МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»

Кафедра оптики и биофотоники

Анализ уязвимостей квантовых протоколов распределения ключей

АВТОРЕФЕРАТ МАГИСТЕРСКОЙ РАБОТЫ

Студента 2 курса 2223 группы
направления 03.04.02 «Физика»
Института физики
Кашичкина Александра Олеговича

Научный руководитель
доцент кафедры оптики и биофотоники,

к.ф.-м.н., доцент И.В. Федосов

Заведующий кафедрой

зав. кафедрой, д.ф.-м.н., профессор В.В. Тучин

Саратов 2023 год

Введение

Квантовая криптография, также известная как метод генерации квантовых ключей, представляет собой инновационное исследовательское направление, которое сегодня находится в фокусе внимания [1-6]. Ее главной целью является обеспечение абсолютно секретной передачи данных между двумя пользователями, которые обычно называются Алисой (отправителем) и Бобом (получателем). Основная преимущественная особенность квантовой криптографии заключается в использовании фундаментальных законов квантовой механики для обеспечения конфиденциальности и защиты передаваемых данных от незаметного перехвата третьими лицами.

Использование одиночных квантовых объектов в качестве носителей информации приводит к неизбежному и необратимому изменению квантовых состояний этих объектов в случае любой попытки перехвата. Это позволяет обнаружить факт вторжения [7]. Целью исследований в области квантовой криптографии является создание всемирной инфраструктуры распределения ключей, которая включает использование волоконных линий связи.

Тема надежности квантовой криптографии и возможности квантового хакинга вызывает значительный интерес и активно исследуется в настоящее время [6,8,9]. Наша исследовательская задача состоит в анализе возможностей злоумышленника для взлома квантового протокола. Важнейшим аспектом является эффективность и условие незаметности злоумышленника.

Изучена и проанализирована атака типа PNS, а также реализована атака этого типа в программе. Получены результаты секретности и эффективности Евы, для случая, когда у Евы нет возможности реализовать квантовый канал без потерь до Боба. Исследования этой атаки актуальны и по сей день [6,10,11,12].

Наше исследование нацелено на выявление новых методов и подходов, которые помогут повысить надежность квантовой криптографии и сделать ее более устойчивой к потенциальным квантовым атакам. Для этого была разработана программа для анализа этих уязвимостей.

Мы надеемся, что данная работа будет способствовать расширению понимания о надежности квантовой криптографии и обеспечении безопасности в сфере криптографии в целом. Рассмотрены атаки на уязвимые части квантовых протоколов и на их улучшенные версии, где эти атаки успешно обнаруживаются. В работе выполнена симуляция работы квантовых алгоритмов для учебной демонстрации. А также внедрен гибкий функционал для моделирования хакинга, благодаря которому мы сможем наглядно оценить возможности злоумышленника.

В настоящем исследовании представлена комплексная теоретическая основа, необходимая для понимания основ квантовой криптографии и метода квантового распределения ключей. Однако, наша основная фокусировка лежит на практической части исследования, где мы активно применяем полученные знания для создания симуляции протокола.

Мы уделяем особое внимание разработке и оптимизации симуляционной модели протокола, чтобы обеспечить реалистичное и точное воспроизведение его работы. Наша цель - предоставить практические рекомендации и примеры, которые могут быть использованы и адаптированы в реальных квантовых системах. Особенность данной программы является возможность использования ее для расчетов и анализа эффективности и секретности злоумышленника. Тем самым даем возможность почувствовать себя в роли Евы. Отлично подходит для лабораторной работы и использования в качестве подпрограммы в других проектах.

Этот подход делает наше исследование особенно ценным, поскольку оно сочетает теоретические основы с практическими примерами,

что способствует более полному и глубокому пониманию квантовой криптографии и метода квантового распределения ключей.

Работа состоит из определений, введения, 2 глав, заключения и списка используемой литературы

Основное содержание работы

В первой главе приводится теория по квантовым протоколам и атакам на эти протоколы.

Протокол Беннета-Брассара (BB84), предложенный в 1984 году, имеет особое значение среди различных протоколов QKD, так как его доказательство безопасности служит отправной точкой для многих других протоколов. В протоколе BB84 две стороны, скажем, Алиса и Боб, хотят совместно использовать одну и ту же последовательность битов в качестве секретного ключа для криптографических целей. Протокол должен работать в публичной среде, где подслушивающее лицо, скажем, Ева, может подслушивает или даже перехватывает сигналы, передаваемые по квантовому каналу. Несмотря на несколько модификаций, предложенных в других местах, основная процедура протокола, основана на подготовке и измерении квантовых состояний. За последние десятилетия была создана множество протоколов квантовой криптографии, которые основаны на передаче информации путем кодирования в состояниях одиночных фотонов. Некоторые из этих протоколов включают BB84, B92, BB84 с шестью состояниями, асимметричный BB84, E91, SARG04, дифференциально-фазовый сдвиг, когерентный односторонний и их модификации.

Таблица 1 – краткий обзор черт протоколов

Название протокола	Характерные черты
Протокол BB84	Преимущество в том, что при однофотонном источнике света минимальное количество ошибок.

Протокол BB92	Преимуществом является необходимость двух источников вместо четырех. А недостатком - удвоенное количество операций передачи фотонов для генерации ключа.
Протокол COW	COW протокол является одним из самых последних практических протоколов КРК (2005г.), но безусловные доказательства безопасности все еще остаются нереализованными.
Протокол SSP	SSP упрощает обнаружение ошибок, поскольку перехватчик должен выбрать правильный базис из трех возможных.
Протокол EPR	Этот протокол использует отброшенные ключи для обнаружения присутствия Евы с помощью неравенства Белла.
Протокол KMB09	Претензии на большое расстояние, квантовая связь с высоким уровнем ошибок.
Протокол SARG04	После процесса просеивания приемнику остается четверть необработанных битов, которых по сравнению с BB84 гораздо меньше.
Протокол S09	Безопасная передача данных по общедоступному каналу.

Последовательность действий в протоколе BB84:

1) На этапе приготовления состояний Алиса случайным образом выбирает один из указанных базисов (2), а зачем случайно выбирает значение бита: ноль или один, и в соответствии с этим выбором посылает один из четырёх сигналов:

2) При посылке каждого из этих сигналов Алиса запоминает свой выбор базиса и выбор бита, что приводит к появлению двух случайных битовых строк на её стороне.

3) Боб, получает каждый из присланных Алисой сигналов, приводит над ними случайным образом одно из двух измерений, каждая из которых способна дать достоверный результат из-за ортогональности в состоянии внутри каждого базиса Алисы:

4) В результате у него указывается две строки: с тем, какие из базисов были выбраны для измерения, и с исходами этих измерений.

5) И так, после передачи всех состояний и проведения измерений Алиса и Боб имеют по две строки. Здесь происходит согласование базисов: по открытому каналу Алиса и Боб объявляют друг другу свои строки с выбором базисов, и они выбрасывают посылки, в которых их базисы не совпали. Важно отметить, что если Алиса и Боб используют одинаковый базис при передаче и измерении квантовых состояний, то в случае отсутствия помех в канале связи и без вмешательства со стороны перехватчика их результаты и соответствующие битовые строки будут совпадать. После этапа согласования базисов и в идеальном канале связи Алиса и Боб должны иметь одинаковые битовые строки.

При разработке и применении квантовых систем связи необходимо учитывать эту особенность и применять соответствующие методы и техники для снижения вероятности появления множественных фотонов и минимизации их воздействия на передаваемую информацию. Это позволяет обеспечить более надежную и безопасную передачу данных в реальных условиях. В связи с этим злоумышленник может перехватить сигнал, в котором более 1 фотона, и получить доступ к части ключа при этом оставаясь незамеченным. Данный вид действий, осуществляемых перехватчиком, получил название атаки с разделением по числу фотонов (PNS-атаки).

Зная, какие импульсы содержат больше 1 фотона, Ева может заблокировать те из них, которые содержат лишь один фотон, а для многофотонных импульсов переслать Бобу один из фотонов, произведя измерения над остальными. Блокировка одночастотных импульсов может быть компенсирована использованием более совершенного канала для транспортировки оставшихся импульсов на сторону Боба. По предложению легитимные пользователи не имеют полного контроля над квантовым каналом связи, и Ева может заменить на свой канал, в котором затухание, в котором меньше, чем в изначальном канале. В перспективе Ева может использовать для пересылки оставшихся фотонов Бобу канал, не дающий никаких потерь. Поэтому при достаточной доле многофотонных импульсов на стороне источника и потерях в канале связи действия Евы не могут быть детектированы.

Покажем, каким образом операция разделения фотонов может быть применена для взлома протоколов BB84. Ева может без каких-либо последствий узнать число фотонов в каждом из импульсов. Атака строится следующим образом: если импульс содержит лишь один фотон, Ева его блокирует, в противном случае она оставляет в своей квантовой памяти (для ее реализации достаточно иметь обычную линию задержки) один из фотонов, пересылая остальные Бобу по-своему более совершенному каналу (в идеале по каналу вообще без потерь). После операции согласования базисов, проводящийся по открытому каналу (в идеале по каналу вообще без потерь). После операции согласованию базисов, проводящийся по открытому каналу, Ева получает всю необходимую информацию для достоверного различения имеющихся у нее фотонов, а значит, способна узнать весь ключ не будучи обнаруженной. Это делает протокол BB84 полностью незащищенным перед PNS-атакой.

Вторая глава описывает разработанную программу и анализ полученных данных в ходе тестирования протокола.

Программа, разработанная в среде программирования LabVIEW, эмулирует работу идеального квантового протокола BB84 и атаку PNS. Протокол BB84 является фундаментальным для множества квантовых протоколов и по сей день. Оригинальный протокол является полностью безопасным для передачи ключа. Это множество раз было доказано, однако при его физической реализации, появляется множество угроз к безопасности из-за физической реализации протокола. Каждая такая угроза рождает новую усовершенствованную версию протокола (BB92, SARG04, BB84 Decoy state). Поэтому алгоритм протокола BB84 разработан в виде конечного автомата.

Конечный автомат — это некоторая абстрактная модель, содержащая конечное число состояний чего-либо. Используется для представления и управления потоком выполнения каких-либо команд. Эта модель отлично подходит для расширения и дополнения изначального алгоритма. Наш конечный автомат имеет множество модулей и переходов между этими модулями. Каждый модуль описывает определённый этап квантового протокола.

Современные квантовые протоколы ориентируется на предположение том, что Еве известно все о Алисе и Бобе и она обладает передовыми технологиями. Из этого предположения, при разработке алгоритмов для Евы, мы добавили ей большой функционал для взлома системы, например Ева способна в процентном соотношении знать какой базис выбрала Алиса. Это было сделано для детального анализа ключа, полученного Евой и Бобом.

Оригинальный протокол представлен для строго однофотонных источников света, но на практике чаще всего используют ослабленное лазерное излучение. Лазерное излучение имеет пуассоновское распределение по числу фотонов, поэтому с некоторой вероятностью, зависящей от числа

фотонов, в когерентных состояниях могут встречаться сигналы, в которых присутствуют два или более фотонов. Поэтому мы добавили возможность включения алгоритма не для однофотонных источников света, а для ослабленного лазера. В связи с этим реализовано пуассоновское распределение, с возможностью выбора среднего числа фотонов в импульсе. В таком случае у Евы появляется возможность незаметно перехватывать фотоны для той части импульсов, где их более одного и получать часть ключа (PNS).

Программа включает в себя следующие модули:

1. Распределение Пуассона
2. Базис Алисы.
3. Базис Боба
4. Базис Евы
5. Бит Алисы
6. Бит Боба
7. Бит Боба, с присутствием Евы
8. Бит Евы
9. Статистика

Переходы автомата схематично показаны на Рис. 2.

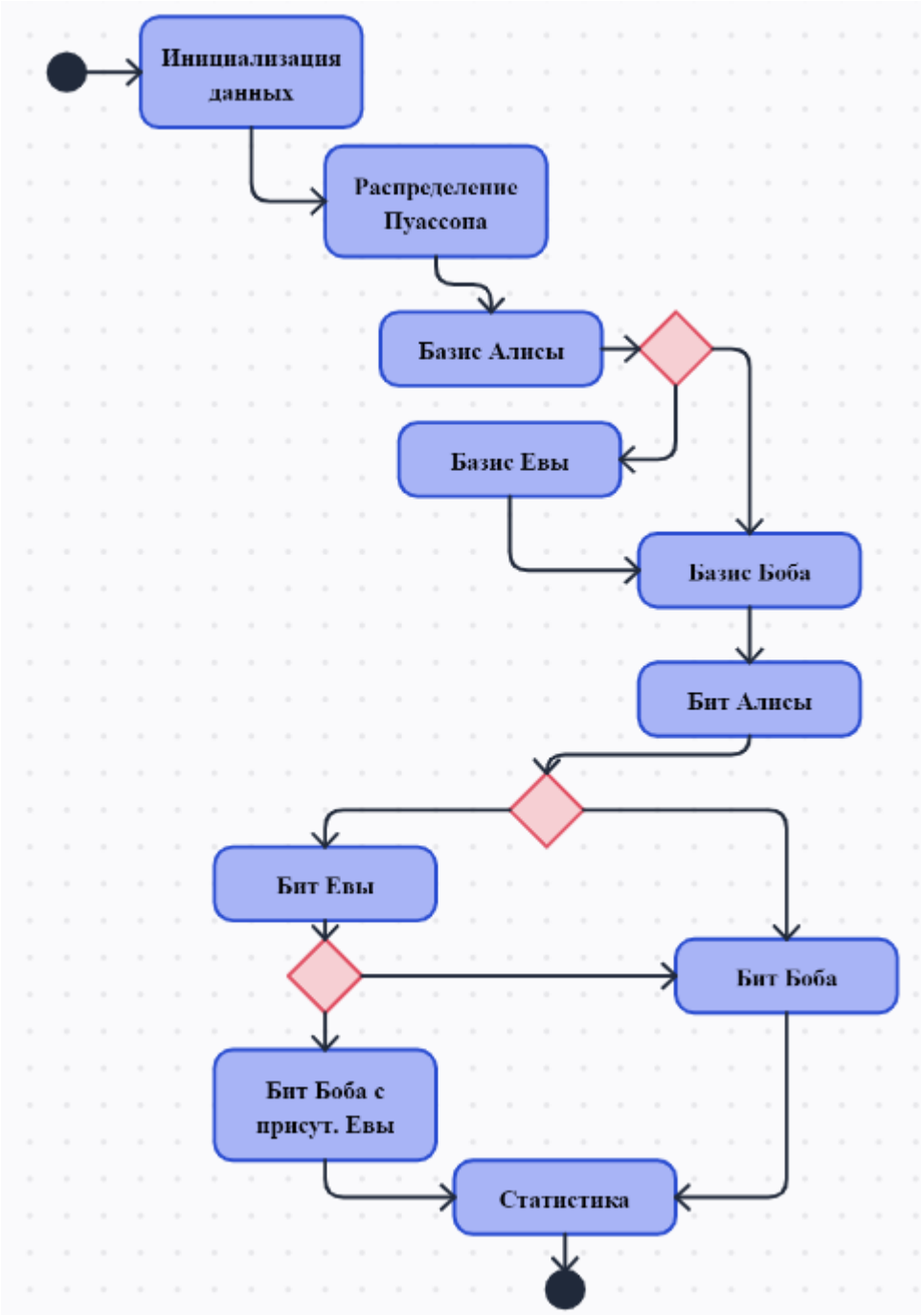

Рис. 2 – Схема переходов конечного автомата

С помощью данной программы мы можем проверить секретность квантового протокола, если на него осуществлялась атака PNS.Рассмотрен случай, когда Алиса и Боб меняются местами и соответственно Ева, старающаяся быть поближе к Алисе, чтобы получать полноценную партию посылок от нее, начинает вносить значительные изменения в протокол, если Алиса и Боб поменялись местами. Для начала Алиса и Боб пробуют обменяться ключами, изучить квантовый канал, когда в нем не присутствовала

Ева, и получить среднее значение потери фотонов, процент ошибок и длину ключа. В протоколе PNS, Ева должна блокировать все 1 фотонные посылки, в связи с этим у боба в конечном итоге будет намного меньше полученных посылок. С помощью программы мы можем управлять процентом блокировки однофотонных импульсов. Мы решили изучить варианты разной настройки злоумышленника, чтобы понять, при каких обстоятельствах Ева останется незамеченной. Для начала мы рассчитали среднее значения для процента ошибок, потерянных фотонов и длины ключа. Графики. Начальные настройки программы были таковыми: среднее число фотонов в импульсе было равно 1, коэффициент поглощения волокна равен 0,2 дБ/км, коэффициент передачи квантового канала равен 0,9, длина квантового канала равна 10км, процент ложного срабатывания в детекторах Боба составляет 15% и число посылок, отправленных Алисой, равнялось 2000. Среднее число длины ключа равен 42. Средний процент ошибок равно 3. Среднее число потерянных фотонов равно 1560, из 2000 переданных фотонов.

Из полученных данных мы приходим к выводам, что Ева для случая, когда она подключилась близко к Алисе будет самым благоприятным. Процент ошибок падает с 4% до 2%, что входит в зону погрешности протокола без злоумышленника. Количество потеряных фотонов детектором Боба возрастает с 1537 до 1729. Она сможет блокировать до 30% однотонных посылок и при этом не будет обнаружена. К тому же эффективность ключа Евы будет в среднем 48%. Из всех вариантов, пожалуй, этот будет самым благоприятным для Евы, но при этом есть риск того, что Алиса и Боб поменяются местами, что вызовет обнаружение злоумышленника.

Нейтральный случай размещения Евы, пожалуй, самый оптимальный. Процент ошибок в среднем равен 3, а количество потерянных фотонов для Боба возрастает с 1561 до 1704. В среднем Ева может заблокировать до 20% единичных фотонов, не рискуя быть обнаруженной. В целом такой вариант событий самый безопасный для Евы, хотя эффективность ключа, полученного

Евой, падает с 48% до 35% по сравнению с случаем, когда Ева находится в близи источника импульсов Алисы.

И наконец рассмотрим вариант, когда Ева подключилась рядом с Бобом. Процент ошибок остался, как и в других случаях, около 3%. В этом случае Боб теряет от 1266 до 1672 фотонов. Ева может выйти из этого положения, если будет блокировать только 10% единичных импульсов и эффективность Евы будет в районе 10%.

В итоге у Евы есть два варианта, чтобы остаться не обнаруженной для остальных. Первый вариант вычислить середину квантового канала и там подключится. Пробовать блокировать не более 20% процентов единичных посылок, но при этом иметь небольшой шанс, что Алиса и Боб ее обнаружат. Второй вариант, уменьшить блокировку однотонных импульсов до 10% и иметь возможность подключаться в любой точке квантового канала. В этом случае эффективность ключа Евы будет варьироваться от 45 до 30 процентов.

Заключение

В работе получены следующие результаты: разработан алгоритм эмуляции квантового протокола распределения ключей BB84; алгоритм реализован виде специально разработанной программы для персонального компьютера; исследована эффективность и вероятность обнаружения PNS атаки при различных вариантах ее реализации.

Благодаря модульной структуре программы, она, может быть, в дальнейшем адаптирована для эмуляции более сложных протоколов квантового распределения ключа и различных вариантов атак. Графический интерфейс пользователя и средства для вывода отчетов и графиков делают разработанную программу удобным инструментом для оценки надежности протоколов квантового распределения ключа на этапе первоначального проектирования, так как позволяют количественно оценить влияние

физических характеристик реальных источников, детекторов и линии передачи на надежность реализации протокола.

Кроме того, разработанная программа может использоваться в учебных целях для выполнения практических и лабораторных работ по квантовой криптографии студентами высших учебных заведений.

Список использованной литературы

1. Su, HY. Simple analysis of security of the BB84 quantum key distribution protocol. Quantum Inf Process 19, 169 (2020).
2. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)
3. Diffie, W., Hellman, M.: New directions in cryptography. IEEE Trans. Inf. Theory 22, 644–654 (1976)
4. Merkle, R.: Secure communications over insecure channels. Commun. ACM 21, 294–299 (1978)
5. Rivest, R.L., Shamir, A., Adleman, L.M.: A method of obtaining digital signatures and public-key cryptosystems. Commun. ACM 21, 120–126 (1978)
6. Li W. et al. High-rate quantum key distribution exceeding 110 Mb s–1 //Nature Photonics. – 2023. – Т. 17. – №. 5. – С. 416-421.
7. 2. Gisin N. et al. Quantum cryptography // Rev. Mod. Phys. 2002. V. 74. P. 145–195.
8. Morrison, C.L., Pousa, R.G., Graffitti, F. et al. Single-emitter quantum key distribution over 175 km of fibre with optimised finite key rates. Nat Commun 14, 3573 (2023).
9. Jain, N., Chin, HM., Mani, H. et al. Practical continuous-variable quantum key distribution with composable security. Nat Commun 13, 4740 (2022).
10. Kulik S. P., Kravtsov K. S., Molotkov S. N. Experimental resources

needed to implement photon number splitting attack in quantum cryptography //Laser Physics Letters. – 2022. – Т. 19. – №. 2. – С. 025203.

11. Chen X., Chen L., Yan Y. Detecting a Photon-Number Splitting Attack in Decoy-State Measurement-Device-Independent Quantum Key Distribution via Statistical Hypothesis Testing //Entropy. – 2022. – Т. 24. – №. 9. – С. 1232.
12. Chen X. M., Chen L., Yan Y. L. Detecting the possibility of a type of photon number splitting attack in decoy-state quantum key distribution //Chinese Physics B. – 2022. – Т. 31. – №. 12. – С. 120304.