

УДК 535.8, 535.015

## РАЗРАБОТКА ЛАБОРАТОРНОГО СТЕНДА: ИЗУЧЕНИЕ ОСНОВ КВАНТОВОЙ КРИПТОГРАФИИ НА БАЗЕ СИСТЕМ ФАЗОВОГО КОДИРОВАНИЯ В ОТКРЫТОМ ПРОСТРАНСТВЕ.

Демидов Д.В. (Университет ИТМО)

Научный руководитель - научный сотрудник лаборатории квантовых коммуникаций  
Савельева С.В. (Университет ИТМО)

Работа посвящена экспериментальному изучению основ квантовой криптографии с фазовым кодированием в открытом пространстве. Разработана лабораторная установка на базе интерферометра Маха-Цендера, которая собрана полностью из элементов объемной оптики. Предложена система обработки получаемых данных и исследовано влияние параметров системы на их точность.

**Введение.** Стремление общества сделать передачу информации безопасной и открытия в области квантовой физики привели к развитию квантовой криптографии, к которой в наше время имеется повышенный интерес. Реализация этого метода защиты информации возможна как в волоконно-оптической линии связи, так и по атмосферному каналу. Первый вариант наиболее распространенный, однако передача ключа в открытом пространстве тоже активно изучается. Одно из основных преимуществ систем квантового распределения ключа по атмосферному каналу – меньше потерь сигнала. Для систем квантовой криптографии разработано несколько протоколов распределения ключа, самый распространенный из которых BB84. В открытом пространстве кодирование по протоколу BB84 возможно по поляризации и по фазе. В работе рассматривается система с фазовым кодированием, которая реализуется на базе интерферометра Маха-Цендера.

**Основная часть.** Для изучения основ квантовой криптографии на базе системы фазового кодирования в открытом пространстве предлагается собрать лабораторную установку с использованием интерферометра Маха-Цендера. Анализ существующих систем помог в выборе схемы реализации лабораторной установки. Световые импульсы генерируются лазерным источником и поступают в интерферометр, который включает в себя два светоделителя. В обоих плечах, отправителя и получателя, находятся фазовые модуляторы. С помощью модулятора отправитель осуществляет кодирование, создавая один из четырех сдвигов фаз ( $0$ ,  $\pi$ , относящихся к одному базису, или  $\pi/2$ ,  $3\pi/2$ , относящихся ко второму базису). Со своей стороны, получатель случайным образом выбирает в каком базисе проводить измерение, чтобы произвести декодирование. Установка полностью состоит из элементов объемной оптики, которые выравниваются таким образом, чтобы минимизировать потери мощности сигнала, попадающего на детектор, относительно мощности излучения лазерного источника. В качестве детектора выступает фотодиод. Осциллограф отображает принятый фотодиодом сигнал и передает данные на компьютер. Программа обрабатывает информацию и на выходе преобразует ее в ключ, состоящий из логических 0 и 1.

**Вывод.** Разработанный лабораторный стенд, выполненный полностью из элементов объемной оптики, позволяет изучать основы квантовой криптографии на базе системы фазового кодирования в открытом пространстве с использованием интерферометра Маха-Цендера.

Демидов Д.В. (автор) \_\_\_\_\_

Савельева С.В. (научный руководитель) \_\_\_\_\_