Федеральное государственное автономное образовательное учреждение высшего образования «Московский физико-технический институт (национальный исследовательский университет)»

УТВЕРЖДЕНО
и.о. директора физтех-школы физики и исследований им. Ландау
А.А. Воронов

Рабочая программа дисциплины (модуля)

по дисциплине: Квантовая криптография
по направлению: Прикладные математика и физика
профиль подготовки: Общая и прикладная физика
Физтех-школа физики и исследований им. Ландау
Физтех-кластер академической и научной карьеры
курс: 1
квалификация: магистр

Семестр, формы промежуточной аттестации: 2 (весенний) - Экзамен

Аудиторных часов: 30 всего, в том числе:
лекции: 30 час.
семинары: 0 час.
лабораторные занятия: 0 час.

Самостоятельная работа: 30 час.

Подготовка к экзамену: 30 час.

Всего часов: 90, всего зач. ед.: 2

Программу составил: Д.А. Кронберг, канд. физ.-мат. наук

Программа обсуждена на заседании Физтех-кластера академической и научной карьеры 04.06.2020

Аннотация

Курс посвящен основным методам доказательства стойкости протоколов квантовой криптографии. Эти знания охватывают постановку задачи секретной передачи данных, введение критериев секретности протоколов квантового распределения ключей, изучение наиболее «чистого» протокола ЭПР-состояний и сведение к нему ряда других протоколов. Даются представления об обеспечении независимости протоколов квантовой криптографии от использования аппаратуры и квантовых аналогов ряда энтропий Реньи, которые участвуют в оценке стойкости схем квантовой криптографии.

1. Цели и задачи

Цель дисциплины

дать студентам знания об основных методах доказательства стойкости протоколов квантовой криптографии. Эти знания охватывают постановку задачи секретной передачи данных, введение критериев секретности протоколов квантового распределения ключей, изучение наиболее «чистого» протокола ЭПР-состояний и сведение к нему ряда других протоколов. Даются представления об обеспечении независимости протоколов квантовой криптографии от использования аппаратуры и квантовых аналогов ряда энтропий Реньи, которые участвуют в оценке стойкости схем квантовой криптографии.

Задачи дисциплины

-овладение математическим аппаратом классической криптографии;

-исследование методов обоснования стойкости протоколов квантовой криптографии;

-изучение квантовых аналогов энтропий Реньи;

-изучение независимых от аппаратуры схем квантовой криптографии.

2. Перечень формируемых компетенций

Освоение дисциплины направлено на формирование следующих компетенций:

Код и наименование компетенции	Индикаторы достижения компетенции
УК-6 Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	УК-6.1 Умеет решать задачи собственного личностного и профессионального развития, определять и реализовывать приоритеты совершенствования собственной деятельности
	УК-6.2 Оценивает свою деятельность, соотносит цели, способы и средства выполнения деятельности с её результатами
ОПК-1 Владеет системой фундаментальных научных знаний в области физико-математических наук	ОПК-1.1 Знает и способен использовать в профессиональной деятельности фундаментальные научные знания в области физико-математических наук
	ОПК-1.2 Способен обобщать и критически оценивать опыт и результаты научных исследований в области профессиональной деятельности
	ОПК-1.3 Понимает междисциплинарные связи в области математики и физики и способен их применять при решении задач профессиональной деятельности
ОПК-2 Имеет представление об актуальных проблемах науки и техники в области своей профессиональной деятельности, способен на научном языке формулировать профессиональные задачи	ОПК-2.1 Имеет представление о современном состоянии исследований в рамках тематической области своей профессиональной деятельности
	ОПК-2.3 Владеет профессиональной терминологией, используемой в современной научно-технической литературе, обладает навыками устного и письменного изложения результатов научной деятельности в рамках профессиональной коммуникации
ОПК-3 Способен выбирать и (или)	ОПК-3.1 Способен анализировать задачу, планировать пути решения, предлагать и комбинировать способы решения

разрабатывать подходы к решению типовых и новых задач в области профессиональной деятельности, учитывая особенности и ограничения различных методов решения	ОПК-3.2 Способен использовать исследовательские методы при решении новых задач, применяя знания в различных областях науки (техники)
	ОПК-3.3 Владеет аналитическими и вычислительными методами решения, понимает и учитывает на практике границы применимости получаемых решений
ОПК-5 Способен и готов к повышению квалификации, профессиональному росту и руководству коллективом в сфере своей профессиональной деятельности, толерантно воспринимая социальные, этнические, конфессиональные и культурные различия	ОПК-5.3 Стремится к получению новых знаний, профессиональному и личностному росту
ПК-1 Способен ставить, формализовывать и решать задачи, в том числе разрабатывать и исследовать математические модели изучаемых явлений и процессов, системно анализировать научные проблемы, получать новые научные результаты	ПК-1.1 Способен находить, анализировать и обобщать информацию об актуальных результатах исследований в рамках тематической области своей профессиональной деятельности
	ПК-1.3 Способен применять теоретические и (или) экспериментальные методы исследований к конкретной научной задаче и интерпретировать полученные результаты
ПК-2 Способен самостоятельно или в качестве члена (руководителя) малого коллектива организовывать и проводить научные исследования и их апробацию	ПК-2.1 Способен планировать и проводить научные исследования самостоятельно или в составе научного коллектива
	ПК-2.2 Способен проводить апробацию результатов научно-исследовательской работы посредством публикации научных статей и участия в конференциях

3. Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

-математические принципы классической криптографии;

-семейство энтропий Реньи в классическом и квантовом случае, их свойства;

-методы сведения обоснования стойкости протоколов квантовой криптографии к стойкости протокола ЭПР;

-методы обоснования стойкости схем квантовой криптографии в условиях влияния перехватчика на оборудование;

-основы квантовых кодов исправления ошибок.

уметь:

-ставить задачи обеспечения секретности для ряда протоколов квантовой криптографии;

-обосновывать секретность некоторых протоколов квантовой криптографии;

-строить простые схемы для обеспечения стойкости протоколов квантовой криптографии в условиях недоверия к оборудованию.

владеть:

-математическим аппаратом классической криптографии;

-математическим аппаратом энтропий одночастичных и составных квантовых состояний;

-методами обеспечения стойкости протоколов для независимости от оборудования.

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины (модуля) и трудоемкости по видам учебных занятий

№	Тема (раздел) дисциплины	Трудоемкость по видам учебных занятий, включая самостоятельную работу, час.			
		Лекции	Семинары	Лаборат. работы	Самост. работа

1	Обзорное занятие	5			5
2	Протокол ЭПР квантового распределения ключей (протокол Экерта)	5			5
3	Условная квантовая энтропия и её роль в обосновании стойкости	5			5
4	Квантовые коды исправления ошибок, стойкость протокола BB84, доказательство Шора-Прескилла	5			5
5	Построение схем квантовой криптографии, независимых от аппаратуры	3			3
6	Семейство квантовых энтропий Реньи	3			3
7	Обоснование стойкости протоколов квантовой криптографии через энтропийные соотношения неопределенностей	4			4
Итого часов		30			30
Подготовка к экзамену		30 час.			
Общая трудоёмкость		90 час., 2 зач.ед.			

4.2. Содержание дисциплины (модуля), структурированное по темам (разделам)

Семестр: 2 (Весенний)

1. Обзорное занятие

План курса, основные современные проблемы квантовой криптографии

2. Протокол ЭПР квантового распределения ключей (протокол Экерта)

Неравенства Белла, CHSH-игра. Протоколы Экерта и BBM92, сведение протокола BB84 к распределению сцепленных состояний

3. Условная квантовая энтропия и её роль в обосновании стойкости

Условная энтропия, роль её отрицательных значений для сцепленных состояний. Обоснование отсутствия информации перехватчика при наличии сцепленного состояния у легитимных пользователей.

4. Квантовые коды исправления ошибок, стойкость протокола BB84, доказательство Шора-Прескилла

Классические линейные коды коррекции ошибок, синдромное декодирование. Квантовые коды коррекции ошибок и их применение для увеличения сцепленности между удаленными пользователями. CSS-коды. Этапы сведения протокола BB84 к измерению сцепленных состояний: протокол Ло-Чу, протокол CSS-кодов.

5. Построение схем квантовой криптографии, независимых от аппаратуры

Понятие независимой от аппаратуры квантовой криптографии (MDI QKD, DI QKD), использование эффекта Хонга-О-Манделя для распределения ключей.

6. Семейство квантовых энтропий Реньи

Относительная энтропия, её свойства. Квантовая относительная энтропия. Энтропия Реньи и её применение в квантовой криптографии

7. Обоснование стойкости протоколов квантовой криптографии через энтропийные соотношения неопределенностей

Энтропийные соотношения неопределенностей и их использование в квантовой криптографии. Связь с традиционными соотношениями неопределенностей. Обоснование стойкости протокола BB84.

5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

1. Необходимое оборудование для лекций и практических занятий: доска, мел, тряпка. Желательно также применение мультимедийного оборудования (проектор), для лучшей организации лекции.
2. Необходимое программное обеспечение: не требуется.
3. Обеспечение самостоятельной работы: наличие учебников и задачников по курсу квантовой криптографии.

6.Перечень рекомендуемой литературы

Основная литература

1. Квантовая информация и квантовые вычисления [Текст] : в 2 т/Дж. Прескилл , -М. : Регулярная и хаотическая динамика ; Ижевск, 2011
2. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. М. : Мир, 2009.

Дополнительная литература

1. Введение в квантовую теорию информации [Текст] : [лекции для студентов вузов] / А. С. Холево ; Независимый Моск. ун-т ; Высший колледж математ. физики .— М : МЦНМО, 2002 .— 128 с.

7. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

xxx.lanl.gov

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень необходимого программного обеспечения и информационных справочных систем (при необходимости)

Нет.

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Работа с учебной и научной литературой является главной формой самостоятельной работы и необходима при подготовке к контрольной работе, экзамену. Она включает проработку лекционного материала – изучение рекомендованных источников и литературы по тематике лекций. Конспект лекции должен содержать реферативную запись основных вопросов лекции, предложенных преподавателем схем (при их демонстрации), основных источников и литературы по темам, выводы по каждому вопросу. Конспект должен быть выполнен в отдельной тетради по предмету. В случае возникших затруднений в понимании учебного материала следует обратиться к другим источникам, где изложение может оказаться более доступным. Необходимо отметить, что работа с литературой не только полезна как средство более глубокого изучения любой дисциплины, но и является неотъемлемой частью профессиональной деятельности будущего выпускника.

ПРИЛОЖЕНИЕ

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

по направлению: Прикладные математика и физика
профиль подготовки: Общая и прикладная физика
Физтех-школа физики и исследований им. Ландау
Физтех-кластер академической и научной карьеры (Фундаментальные проблемы физики квантовых технологий)
курс: 1
квалификация: магистр

Семестр, формы промежуточной аттестации: 2 (весенний) - Экзамен

Разработчик: Д.А. Кронберг, канд. физ.-мат. наук

1. Компетенции, формируемые в процессе изучения дисциплины

Код и наименование компетенции	Индикаторы достижения компетенции
УК-6 Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	УК-6.1 Умеет решать задачи собственного личностного и профессионального развития, определять и реализовывать приоритеты совершенствования собственной деятельности
	УК-6.2 Оценивает свою деятельность, соотносит цели, способы и средства выполнения деятельности с её результатами
ОПК-1 Владеет системой фундаментальных научных знаний в области физико-математических наук	ОПК-1.1 Знает и способен использовать в профессиональной деятельности фундаментальные научные знания в области физико-математических наук
	ОПК-1.2 Способен обобщать и критически оценивать опыт и результаты научных исследований в области профессиональной деятельности
	ОПК-1.3 Понимает междисциплинарные связи в области математики и физики и способен их применять при решении задач профессиональной деятельности
ОПК-2 Имеет представление об актуальных проблемах науки и техники в области своей профессиональной деятельности, способен на научном языке формулировать профессиональные задачи	ОПК-2.1 Имеет представление о современном состоянии исследований в рамках тематической области своей профессиональной деятельности
	ОПК-2.3 Владеет профессиональной терминологией, используемой в современной научно-технической литературе, обладает навыками устного и письменного изложения результатов научной деятельности в рамках профессиональной коммуникации
ОПК-3 Способен выбирать и (или) разрабатывать подходы к решению типовых и новых задач в области профессиональной деятельности, учитывая особенности и ограничения различных методов решения	ОПК-3.1 Способен анализировать задачу, планировать пути решения, предлагать и комбинировать способы решения
	ОПК-3.2 Способен использовать исследовательские методы при решении новых задач, применяя знания в различных областях науки (техники)
	ОПК-3.3 Владеет аналитическими и вычислительными методами решения, понимает и учитывает на практике границы применимости получаемых решений
ОПК-5 Способен и готов к повышению квалификации, профессиональному росту и руководству коллективом в сфере своей профессиональной деятельности, толерантно воспринимая социальные, этнические, конфессиональные и культурные различия	ОПК-5.3 Стремится к получению новых знаний, профессиональному и личностному росту
ПК-1 Способен ставить, формализовывать и решать задачи, в том числе разрабатывать и исследовать математические модели изучаемых явлений и процессов, системно анализировать научные проблемы, получать новые научные результаты	ПК-1.1 Способен находить, анализировать и обобщать информацию об актуальных результатах исследований в рамках тематической области своей профессиональной деятельности
	ПК-1.3 Способен применять теоретические и (или) экспериментальные методы исследований к конкретной научной задаче и интерпретировать полученные результаты
ПК-2 Способен самостоятельно или в качестве члена (руководителя) малого коллектива организовывать и проводить научные исследования и их апробацию	ПК-2.1 Способен планировать и проводить научные исследования самостоятельно или в составе научного коллектива
	ПК-2.2 Способен проводить апробацию результатов научно-исследовательской работы посредством публикации научных статей и участия в конференциях

2. Показатели оценивания компетенций

В результате изучения дисциплины «Квантовая криптография» обучающийся должен:

знать:

-математические принципы классической криптографии;
-семейство энтропий Реньи в классическом и квантовом случае, их свойства;
-методы сведения обоснования стойкости протоколов квантовой криптографии к стойкости протокола ЭПР;
-методы обоснования стойкости схем квантовой криптографии в условиях влияния перехватчика на оборудование;
-основы квантовых кодов исправления ошибок.

уметь:

-ставить задачи обеспечения секретности для ряда протоколов квантовой криптографии;
-обосновывать секретность некоторых протоколов квантовой криптографии;
-строить простые схемы для обеспечения стойкости протоколов квантовой криптографии в условиях недоверия к оборудованию.

владеть:

-математическим аппаратом классической криптографии;
-математическим аппаратом энтропий одночастичных и составных квантовых состояний;
-методами обеспечения стойкости протоколов для независимости от оборудования.

3. Перечень типовых (примерных) вопросов, заданий, тем для подготовки к текущему контролю

Не предусмотрено.

4. Перечень типовых (примерных) вопросов и тем для проведения промежуточной аттестации обучающихся

Перечень контрольных вопросов:

1. Определение относительной квантовой энтропии, специфика квантового случая
2. CHSH-игра, возможности игроков в случае использования сцепленных квантовых состояний
3. Квантовые коды коррекции ошибок, построение кода Стина
4. Основные этапы сведения протокола BB84 к протоколу ЭПР
5. Примеры действий перехватчика при его влиянии на аппаратуру легитимных пользователей
6. Определение квантовых энтропий Реньи, их свойства
7. Энтропийные соотношения неопределенностей, их роль в квантовой криптографии

Примеры контрольных заданий:

1. Посчитать ту или иную энтропии Реньи для данных квантовых состояний
2. Построить квантовый код коррекции ошибок для данных возможных ошибок
3. Посчитать зависимость длины секретного ключа от затухания в линии связи для данного протокола
4. Предложить простые атаки для ряда протоколов квантовой криптографии
5. Обосновать стойкость протокола на ЭПР-состояниях через относительную энтропию

Примеры экзаменационных билетов

Билет 1.

1. Основные этапы сведения протокола BB84 к протоколу ЭПР
2. Посчитать ту или иную энтропии Реньи для данных квантовых состояний

Билет 2.

1. CHSH-игра, возможности игроков в случае использования сцепленных квантовых состояний
2. Построить квантовый код коррекции ошибок для данных возможных ошибок

Билет 3.

1. Примеры действий перехватчика при его влиянии на аппаратуру легитимных пользователей
2. Посчитать зависимость длины секретного ключа от затухания в линии связи для данного протокола

Билет 4.

1. Определение относительной квантовой энтропии, специфика квантового случая

2. Предложить простые атаки для ряда протоколов квантовой криптографии

Билет 5.

1. Квантовые коды коррекции ошибок, построение кода Стина

2. Обосновать стойкость протокола на ЭПР-состояниях через относительную энтропию

Критерии оценивания

- оценка "отлично (10)" выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений;

- оценка "отлично (9)" выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений;

- оценка "отлично (8)" выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение применять их на практике при решении конкретных задач, и правильное обоснование принятых решений;

- оценка "хорошо (7)" выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применить полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;

- оценка "хорошо (6)" выставляется студенту, если он знает материал, грамотно и по существу излагает его, умеет применить полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;

- оценка "хорошо (5)" выставляется студенту, если он знает материал, по существу излагает его, умеет применить полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;

- оценка "удовлетворительно (4)" выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировка базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом владеющему основными разделами учебной программы, необходимыми для дальнейшего обучения и способному применять полученные знания по образцу в стандартной ситуации;

- оценка "удовлетворительно (3)" выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировка базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом владеющему фрагментарно основными разделами учебной программы, необходимыми для дальнейшего обучения и способному применять полученные знания по образцу в стандартной ситуации;

- оценка "неудовлетворительно (2)" выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении типовых практических задач;

- оценка "неудовлетворительно (1)" выставляется студенту, который не знает формулировок основных понятий дисциплины.

5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Во время проведения экзамена обучающиеся могут пользоваться только программой дисциплины.

При проведении экзамена обучающемуся предоставляется 1 астрономический час на подготовку. Опрос обучающегося по билету на устном экзамене не должен превышать двух астрономических часов.