Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования «Новосибирский национальный исследовательский
государственный университет» (Новосибирский государственный университет, НГУ)

Факультет информационных технологий

Согласовано
Декан ФИТ НГУ
_____ М.М. Лаврентьев
«28» сентября 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОСНОВЫ ПОСТ-КВАНТОВОЙ КРИПТОГРАФИИ

Научная специальность: 2.3.5 Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей
Направленность (профиль): Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей

Форма обучения: очная

Разработчик:
ассистент кафедры теоретической кибернетики ММФ,
кандидат физико-математических наук А.В. Куценко

Заведующий кафедрой систем информатики ФИТ
доктор физико-математических наук М.М. Лаврентьев

Ответственный за образовательную программу:
заведующий кафедрой систем информатики ФИТ,
доктор физико-математических наук М.М. Лаврентьев

Новосибирск 2022

Аннотация к рабочей программе дисциплины
«Основы пост-квантовой криптографии»

Дисциплина «Основы пост-квантовой криптографии» реализуется в рамках программы аспирантуры по научной специальности 2.3.5 «Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей» (профилю): Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей по очной форме обучения на русском языке.

Дисциплина «Основы пост-квантовой криптографии» входит в блок элективных дисциплин, реализуемых в рамках программы аспирантуры и направлена на формирование знаний и умений, связанных с осуществлением эффективного криптоанализа известных алгоритмов асимметричного шифрования, с необходимостью в разработке новых, квантово-устойчивых криптографических систем.

Целью курса является ознакомление обучающихся с современными подходами к созданию пост-квантовых криптографических систем, а также методами квантового криптоанализа. В рамках курса будут изучены математические основы квантовой информатики и её приложения в криптографии и криптоанализе. Проводится разбор известных квантовых атак, в частности, основанных на использовании квантовых алгоритмов Шора, Гровера. Также детально изучаются основные подходы к построению криптографических систем, потенциально устойчивых к атакам, использующим квантовый компьютер. Особое внимание уделяется криптосистемам, основанным на теории решёток, а также кодов, исправляющих ошибки.
Перечень основных разделов дисциплины: понятие квантового бита, пространство квантовых состояний, квантовые вычисления: базовые наборы вентилей, квантовые алгоритмы нахождения порядка и периода, квантовый алгоритм поиска в неупорядоченном списке и его применение в криптоанализе, задача нахождения кратчайшего вектора в решётке, пост-квантовая криптография на решётках: криптосистема NTRU, пост-квантовая криптография на кодах, исправляющих ошибки: криптосистемы Мак-Элиса и Нидеррайтера.

Общий объем дисциплины – 2 зачетных единицы (72 часа). Из которых лекции составляют 24 часа, практические занятия 8 часов, самостоятельная работа 38 часов.

Правила аттестации по дисциплине. Промежуточная аттестация по дисциплине «Основы пост-квантовой криптографии» проводится в виде сдачи дифференцированного зачета. Дифференцированный зачет проводится в устной форме, по билетам. Билет выбирается обучающимся случайным образом. При подготовке ответа на вопросы билета не разрешается использование каких-либо источников информации.

1. Результаты освоения дисциплины:

- знать модель квантовых вычислений и основные алгоритмы квантового криптоанализа симметричных и асимметричных шифров;
- знать основные подходы к построению и анализу пост-квантовых криптографических систем.

2. Трудоемкость дисциплины по видам учебной деятельности

Трудоемкость дисциплины – 2 з.е. (72 ч)
Форма промежуточной аттестации: диф.зачет.

№	Вид деятельности	Количество часов
1	Лекции, час.	24
2	Практические занятия, час.	8
3	Лабораторные занятия, час	
4	Занятий в контактной форме без учета промежуточной аттестации, час, из них	32
5	в электронной форме, час.	
6	аудиторных занятий, час.	32
7	из них в активной и интерактивной форме, час.	
8	консультаций, час.	
9	Самостоятельная работа, час.	38
10	Всего, ч	72

3. Содержание дисциплины

Лекции (24 ч)

Наименование тем и их содержание	Объем час
Математические основы квантовой информатики	
1. Чистые и смешанные квантовые состояния, пространство квантовых состояний	2
2. Квантовые измерения, квантовая запутанность	4
Основы квантового криптоанализа	
3. Математическая модель квантовых вычислений	2
4. Квантовый криптоанализ асимметричных шифров	4
5. Квантовый криптоанализ симметричных шифров.	2
Основные направления постквантовой криптографии	
6. Криптография, основанная на кодах, исправляющих ошибки	4

7. Криптография, основанная на решётках	4
8. Стойкость алгоритмов постквантовой криптографии	2

Практические занятия (8 ч)

Наименование тем и их содержание	Объем час
Математические основы квантовой информатики	
1. Вычисление численных характеристик квантовых состояний	2
Основы квантового криптоанализа	
2. Построение квантовых схем с помощью вентилей из базовых наборов	2
3. Квантовое преобразование Фурье и алгоритмы, основанные на его использовании	2
Основные направления постквантовой криптографии	
4. Вычислительно трудные задачи из теории решёток и кодов, исправляющих ошибки	2

Самостоятельная работа аспиранта 38 часов

Перечень занятий на СР аспиранта	Объем час
1. История развития квантовой механики. Чистое и смешанное квантовое состояние. Квантовые измерения общего вида, проективные измерения (измерения фон Неймана). Теорема о неразличимости неортогональных квантовых состояний. Теорема о невозможности копирования произвольного квантового состояния. Запутанность (сцепленность) квантовых состояний.	6
2. Эволюция квантового состояния во времени. Уравнение Шрёдингера. Вентиль Адамара. Универсальные наборы квантовых вентилей. Алгоритм Дойча. Алгоритм Дойча-Йожа. Модели Q1 и Q2 квантовых вычислений.	8
3. Алгоритмы Шора решения задач факторизации и дискретного лагарифмирования. Алгоритм Саймона. Квантовая атака на криптосистему Even-Mansour. Алгоритм Гровера. Квантовая атака на режим шифрования CBC-MAC.	8
4. Коды, исправляющие ошибки. Линейный код. Задача декодирования линейного кода. Криптосистема Мак-Элиса. Криптосистема Нидеррайтера. Атака на основе процедуры Information set decoding.	8
5. Основные сведения из теории решеток. Задача нахождения ближайшего вектора (CVP). Задача нахождения кратчайшего вектора в решетке (SVP). Задача обучения с ошибками в кольце. Криптосистема NTRU, известные атаки на нее.	8

4. Перечень учебно-методических материалов, необходимых для изучения дисциплины (модуля)

1. В.Г. Сербо, И.Б. Хриплович. Квантовая механика. Учебное пособие / Новосиб. гос. ун-т. Новосибирск : Редакционно-издательский центр НГУ, 2008. 273 с. (53 экз.)

5. Перечень учебных изданий, необходимых для освоения дисциплины

1. Д.И. Блохинцев. Основы квантовой механики. Учебное пособие для студентов высших учебных заведений / Изд. 5-е, перераб. Москва : Наука, 1976. 664 с.
(34 экз.)

6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Для реализации дисциплины «Основы пост-квантовой криптографии» используются специальные помещения:

1. Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля, промежуточной и итоговой аттестации;

2. Помещения для самостоятельной работы обучающихся;

3. Лаборатории;

4. Помещения для хранения и профилактического обслуживания учебного оборудования.

Учебные аудитории укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду НГУ

Для проведения занятий лекционного типа предлагаются следующие наборы демонстрационного оборудования и учебно-наглядных пособий:

- комплект лекций-презентаций по темам дисциплины;

Материально-техническое обеспечение образовательного процесса по дисциплине для аспирантов из числа лиц с ограниченными возможностями здоровья осуществляется согласно «Порядку организации и осуществления образовательной деятельности по

образовательным программам для инвалидов и лиц с ограниченными возможностями здоровья в Новосибирском государственном университете

7. Оценочные средства для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

7.1 Порядок проведения текущего контроля и промежуточной аттестации по дисциплине

Промежуточная аттестация:

Промежуточная аттестация по дисциплине «Основы пост-квантовой криптографии» проводится в виде сдачи дифференцированного зачета.

Дифференцированный зачет проводится в устной форме, по билетам. Билет выбирается обучающимся случайным образом. При подготовке ответа на вопросы билета не разрешается использование каких-либо источников информации. В процессе ответа обучающегося на вопросы билета преподаватель может задавать дополнительные вопросы по темам дисциплины. Результаты промежуточной аттестации определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

Описание критериев и шкал оценивания результатов освоения дисциплины:

Результат освоения дисциплины	**Критерии оценивания результатов освоения дисциплины**	**Шкала оценивания**
знать модель квантовых вычислений и основные алгоритмы квантового криптоанализа симметричных и асимметричных шифров	Вопросы диф.зачета категорий 1,2 Имеет достаточно глубокие знания о модели квантовых вычислений и основных алгоритмах квантового криптоанализа симметричных и асимметричных шифров	Отлично
	Вопросы диф.зачета категорий 1,2 знает модель квантовых вычислений и основные алгоритмы квантового криптоанализа симметричных и асимметричных шифров	Хорошо
	Вопросы диф.зачета категорий 1,2 имеет представление о	удовлетворительно

	модели квантовых вычислений и основных алгоритмах квантового криптоанализа симметричных и асимметричных шифров	
	Вопросы диф.зачета категорий 1,2 имеет фрагментарное представление о модели квантовых вычислений и основных алгоритмах квантового криптоанализа симметричных и асимметричных шифров	неудовлетворительно
знать основные подходы к построению и анализу постквантовых криптографических систем	Вопросы диф.зачета категорий 3,4 Имеет достаточно глубокие знания об основных подходах к построению и анализу постквантовых криптографических систем	Отлично
	Вопросы диф.зачета категорий 3,4 знает основные подходы к построению и анализу постквантовых криптографических систем	Хорошо
	Вопросы диф.зачета категорий 3,4 имеет представление об основных подходах к построению и анализу постквантовых криптографических систем	удовлетворительно
	Вопросы диф.зачета категорий 3,4 имеет фрагментарное представление об основных подходах к построению и анализу постквантовых криптографических систем	неудовлетворительно

Результаты итоговой аттестации, проводимой в форме кандидатского экзамена, определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение итоговой аттестации.

Типовые контрольные задания и иные материалы, необходимые для оценки результатов освоения дисциплины (оценочные материалы)

7.1. Перечень вопросов диф.зачета, структурированный по категориям

Категория	Формулировка вопроса
Категория 1	Вопрос 1. Чистое и смешанное квантовое состояние.
	Вопрос 2. Пространство квантовых состояний.
	Вопрос 3. Квантовые измерения общего вида, проективные измерения (измерения фон Неймана).
	Вопрос 4. Теорема о невозможности копирования произвольного квантового состояния.
	Вопрос 5. Эволюция квантового состояния во времени
Категория 2	Вопрос 6. Универсальные наборы квантовых вентилей
	Вопрос 7. Алгоритмы Шора решения задач факторизации и дискретного лагарифмирования.
	Вопрос 8. Алгоритм Саймона.
	Вопрос 9. Алгоритм Гровера.
	Вопрос 10. Квантовая атака на криптосистему Even-Mansour.
	Вопрос 11. Квантовая атака на режим шифрования CBC-MAC.
Категория 3	Вопрос 12. Коды, исправляющие ошибки. Линейный код.
	Вопрос 13. Линейный код. Задача декодирования линейного кода.
	Вопрос 14. Криптосистема Мак-Элиса.
	Вопрос 15. Криптосистема Нидеррайтера.
	Вопрос 16. Структурная атака.
	Вопрос 17. Атака на основе процедуры Information set decoding.
Категория 4	Вопрос 18. Задача нахождения ближайшего вектора (CVP).
	Вопрос 19. Задача нахождения кратчайшего вектора в решетке (SVP).
	Вопрос 20. Задача обучения с ошибками в кольце.
	Вопрос 21. Криптосистема NTRU.
	Вопрос 22. Известные атаки на криптосистему NTRU.