Моделирование релятивистской системы квантового распределения ключей

Промежуточный отчет о выполнении дипломной работы

Большаков Роман Алексеевич, группа 523
Научный руководитель профессор Молотков С. Н.

Московский государственный университет имени М.В. Ломоносова
Факультет вычислительной математики и кибернетики
Кафедра суперкомпьютеров и квантовой информатики

19 декабря 2014

Постановка задачи

Требуется смоделировать релятивистский протокол квантового распределения ключей в виде программного средства, визуализирующего различные состояния протокола, реализующей его аппаратуры, а также окружающей среды с учетом известных на данный момент физических взаимодействий и ограничений.

Актуальность релятивистского протокола

В области квантовой криптографии уже имеется много наработок и разработано достаточное число протоколов. Но все они подвержены техническим ограничениям современного уровня развития технологий, а именно имеется две основные проблемы: лазеры не могут испустить ровно один фотон, в каналах связи возможны потери.
Релятивистский протокол делает эти проблемы несущественными, так как кроме законов квантовой механики он опирается еще и на специальную теорию относительности с ее ограничением на максимальную скорость передачи информации.

Актуальность моделирования, состояние в области

На декабрь 2014 года не имеется никаких других средств визуализации и моделирования указанного протокола. Однако наличие таких средств принципиально важно как для лучшего понимания работы самого протокола, так и для поиска возможных сложностей в реализации, которые дешевле обнаружить на этапе компьютерного моделирования, чем на этапе постройки прототипа работающей установки.

Суть выполненной работы

За полгода было сделано:

- исследование и разбор словесного описания протокола,
- поиск существующих решений моделирования (безрезультатно),
- выбор средства и технологии разработки,
- создание первой версии программы визуализации.

Основные результаты

В разработанном программном средстве

- реализована подсистема визуализации времени и пространства протокола,
- реализована подсистема внутренней работы протокола,
- смоделировано поведение протокола по словесному описанию в идеальном случае,
- смоделировано поведение протокола в условиях наличия перехватчика в канале связи при различных его действиях.

Что еще должно быть сделано

Для завершения работы над программной частью нужно

- улучшить физическую составляющую подсистемы моделирования,
- исправить различные ошибки в программном коде,
- улучшить представление данных на экране,
- внести в сценарии для моделирования больше нестандартных ситуаций.

Производственнная практика

Производственнная практика проходится в ЗАО «Лаборатория Касперского».
Тема практики: создание средств автоматизированного развертывания и тестирования программного обеспечения.
Руководитель практики от организации: Штаут Золтан

Производственнная практика

В ходе производственной практики была настроена и развернута система автоматической сборки программных продуктов, разрабатываемых в Лаборатории, а так же система их автоматизированного тестирования. Для автоматизированного тестирования были созданы и настроены специальные тестовые окружения, кроме того, был написан и постоянно поддерживается в актуальном состоянии набор автотестов, собственно и производящих функциональное тестирование продуктов.

Спасибо за внимание