

Реферат

Объем 100 с., 18 рис., 17 табл., 35 источников, 1 прил.

КВАНТОВОЕ ШИФРОВАНИЕ, КВАНТОВОЕ ХЕШИРОВАНИЕ, КВАНТОВАЯ КРИПТОГРАФИЯ, КВАНТОВЫЙ КОМПЬЮТЕР

В дипломном проекте рассмотрено решение криптографических задач при передаче информации по квантовым сетям.

Объект исследования – методы квантовой передачи и обработки информации.

Предметом исследования являются схемы построения каналов квантовой связи и протоколы квантового шифрования.

Цель работы – анализ технических решений и аппаратных возможностей в области создания квантовых вычислительных систем.

В процессе работы был выполнен литературный обзор по криптографическим приложениям квантовых алгоритмов.

Рассмотрены особенности квантовой передачи информации и изучено применение классических и квантовых алгоритмов, а так же особенности выполнения пошаговых процедур на квантовом компьютере.

В процессе работы были освещены особенности квантовой передачи информации, раскрыто понятие квантового шифрования, а так же и рассмотрены основные протоколы квантового шифрования.

Были изучены системы фотонной криптографии и их применение в прикладной криптографии. В дипломной работе рассмотрены криптографические хеш-функции, а так же применение базовых принципов криптографических хеш-функций в квантовом хешировании.

Рассмотрено решение практической задачи по созданию регистра с заданным числом кубитов и принципов построения квантовых симуляторов.

Так же в дипломной работе рассмотрены варианты сопряжения квантовых вычислительных систем в квантовую сеть.