О Т З Ы В

на автореферат диссертации Д.А.Махорина «Модель системы квантового распределения ключа с временным кодированием по волоконно-оптической линии связи», представленной на соискание ученой степени кандидата технических наук по специальности 05.11.07 – оптические и оптико-электронные приборы и комплексы

Диссертационная работа Д.А.Махорина посвящена исследованию в области квантовой криптографии и распределения защищенного квантового ключа посредством одиночных фотонов, предаваемых в оптоволоконном квантовом канале связи. Квантовый ключ применяется для кодирования информации в симметричной криптосистеме, а его абсолютная защищенность обусловлена законами квантовой механики – невозможностью точного воспроизведения (клонирования) квантового состояния одиночного фотона нелегитимным пользователем. Целью работы было моделирование квантового распределения ключа (КРК) между передатчиком и приемником с временным кодированием одиночных фотонов в волоконно-оптической линии связи. Эта тематика актуальна для создания будущих защищенных систем оптической связи, не подверженных опасности взлома с применением квантового компьютера, на котором возможна реализация алгоритма Шора для быстрой факторизации больших чисел и дешифрования ключей в современных асимметричных криптосистемах.

В первой главе диссертации рассмотрены основные принципы построения систем КРК на основе протоколов с поляризационным, фазовым и временным кодированием квантовых состояний одиночных фотонов. Изучены помехоустойчивость и характеристики лавинных фотодиодов (ЛФД), предназначенных для регистрации одиночных фотонов в линейном и гейгеровском режимах.

Во второй главе диссертации обсуждаются особенности создания аппаратной части систем КРК, а также моделей их функционирования. Показано, что при большом коэффициенте лавинного умножения ЛФД в его сигнале в линейном режиме можно различить отсутствие или присутствие одиночных фотонов и выполнить оптимизацию помехоустойчивости модуля приемника. Расчеты для теоретической модели линейного приемника на основе ЛФД Hamamatsu S8664-05K показали, что при длине оптоволоконного канала 1 км и затухании в волокне 2 дБ/км скорость генерации ключа будет составлять 10,2 кб/с при уровне квантовых ошибок 7%, что в принципе позволяет реализовать протокол BB84 с алгоритмом коррекции ошибок. Это может быть использовано для удешевления систем КРК путем замены дорогостоящих гейгеровских ЛФД на сравнительно дешевые линейные ЛФД. Построена матричная модель трансформации временных кубитов при прохождении нескольких последовательно включенных разбалансированных интерферометров Маха-Цендера. Для увеличения скорости генерации ключа в схеме с временным кодированием фотонов предложено использовать схемы, в которой все порты интерферометров передатчика и приемника соединены оптическими волокнами. В практической части работы был создан малогабаритный высоковольтный источник питания для ЛФД Hamamatsu S8664-05K. Также была создана компьютерная модель формирователя импульсного питания для гейгеровского ЛФД Laser Components SAP500-Series на основе разрядной линии и исследованы его динамические характеристики.

В третьей главе диссертации рассмотрена модель системы КРК с временным кодированием одиночных фотонов, дополненной подсистемами статистического и

интерферометрического контроля фотонов. Показано, что в данной модели ошибочные биты ключа возникают лишь при наличии шумов в системе. Отмечена возможность удержания количества ошибок на уровне ~11% с помощью регулировки порога срабатывания однофотонных детекторов ценой уменьшения скорости генерации ключа. Дополнительным способом защиты протокола является использование подсистем статистического и интерферометрического контроля состояний принятых фотонов, что может быть реализовано программно-аппаратным способом.

В четвертой главе исследуется оптоволоконная система, работающая по протоколу BB84 с кодированием фотонов с одно- или двукратными временными сдвигами. Временное кодирование обеспечивают большую устойчивость однофотонных состояний к флуктуациям параметров оптоволоконного квантового канала связи, чем поляризационное или фазовое. Отмечено, что основной объем информации об ошибках квантового ключа содержится в обычно отбрасываемых сведениях о состояниях фотонов, где базисы измерения передатчика и приемника не совпадали. Для повышения защищенности системы в работе предложено передатчику и приемнику обмениваться этой информацией по классическому каналу. Контроль целостности фотонов с временным кодированием предлагается реализовать подсистемой интерференционного контроля. Проведенное моделирование КРК в данной системе в условиях присутствия нелегитимного пользователя в квантовом канале подтвердило общую функциональность системы и позволило сделать вывод о дальнейших путях совершенствования систем КРК с временным кодированием фотонов.

Оценивая работу в целом, следует отметить актуальность поставленных задач, большой объем проведенных исследований, построение различных моделей КРК с временным кодированием одиночных фотонов. Научная ценность работы подтверждается наличием публикаций в журналах, рекомендуемых ВАК.

В то же время, работа несвободна от недостатков. В качестве основных замечаний можно отметить следующее:

1. До сих пор во всех системах КРК в мире применялись только ЛФД, работающие в гейгеровском режиме. Однако автор утверждает, что регистрация одиночных фотонов возможна и в линейном режиме, что показано на примере расчетов с ЛФД Hamamatsu S8664-05K. Из текста автореферата на стр.8-9 непонятно, использовались ли для расчета реальные характеристики данного ЛФД, например, какими брались его температура и темновой ток.
2. Для расчетов скорости КРК на стр.9 берется затухание оптоволокна 2 дБ/км, однако не обсуждается ни длина волны фотонов, ни какому известному типу волокна такое затухание соответствует, ни то, соответствует ли эта длина волны максимуму чувствительности ЛФД S8664-05K.
3. На стр.7. автореферата написано, что "... в квантовом канале, построенном на основе одномодового оптического волокна уровень системных ошибок p, в основном, определяется приемным оптическим модулем." Однако в протяженных оптоволоконных линиях связи потери фотонов, в основном, обусловлены их затуханием в оптоволокне.
4. На стр.13 автореферата написано, что "Снижение указанных потерь битрейта можно получить в схеме, в которой порты обоих интерферометров соединены оптическими волокнами." Однако не обсуждается, должны ли это быть абсолютно идентичные волокна, обеспечивающие постоянную разность фаз для интерферометров Маха-Цендера, или, что то же самое, временных задержек при

распространении фотонов в протяженном оптоволокне. Автору следовало бы обсудить требования к температурной и поляризационной стабильности этих волокон.

Указанные замечания не влияют на общую положительную оценку диссертационной работы.

Диссертация Д.А.Махорина выполнена на хорошем научно-техническом уровне и имеет практическую значимость для создания квантовых систем связи на основе одиночных фотонов. Диссертация соответствует всем требованиям ВАК, предъявляемым к кандидатским диссертациям, а Д.А.Махорин заслуживает присуждения ученой степени кандидата технических наук по специальности 05.11.07 – оптические и оптико-электронные приборы и комплексы.

Зав. лаб. Института физики
полупроводников им. А.В.Ржанова
СО РАН, д.ф.-м.н. И.И.Рябцев

Адрес: 630090, Новосибирск,
проспект Лаврентьева 13
Тел. (383) 333-24-08
E-mail: ryabtsev@isp.nsc.ru

Ученый секретарь Института физики
полупроводников им. А.В.Ржанова
СО РАН, к.ф.-м.н. С.А.Аржанникова

15.06.2016