования информации требуется закрытый ключ, который известен только адресату сообщения. Подобная асимметрия между процедурами шифрования и расшифрования достигается благодаря использованию односторонних функций. Тем не менее до сих пор остаётся открытым вопрос о существовании таких функций, а это означает, что нет гарантии стойкости асимметричного шифрования. Наиболее распространенным асимметричным методом шифрования является алгоритм RSA. Задачей, лежащей в его основе, является задача разложения больших чисел на простые сомножители. До сих пор не было предъявлено быстрого решения этой задачи. В то же время если такое решение будет найдено, это будет означать крах стойкости алгоритма RSA. В 1994 г. Питером Шором был предоставлен алгоритм решения этой задачи на квантовом компьютере, который имеет полиномиальную сложность. Это означает, что при создании квантового компьютера схема RSA перестанет быть секретной, что повергает большому риску и другие асимметричные системы шифрования.

Вторая часть введения посвящена квантовой теории информации — науки, объединяющей теорию информации и квантовую механику. В отличие от классической теории, носителями информации здесь являются не полупроводниковые элементы, а элементарные частицы, подчиняющиеся законам квантовой физики. Все свойства таких частиц определяются их состоянием, поэтому в квантовой теории информации принято говорить не о конкретных частицах, а о их состояниях, не акцентируя внимание на процедуре приготовления частиц в этих состояниях.

Чистым квантовым состоянием, обозначаемым $|\psi\rangle$, называется вектор в гильбертовом пространстве с единичной нормой. Также важен случай

статистического ансамбля нескольких чистых состояний, который задаётся их выпуклой комбинацией, что математически оказывается эквивалентно заданию положительно определённого эрмитового оператора с единичным следом — такой оператор, называемый оператором плотности, и является общим случаем квантового состояния. Множество операторов плотности обозначают как $S(\mathcal{H})$. Чистому состоянию $|\psi\rangle$ соответствует оператор плотности $\rho_\psi = |\psi\rangle\langle\psi|$.

Изменение элементарных частиц со временем подчиняется уравнению Шредингера, которое в квантовой теории информации принимает вид $\rho' = U\rho U^*$, где U — унитарный оператор. Таким образом, вся динамика квантовой системы сводится к унитарным преобразованиям соответствующих операторов плотности.

Процедура измерения квантового состояния подразумевает получение определённого исхода x из множества X, и задается набором положительных эрмитовых операторов $\{M_x\}$, удовлетворяющих условию $\sum_x M_x = I$. Вероятность получения исхода x при таком измерении состояния ρ равна $\mathrm{Tr}M_x\rho$. Фундаментальным свойством квантовый измерений является коллапс волновой функции, в результате которого исходное состояние после измерения $\{M_x\}$ и получения исхода x переходит в состояние

$$\rho_x = \frac{\sqrt{M_x}\rho\sqrt{M_x}}{\mathrm{Tr}M_x\rho}.$$

Два важных следствия коллапса волновой функции — это, во-первых, невозможность достоверного различения двух неортогональных квантовых состояний, а во-вторых, невозможность копирования произвольного квантового состояния.

Состояние квантовой системы из нескольких частиц выражается оператором плотности в тензорном произведении соответствующих гильбертовых пространств каждой его составляющей. Состояние, чей оператор плотности можно представить в виде тензорного произведения операторов плотности, относящихся к отдельным подсистемам ($\rho = \rho_1 \otimes \rho_2 \otimes ... \otimes \rho_n$), называется разделимым состоянием, иначе же состояние называют сцепленным. Традиционным примером сцепленного состояния является состояние ЭПР $|\psi_{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, важным свойством которого является то, что измерение каждой его подсистемы фиксирует также состояние другой подсистемы, в результате чего результаты измерений обоих подсистем оказываются строго согласованными, несмотря на то, что сами частицы могут быть сколь угодно далеки друг от друга.

Одним из важнейших результатов квантовой теории информации является квантовая теорема кодирования, которая даёт величину для

классической пропускной способности канала с заданными квантовыми состояниями на выходе. Эта теорема говорит о том, что пропускная способность квантового канала связи с состояниями $\{\rho_i\}$ на выходе даётся выражением

$$C = \max_{\pi} \chi(\pi, \{\rho_x\}), \tag{1}$$

где $\pi = \{\pi_x\}$ — априорное распределение вероятности квантовых состояний, а $\chi(\pi, \{\rho_x\}) = H\left(\sum_x \pi_x \rho_x\right) - \sum_x \pi_x H(\rho_x)$ — величина, называемая χ-энтропией, или величиной Холево. $H(\rho)$ здесь — энтропия фон Неймана оператора плотности, выражаемая через его собственные значения:

$$H(\rho) = -\sum_i \lambda_i \log \lambda_i.$$

Наконец, третья часть введения посвящена протоколам квантового распределения ключей. Ниболее известный из них — протокол BB84. Он использует два базиса:

$$+ : |x\rangle = |0\rangle, \quad |y\rangle = |1\rangle,$$

$$\times : |u\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |v\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

При посылке сигнала передающая сторона (Алиса) случайно выбирает базис и состояние в нём. На приёмной стороне (пользователя-получателя принято называть Бобом) случайным образом выбирается одно из двух измерений

$$M_0^+ = |x\rangle\langle x|, \quad M_1^+ = |y\rangle\langle y|,$$
$$M_0^\times = |u\rangle\langle u|, \quad M_1^\times = |v\rangle\langle v|.$$

После передачи и измерения всех состояний происходит согласование базисов, в ходе которого Алиса и Боб по открытому каналу сопоставляют используемые в каждой посылке базисы. Те позиции, где базисы не совпали, отбрасываются. Затем раскрывается примерно половина последовательности для оценки ошибки. Если ошибка оказалась больше критической величины, выполнение протокола прерывается, иначе пользователи производят коррекцию ошибок, в результате которой их битовые строки становятся идентичными, а затем усиление секретности, после которого информация Евы становится ограничена наперед заданной (небольшой) величиной.

Неформально секретность протокола обосновывается тем, что перехватчик (Ева) не знает, в каком базисе ей следует измерять передаваемое состояние, в результате чего она неизбежно вносит ошибку в передаваемый сигнал. Более строго секретность протокола BB84

обосновывается его последовательным сведением к измерению ЭПР-состояний, которое гарантированно даёт согласованные результаты, никак не коррелированные с окружающими квантовыми системами.

Одними из важнейших технических проблем при реализации квантовой криптографии является сложность генерации однофотонных импульсов, а также неизбежное затухание в реальных каналах связи. В сочетании неидеальный источник фотонов (обычно это лазер с ослабленной интенсивностью излучения) и канал с затухании способны привести к возможности проведения так называемой PNS-атаке, при которой перехватчик оставляет часть фотонов каждого многофотонного импульса у себя до согласования базисов, а оставшиеся импульсы блокирует. При больших длинах в канале связи потери от блокировки состояний перехватчиком могут быть списаны на затухание, поэтому перехватчик оказывается не обнаруженным, получая всю необходимую информацию о передаваемых состояниях. Таким образом, можно говорить о критической длине линии связи, до которой перехватчик не имеет возможности блокировать достаточное количество импульсов. Противостояние PNS-атаке поэтому заключается в увеличении показателя критической длины. Так, для незащищенного против PNS-атаки протокола BB84 критическая длина составляет всего около 80 км, что затрудняет практическое применение подобных схем шифрования.

Одно из решений по противостоянию PNS-атаке заключается в том, что состояния внутри базиса можно сделать неортогональными, затрудняя тем самым для перехватчика их различение даже при знании используемого базиса. На этой технологии построен протокол SARG04 со следующей конфигурацией сигнальных состояний:

$$\begin{aligned} |0^a\rangle &= \cos\frac{\eta}{2}|0\rangle + \sin\frac{\eta}{2}|1\rangle, \qquad |0^b\rangle = \sin\frac{\eta}{2}|0\rangle - \cos\frac{\eta}{2}|1\rangle, \\ |1^a\rangle &= \cos\frac{\eta}{2}|0\rangle - \sin\frac{\eta}{2}|1\rangle, \qquad |1^b\rangle = \sin\frac{\eta}{2}|0\rangle + \cos\frac{\eta}{2}|1\rangle, \end{aligned} \tag{2}$$

Здесь угол между состояниями внутри каждого базиса равен η. Так как теперь перехватчику надостаточно задержать у себя по одному фотону каждого импульса, ему приходится применять измерение над дополнительными фотонами сразу после их получения. Поскольку протокол использует два базиса, перехватчику потребуется минимум два фотона для проведения измерений в обоих базисах. Однако и в этом случае из-за неортогональности состояний велика вероятность, что перехватчик не получи достоверной информации о состоянии, поэтому можно считать, что протокол SARG04 может быть атакован с помощью PNS-атаки только в том

случае, когда перехватчик имеет возможность блокировать все трёхфотонные компоненты. Это существенно увеличивает критическую длину канала связи, делая протокол SARG04 более защищенным против PNS-атаки.

Вторая глава посвящена исследованию криптографической стойкости протокола SARG04. Сначала в ней приводятся критерии секретности ключей в квантовой криптографии, на основании которых можно делать выводы о стойкости того или иного протокола. Чаще всего используется следующее выражение для финальной длины секретного ключа при исходной длины последовательности n:

$$\frac{r}{n} = I(A;B) - I(A;E),$$

где $I(A;B)$ и $I(A;E)$ — соответственно пропускная способность классического канала между Алисой и Бобом и квантового канала между Алисой и Евой.

Задача исследования стойкости сводится, таким образом, к оценке информации Евы $I(A;E)$ через наблюдаемую на приёмной стороне ошибку q. Наиболее эффективной стратегией Евы является коллективная атака, которая сводится к следующему. Для каждого передаваемого состояния $|\psi\rangle$ Ева готовит вспомогательное состояние $|e\rangle$ и подвергает совместное состояние $|\psi \otimes e\rangle$ унитарному преобразованию U_E, в результате чего полученное состояние Ψ оказывается сцепленым. Действие преобразования U_E на сигнальные состояния (2) можно выразить как

$$\begin{aligned}
U_E(|0_a \otimes e\rangle) &= |\widetilde{0_a}\rangle = \sqrt{1-p}|0_a\rangle|\psi_{0_a}\rangle + \sqrt{p}|0_b\rangle|\theta_{0_a}\rangle,\\
U_E(|1_a \otimes e\rangle) &= |\widetilde{1_a}\rangle = \sqrt{1-p}|1_a\rangle|\psi_{1_a}\rangle + \sqrt{p}|1_b\rangle|\theta_{1_a}\rangle,\\
U_E(|0_b \otimes e\rangle) &= |\widetilde{0_b}\rangle = \sqrt{1-p}|0_b\rangle|\psi_{0_b}\rangle + \sqrt{p}|0_a\rangle|\theta_{0_b}\rangle,\\
U_E(|1_b \otimes e\rangle) &= |\widetilde{1_b}\rangle = \sqrt{1-p}|1_b\rangle|\psi_{1_b}\rangle + \sqrt{p}|1_a\rangle|\theta_{1_b}\rangle,
\end{aligned} \tag{3}$$

где из соображений унитарности U_E и симметрии состояния $|\psi_{i_j}\rangle$ можно выразить через 3 параметра — p, α и β, где

$$\langle\psi_{0_a}|\psi_{0_b}\rangle = \langle\psi_{1_a}|\psi_{1_b}\rangle = \cos\alpha, \langle\theta_{0_a}|\theta_{0_b}\rangle = \langle\theta_{1_a}|\theta_{1_b}\rangle = \cos\beta,$$

а параметры связаны соотношением

$$1 - 2p = (1-p)\cos\alpha + p\cos\beta, \tag{4}$$

которое оставляет лишь два параметра в распоряжении Евы, определяющие унитарный оператор U_E.

После измерения на стороне Боба и отбрасывания исходов с неопределенным результатом его ошибка оказывается равной

$$Q = \frac{p}{(1-p)\sin^2\eta + p\cos^2\eta + p}. \tag{5}$$

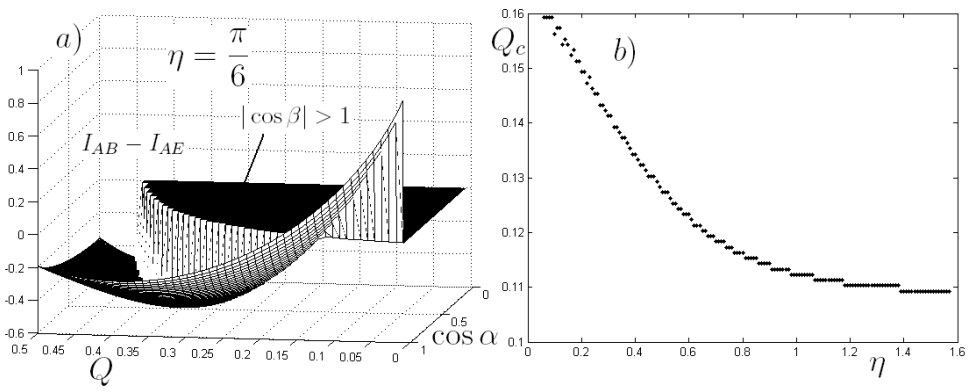

Рис. 1: a) Зависимость разности между информацией информацией легитимных пользователей и Евы от параметров (Q, α) при величине угла $\eta = \frac{\pi}{6}$. Плоскостью показана область, где параметры Q и α несовместны, то есть из соотношения (4) вытекает, что $|\cos\beta| > 1$, и решения отсутствуют. b) зависимость критической ошибки от угла η между состояниями внутри базисов.

После измерения на стороне Боба и публичном согласовании базисов Ева имеет последовательность частичных состояний вида

$$\begin{aligned} \rho^E_{0_a} &= \gamma|\psi_{0_a}\rangle\langle\psi_{0_a}| + \delta|\theta_{0_a}\rangle\langle\theta_{0_a}| - c(|\psi_{0_a}\rangle\langle\theta_{0_a}| + |\theta_{0_a}\rangle\langle\psi_{0_a}|), \\ \rho^E_{1_a} &= \gamma|\psi_{1_a}\rangle\langle\psi_{1_a}| + \delta|\theta_{1_a}\rangle\langle\theta_{1_a}| - c(|\psi_{1_a}\rangle\langle\theta_{1_a}| + |\theta_{1_a}\rangle\langle\psi_{1_a}|). \end{aligned} \tag{6}$$

и можно говорить о квантовом канале между Алисой и Евой, пропускная способность которого даётся величиной Холево (1). Собственные значения оператора $\frac{1}{2}(\rho^E_{0_a} + \rho^E_{1_a})$, необходимые для нахождения величины Холево, легко найти как корни алгебраического уравнения четвёртой степени: методы решения подобных уравнений хорошо известны.

На рис.1, a) показан график разности между информацией легитимных пользователей и Евы в зависимости от параметров (Q, α) при величине угла $\eta = \frac{\pi}{6}$. На рис.1, b) показана зависимость критической ошибки, до которой возможно распространение секретного ключа, от угла η между состояниями внутри базисов.

В **третей главе** рассматривается протокол квантового распределения ключей с фазово-временным кодированием и его криптографическая стойкость. Этот протокол использует три временных окна (что соответствует пространству кутритов), которые обозначаются как $|1\rangle, |2\rangle$ и $|3\rangle$, и 4 различных базиса, которые разделены на две группы: левые и правые. Состояния из левой пары базисов являются комбинациями первого и второго временного окна, а состояния правой пары базисов — суперпозициями второго и третьего окон (рис. 2).

Существуют две версии протокола с фазово-временным кодированием. В ортогональной версии состояния внутри каждого базиса взаимно

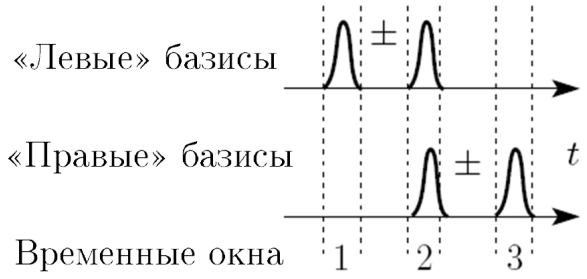

Рис. 2: Конфигурация сигнальных состояний в протоколе с фазово-временным кодированием

ортогональны и задаются соотношением

$$\begin{aligned}
|0^{+L}\rangle &= \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle), \quad |0^{+R}\rangle = \frac{1}{\sqrt{2}}(|2\rangle + |3\rangle),\\
|1^{+L}\rangle &= \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle), \quad |1^{+R}\rangle = \frac{1}{\sqrt{2}}(|2\rangle - |3\rangle),\\
|0^{\times L}\rangle &= \frac{1}{\sqrt{2}}(|1\rangle + i|2\rangle), \quad |0^{\times R}\rangle = \frac{1}{\sqrt{2}}(|2\rangle + i|3\rangle),\\
|1^{\times L}\rangle &= \frac{1}{\sqrt{2}}(|1\rangle - i|2\rangle), \quad |1^{\times R}\rangle = \frac{1}{\sqrt{2}}(|2\rangle - i|3\rangle).
\end{aligned} \tag{7}$$

В неортогональной же версии конфигурация состояний в левом и правом базисах идентична конфигурации векторов в протоколе SARG04, и сигнальные состояния равны

$$\begin{aligned}
|0^{L_a}\rangle &= \cos\frac{\eta}{2}|1\rangle + \sin\frac{\eta}{2}|2\rangle, \quad |0^{R_a}\rangle = \cos\frac{\eta}{2}|2\rangle + \sin\frac{\eta}{2}|3\rangle,\\
|1^{L_a}\rangle &= \cos\frac{\eta}{2}|1\rangle - \sin\frac{\eta}{2}|2\rangle, \quad |1^{R_a}\rangle = \cos\frac{\eta}{2}|2\rangle - \sin\frac{\eta}{2}|3\rangle,\\
|0^{L_b}\rangle &= \sin\frac{\eta}{2}|1\rangle - \cos\frac{\eta}{2}|2\rangle, \quad |0^{R_b}\rangle = \sin\frac{\eta}{2}|2\rangle - \cos\frac{\eta}{2}|3\rangle,\\
|1^{L_b}\rangle &= \sin\frac{\eta}{2}|1\rangle + \cos\frac{\eta}{2}|2\rangle, \quad |1^{R_b}\rangle = \sin\frac{\eta}{2}|2\rangle + \cos\frac{\eta}{2}|3\rangle,
\end{aligned} \tag{8}$$

Измерение на приемной стороне происходит в случайно выбранном базисе. В ортогональной версии это ортогональное измерение, дающее достоверный исход при отсутствии помех в канале. В неортогональной версии это измерение с тремя исходами, которое способно дать несовместный исход (вероятность которого зависит от угла между состояниями), но также не даёт ошибки при отсутствии помех в канале связи. Однако важным отличием от SARG04 в обеих версиях является возможность получения ещё одного исхода — отсчета в контрольном временном окне. Для сигналов из левых базисов это третье верменное окно, а для состояний из правых базисов — первое.

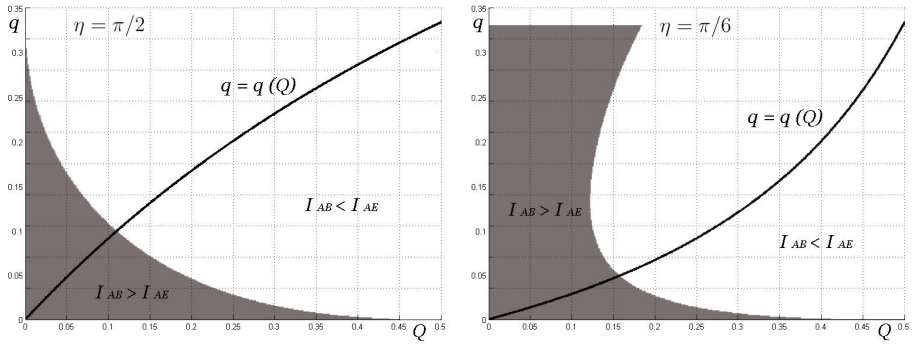

Рис. 3: Области секретности протокола квантового распределения ключей с фазово-временным кодированием. Левая половина соответствует ортогональному случаю, правая — значению угла $\eta = \pi/6$. Оптимальной атаке отвечает зависимость $q(Q)$, показанная линией.

После пересылки и измерений всех сигнальных состояний, как и в протоколе BB84, проводятся этапы коррекции ошибок и усиления секретности.

Для обоснования стойкости протокола в однофотонном режиме рассматривается унитарное преобразование Евы и строится его зависимость от наблюдаемых на приёмной стороне параметров — битовой ошибки и количества контрольных отсчётов. В силу сходства в конфигурации сигнальных состояний с протоколом SARG04, многие выкладки оказываются аналогичными. Результатом введния дополнительного параметра на приемной стороне (контрольных отсчётов) оказывается то, что теперь длина ключа оценивается по двум параметрам, и наблюдается область секретности на плоскости (Q,q) битовой ошибки Q и контрольных временных отсчётов q. Области секретности для ортогональной версии протокола и для его неортогональной версии (при значении угла η между сигнальными состояниями внутри базиса, равном $\pi/6$) приведены на рис.3.

Стойкость протокола против PNS-атаки исследуется следующим образом. Рассмотрим, при каких условиях перехватчик может получить всю информацию о передаваемых состояниях. Протокол использует 4 базиса с неортогональными состояниями в каждом из них, поэтому для получения точной информации придется провести измерение с тремя исходами сразу во всех базисах, а для этого потребуется, чтобы испульс содержал как минимум пять фотонов. Так как и в этом случае вероятность совместных исходов во всех измерениях мала, можно считать, что протокол перестаёт быть стойким против PNS-атаки в том случае, когда перехватчик имеет возможность блокировать все посылки, содержащие от одного до пяти фотонов.

На рис.4 приведены зависимости критических длин ключа от максимального количества фотонов, которые могут быть блокированы

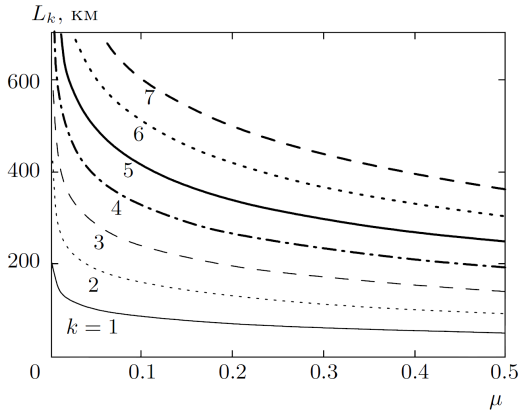

Рис. 4: Зависимости длины линии L_k от среднего числа фотонов μ в когерентном состоянии, начиная с которых Ева может блокировать посылки, содержащие k фотонов.

перехватчиком. Таким образом, при значении интенсивности порядка $\mu \approx 0.2$ критическая длина линии связи для протокола с фазово-временным кодированием превосходит 300 км.

В **четвертой главе** происходит построение квантовой схемы оптимального подслушивания для протокола BB84 и протокола с фазово-временным кодированием. Построение такой схемы позволяет дать представление о физической реализации схем квантовых вычислений, а также оценить масштабы требований к техническому арсеналу перехватчика.

Сначала схема строится в логическом базисе, который не привязан к физической природе входящих в него элементов. Затем происходит переход к физическому базису, на котором описывается техническая реализация всех основных составляющих квантовой схемы.

Для построения логической схемы достаточно выбрать конкретные состояния перехватчика в качестве состояний $|e\rangle$, $|\psi_i\rangle$ и $|\theta_i\rangle$ в (3), затем выписать явный вид унитарного оператора, производящего над выбранными состояниями преобразование (3), после чего построить квантовую схему из доступных элементарных преобразований. Заметим, что как состояния, так и преобразование перехватчика могут выбираться несколькими способами.

Как известно, любое многокубитовое унитарное преобразование может быть сведено к последовательному применению и одного двухкубитового преобразования «контролируемое НЕ» (CNOT), которое действует по закону

$$\begin{aligned} CNOT|\overline{00}\rangle &= |\overline{00}\rangle, \\ CNOT|\overline{01}\rangle &= |\overline{01}\rangle, \\ CNOT|\overline{10}\rangle &= |\overline{11}\rangle, \\ CNOT|\overline{11}\rangle &= |\overline{10}\rangle, \end{aligned} \tag{9}$$

Ввиду громоздкости здесь не будут приводиться все детали построения квантовой схемы. Основными однокубитовыми преобразованиями в ней являются поворот $R(\alpha)$ на угол α, операция Адамара H, смена фазы $P_i(\varphi)$ у i-й позиции кубита на угол φ и «размазывание» амплитуды с коэффициентом Q. Матрицы операторов перечисленных вентилей таковы:

$$R(\alpha) = \begin{pmatrix} \cos_\alpha & \sin_\alpha \\ -\sin_\alpha & \cos_\alpha \end{pmatrix}, \qquad H = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$
$$P_0(\varphi) = \begin{pmatrix} e^{i\varphi} & 0 \\ 0 & 1 \end{pmatrix}, \qquad Q = \begin{pmatrix} \sqrt{1-Q} & \sqrt{Q} \\ \sqrt{Q} & -\sqrt{1-Q} \end{pmatrix}, \tag{10}$$

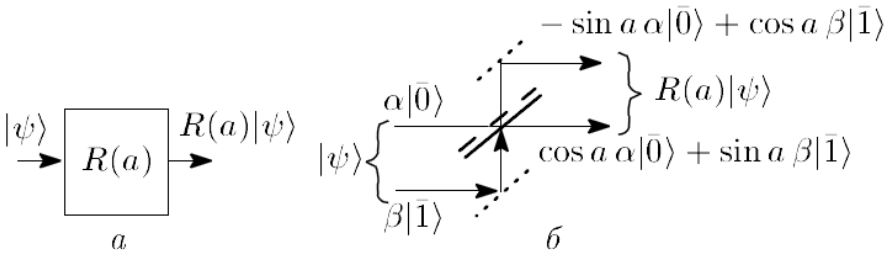

Рис. 5: Пример преобразования квантовых состояний — a) формальное обозначение квантового вентиля поворота, b) физическая реализация квантового вентиля.

В качестве примера физической реализации рассмотрим поворот на угол α — $R(\alpha)$. Схема реализации этого преобразования показана на рис.5. Физическая структура преобразований такова, что для каждого значения кубита используется свой квантовый канал: так, значению $|0\rangle$ соответствует верхний канал, а значению $|1\rangle$ — нижний. Исходное состояние кубита, таким образом, представляется суперпозицией состояний, идущих по двум физическим каналам. Поворот реализуется асимметричным светоделителем, показатель отражения которого равен $\sin\alpha$.

Переход к физическому базису требует проведения следующих шагов: разведения амплитуд, отвечающих разным базисным состояниям и последующее приведение их к одному временному интервалу, целью которого является возможность возникновения интерференци, необходимая для применения квантовых вентилей.

Наибольшие сложности в практическом построении подобной схемы атаки связаны с реализацией оператора CNOT. Это объясняется тем, что для такого преобразования требуется гамильтониан специального вида, который не встречается в природе. Поэтому в настоящее время все практически реализуемые вентили CNOT носят не детерминистический, а вероятностный характер. Учитывая общее число подобных элементов в схеме (около ста),

можно оценить конечную вероятность успешной работы всей схемы. Таким образом, задача оптимального прозрачного подслушивания протокола с фазово-временным кодированием является существенно более сложной, чем подслушивание протокола BB84.

Пятая глава посвящена увеличению критической ошибки протоколов квантового распределения ключей с помощью классической предварительной обработки данных. Эта обработка происходит после публичного согласования базисов и раскрытия части последовательности для оценки ошибки. На этом этапе Алиса и Боб, напомним, находятся в состоянии классического канала связи с известной им вероятностью ошибки q, в то время как Алиса и Ева находятся в состоянии классически-квантового (c-q) канала связи, максимальная пропускная способность которого может быть вычислена по приведённой выше схеме.

Классическая предварительная обработка данных заключается в том, что Алиса объединяет свои биты с одинаковыми значениями в блоки длины N, а затем открыто сообщает Бобу позиции битов каждого блока, не раскрывая при этом их значения. Если все биты в блоке совпали, то этот блок используется в качестве одного бита в новой последовательности символов, в противном же случае все позиции, соответствующие блоку, отбрасываются. Это сокращает длину последовательности, но способно уменьшить информацию перехватчика, что в конечном итоге влечет к увеличению длины секретного ключа.

Обозачим как $\rho_{0,OK}$ и $\rho_{0,Err}$ состояния Евы при посылке сигнала 0 в случае соответственно верного и ошибочного исхода измерения Боба. Аналогично состояния $\rho_{1,OK}$ и $\rho_{1,Err}$ попадают в распоряжение Евы при посылке сигнала 1. Если предварительная обработка данных не была произведена, то Ева стоит перед задачей различения операторов $\rho_0^E = (1-q)\rho_{0,OK} + q\rho_{0,Err}$ и $\rho_1^E = (1-q)\rho_{1,OK} + q\rho_{1,Err}$. В случае же объединения сигналов в блоки Ева должна будет отличить состояния

$$\begin{aligned} \rho_0^E &= \frac{(1-q)^N}{(1-q)^N+q^N}\rho_{0,OK}^{\otimes N} + \frac{q^N}{(1-q)^N+q^N}\rho_{0,Err}^{\otimes N} \\ \rho_0^E &= \frac{(1-q)^N}{(1-q)^N+q^N}\rho_{0,OK}^{\otimes N} + \frac{q^N}{(1-q)^N+q^N}\rho_{1,Err}^{\otimes N} \end{aligned} \tag{11}$$

Так как ошибка на стороне Боба равна $Q = \frac{q^N}{(1-q)^N+q^N}$, то длина финального ключа оказывается равной

$$\frac{r}{n} = 1 - h(Q) - \chi(\{\frac{1}{2},\frac{1}{2}\},\{\rho_0^E,\rho_1^E\}).$$

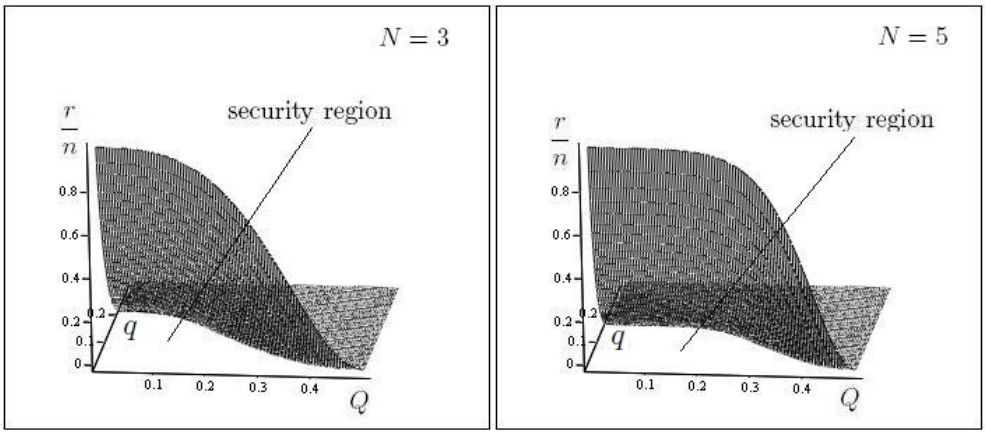

Рис. 6: Области секретности (отвечают положительным значениям длины ключа $\frac{r}{n}$) в зависимости от наблюдаемых параметров (Q, q) при величине блоков $N = 3$ и $N = 5$

На рис.6 показана область секретности протокола с фазово-временным кодированием при использовании предварительной обработки данных с длиной блоков, равной 3 и 5. Как видно из этих риснуков, предварительная обработка данных способна существенно расширить область секретности протокола.

В **заключении** приведены основные результаты работы, которые заключаются в следующем:

- Исследована стойкость протокола SARG04 в однофотонном режиме: получены значения критической ошибки на приёмной стороне при произвольном значении угла между сигнальными состояниями внутри базиса. При состояниях внутри базиса, близким к ортогональным, значение критической ошибки, как и ожидалось, близко к 11%, а при уменьшении значения угла оно увеличивается и приближается к 16%.

- Найдена область секретности протокола с фазово-временным кодированием на плоскости параметров, наблюдаемых на приёмной стороне: битовой ошибки и количества отсчётов в контрольных временных окнах. При отсутствии контрольных отсчётов распределение ключей оказывается возможным при битовой ошибке, не превышающей 50%, что соответствует теоретическому пределу.

- Получена зависимость критической длины линии связи от среднего числа фотонов в лазерном импульсе для неортогональной модификации протокола с фазово-временным кодированием. Эта величина существенно превосходит аналогичные значения, полученные для других известных на сегодняшний день протоколов.

- Построена квантовая схема оптимальной однофотонной атаки на протокол с фазово-временным кодированием. Из её построения видно, что задача прозрачного подслушивания этого протокола является существенно более сложной, чем для протокола BB84 и фактически требует наличия в распоряжении перехватчика квантового компьютера.
- Исследован способ увеличения области секретности с помощью классической предварительной обработки сигналов: рассмотрено объединение в блоки битов с одинаковыми значениями при совпадении их значений у легитимных пользователей, что позволяет расширить область секретности.

Публикации автора по теме диссертации

1. Д.А.Кронберг, С.Н.Молотков, *Квантовая схема для оптимального подслушивания квантового распределения ключей с фазово-временным кодированием.//* Журнал экспериментальной и теоретической физики, том 137 вып. 7, 33–66 (2010)
2. Д.А.Кронберг, С.Н.Молотков, *Квантовая схема для оптимального подслушивания протокола BB84 квантового распредления ключей.//* Известия РАН (серия физическая), том 74 вып. 7, 954–960 (2010)
3. Д.А.Кронберг, С.Н.Молотков, *Усиление стойкости фазово-временной квантовой криптографии блочным исправлением ошибок.//* Письма в Журнал экспериментальной и теоретической физики, том 92 вып. 7, 539–544 (2010)
4. Д.А.Кронберг, С.Н.Молотков, *Двухпараметрическая квантовая криптография на временных сдвигах, устойчивая к атаке с расщеплением по числу фотонов.//* Журнал экспериментальной и теоретической физики, том 136 вып. 4, 650–683 (2009)
5. Д.А.Кронберг, С.Н.Молотков, *Квантовое распределение ключей в однофотонном режиме с неортогональными состояниями внутри базиса.//* Письма в Журнал экспериментальной и теоретической физики, том 89 вып. 7, 432–438 (2009)
6. D.A.Kronberg, S.N.Molotkov, *Robustness of quantum cryptography: SARG04 key-distribution protocol.//* Laser Physics, volume 19 number 4, 884–893 (2009)