

Магистерская программа

«Квантовая криптография и квантовая связь»

1. Руководитель программы.

Молотков Сергей Николаевич, доктор физико-математических наук, профессор, руководитель сектора квантовой криптографии Центра квантовых технологий физического факультета МГУ имени М.В. Ломоносова.

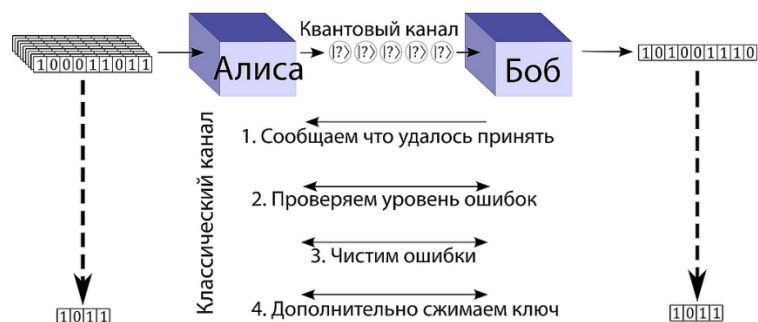
2. Кафедра, реализующая магистерскую программу.

Центр квантовых технологий физического факультета МГУ имени М.В. Ломоносова.

3. Краткая аннотация магистерской программы.

Цель этой магистерской программы – подготовка специалистов по вопросам квантового распределения ключей и квантовой связи – молодого и активно развивающегося направления современных квантовых технологий. В настоящее время квантовым технологиям уделяется огромное внимание, так как использование квантовых объектов для таких практических применений, как вычисления, моделирование больших систем и криптография, позволяет принципиально выйти за рамки традиционного классического понимания данных проблем. Наиболее состоявшейся областью, уже на деле продемонстрировавшей свои преимущества, является квантовая криптография – единственный способ обмена секретными ключами, безусловно гарантирующий их секретность.

Квантовая криптография по своей сути очень междисциплинарна: она сочетает в себе и глубокое использование квантовой механики, и продвинутую математику с теорией информации, а также необходимость применять многие инженерные навыки из области оптической передачи данных. Все это требуется знать в достаточном объеме, чтобы не просто копировать чьи-то идеи, а генерировать новые и их реализовывать на практике. В связи с этим, команда разработчиков в нашем Центре сильно заинтересована в талантливых и разносторонне образованных студентах. Поскольку и само направление и эта магистерская программа очень молоды, при желании, каждый успешно прошедший эту программу, может быть тесно вовлечен в разработку практических систем квантовой криптографии, которые в настоящее время активно выходят на конкурентный рынок высокотехнологичной продукции.

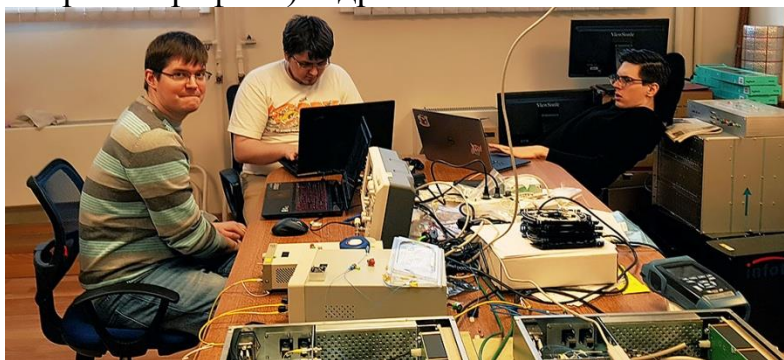


1. Грубая схема квантового распределения ключей.



2. Квантовый генератор случайных чисел

В рамках программы, будут рассмотрены как вопросы классической теории информации и методов передачи данных, так и изучение в требуемом объеме квантовой теории. В первую часть войдут вопросы кодирования информации и исправления ошибок, классической криптографии, основ цифровых систем связи, некоторые аспекты современных методов разработки цифровых электронных устройств. Вторая часть посвящена основам квантовой оптики, квантовым технологиям в целом, физическим основам квантовой криптографии и изучению известных протоколов квантового распределения ключей. Также будут подробно рассмотрены такие смежные вопросы, как генерация случайных чисел, традиционная криптография, устойчивая к атакам на квантовом компьютере («постквантовая криптография») и др.



3. Команда разработчиков волоконно-оптической системы квантовой криптографии



4. Система квантового распределения ключей по открытому пространству

4. Области науки и профессии, где может применить свои знания выпускник программы.

Программа по квантовой криптографии и квантовой связи уникальна и не имеет аналогов в России. Её ключевой особенностью является включение участников образовательного процесса в разработку реальных коммерческих систем квантовой связи, их включение в опытные команды разработчиков из предприятий-партнеров Консорциума. Такой подход к обучению позволяет получить на выходе программы специалистов, готовых сразу же участвовать в разработках и коммерциализации квантовых систем связи на лидирующих ролях, что безусловно обеспечивает их востребованность.

5. Перечень обязательных дисциплин магистерской программы

- Квантовая криптография

- Основы квантовой оптики
- Теория кодирования и ее приложения к криптографии
- Дополнительные главы математики
- Протоколы квантовой криптографии: от теории к практике
- Основы волоконно-оптических систем связи
- Физические генераторы случайных чисел
- Физические методы взлома систем квантовой связи
- Введение в теорию вероятностей
- Постквантовая криптография: алгоритмические методы шифрования в эпоху квантовых компьютеров
- Квантовая томография
- Теория квантовых алгоритмов и квантовая вычислительная сложность

6. Предприятия, научные организации, на которых обучающийся может проходить научно-исследовательскую практику.

Прохождение научно-исследовательской практики возможно как в команде разработчиков Центра квантовых технологий Физфака МГУ, так и на предприятиях, тесно связанных с деятельностью консорциума при Центре: ОАО «Инфотекс», НПО «Криптософт», МГТУ им. Баумана и др.

7. Контактные данные для вопросов

к.ф.-м.н., снс, руководитель отдела образовательных программ Центра квантовых технологий физического факультета МГУ Владимирова Юлия Викторовна, yu.vladimirova@physics.msu.ru.