МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ РАДИОФИЗИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

Кафедра физики и аэрокосмических технологий

Аннотация к дипломной работе

ПОМЕХОУСТОЙЧИВОСТЬ ВОЛОКОННО-ОПТИЧЕСКИХ СИСТЕМ КВАНТОВОЙ КРИПТОГРАФИИ

Ляховская Елизавета Игоревна

Научный руководитель — доцент А.В. Поляков

Минск, 2022

РЕФЕРАТ

Дипломная работа: 58 страниц, 24 рисунка, 2 таблицы, 46 источников

КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧА, ПРОТОКОЛЫ КОДИРОВАНИЯ, БИТОВАЯ СКОРОСТЬ, ВОЛОКОННО-ОПТИЧЕСКАЯ СИСТЕМА, ЛАВИННЫЙ ФОТОДИОД

Объект исследования – квантовые волоконно-оптические каналы связи.

Цель работы – рассмотрение протоколов квантовой криптографии, исследование скорости формирования квантового распределения ключа в волоконно-оптических системах квантовой криптографии на разных длинах волн при использовании Si- и InGaAs-лавинных фотодиодов.

Разработана математическая модель, описывающая помехоустойчивость систем квантовой криптографии для оценки битовой скорости формирования квантового распределения ключа при кодировании через временные сдвиги.

Установлено, что минимальная вероятность пропуска сигнала будет наблюдаться при минимуме дисперсии σ, которая, в свою очередь, зависит от длительности импульсной характеристики приемного блока τ при условии $\xi_1=\tau/\tau_0=12$ для Si-ЛФД и $\xi_2=\tau/\tau_0=10$ для InGaAs-ЛФД, где $\tau_0=2$ нс– длительность исходного сигнального импульса. Данные значения σ достигаются при величине нагрузочных сопротивлений R=4 МОм для Si-ЛФД и R=2,5 МОм для InGaAs-ЛФД.

Получено, что уровень коэффициента квантовых ошибок Q-BER=11% будет выполняться при значениях $U_{пор}$=33 В для Si-ЛФД и $U_{пор}$=42 В для InGaAs-ЛФД.

Выявлены зависимости битовой скорости формирования квантового распределения ключа от длины волоконно-оптической линии. Показано, что для длины одномодового волокна до 2,5 км предпочтительнее использовать передачу данных на длине волны 0,85 мкм с использованием Si-ЛФД, а для более длинных волокон необходимо применять InGaAs-ЛФД, работающие на длине волны 1,55 мкм.

Установлено, что потери на стыковку могут приводить к уменьшению скорости генерации квантового распределения ключа до двух раз. Это необходимо учитывать при проектировании волоконно-оптических систем квантовой криптографии.

РЭФЕРАТ

Дыпломная работа: 58 старонак, 24 малюнка, 2 табліцы, 46 спасылак

КВАНТАВАЕ РАЗМЕРКАВАННЕ КЛЮЧА, ПРАТАКОЛЫ КАДАВАННЯ, БІТАВАЯ ХУТКАСЦЬ, ВАЛАКОННА-АПТЫЧНАЯ СІСТЭМА, ЛАВІННЫ ФОТАДЫЁД

Аб'ект даследавання – квантавыя валаконна-аптычныя каналы сувязі. Мэта работы – разгляд пратаколаў квантавай крыптаграфіі, даследаванне хуткасці фарміравання квантавага размеркавання ключа ў валаконна-аптычных сістэмах квантавай крыптаграфіі на розных даўжынях хваль пры выкарыстанні Si- і InGaAs-лавінных фотадыёдаў.

Спраектавана матэматычная мадэль, якая апісвае перашкодаўстойлівасць сістэм квантавай крыптаграфіі для ацэнкі бітавай хуткасці фарміравання квантавага размеркавання ключа пры кадаванні праз часовыя зрухі.

Устаноўлена, што мінімальная верагоднасць пропуску сігналу будзе назірацца пры мінімуме дысперсіі σ, якая, у сваю чаргу, залежыць ад працягласці імпульснай характарыстыкі прыёмнага блока τ пры ўмове $\xi_1=\tau/\tau 0=12$ для Si-ЛФД і $\xi_2=\tau/\tau 0=10$ для InGaAs-ЛФД, дзе $\tau_0=2$ нс – працягласць зыходнага сігнальнага імпульсу. Дадзеныя значэння σ дасягаюцца пры велічыні нагрузачных супраціваў R=4 МОм для Si-ЛФД і R=2,5 МОм для InGaAs-ЛФД.

Атрымана, што ўзровень каэфіцыента квантавых памылак Q-BER=11% будзе выконвацца пры значэннях $U_{пор}$=33 В для Si-ЛФД і $U_{пор}$=42 В для InGaAs-ЛФД.

Выяўлены залежнасці бітавай хуткасці фарміравання квантавага размеркавання ключа ад даўжыні валаконна-аптычнай лініі. Паказана, што для даўжыні аднамодавага валакна да 2,5 км пераважней выкарыстоўваць перадачу дадзеных на даўжыні хвалі 0,85 мкм з выкарыстаннем Si-ЛФД, а для больш доўгіх валокнаў неабходна ўжываць InGaAs-ЛФД, якія працуюць на даўжыні хвалі 1,55 мкм.

Устаноўлена, што страты на стыкоўку могуць прыводзіць да памяншэння хуткасці генерацыі квантавага размеркавання ключа да двух разоў. Гэта неабходна ўлічваць пры праектаванні валаконна-аптычных сістэм квантавай крыптаграфіі.

ABSTRACT

Graduate work: 58 pages, 24 figures, 2 tables, 46 sources

QUANTUM KEY DISTRIBUTION, ENCODING PROTOCOLS, BIT RATE, FIBER-OPTIC SYSTEM, AVALANCHE PHOTODIOD

The object of research is quantum fiber-optic communication channels.

The purpose of the work is to consider the protocols of quantum cryptography, to study the rate of formation of the quantum key distribution in fiber–optic quantum cryptography systems at different wavelengths using Si- and InGaAs-avalanche photodiodes.

A mathematical model describing the noise immunity of quantum cryptography systems has been developed to estimate the bit rate of the formation of a quantum key distribution when encoding through time shifts.

It is established that the minimum probability of missing a signal will be observed at a minimum of the variance σ, which, in turn, depends on the duration of the pulse response of the receiving unit τ, provided $\xi_1=\tau/\tau_0=12$ for Si-APD and $\xi_2=\tau/\tau_0=10$ for InGaAs-APD, where $\tau_0=2$ ns is the duration of the initial signal pulse. These values of σ are achieved when the load resistances are R=4 MOhm for Si-APD and R=2.5 MOhm for InGaAs-APD.

It is obtained that the level of the quantum error coefficient BER=11 % will be performed at the values of U_{th}=33 V for Si-APD and U_{th}=42 V for InGaAs-APD.

The dependences of the bit rate of the quantum key distribution formation on the length of the fiber-optic line are revealed. It is shown that for a single-mode fiber length up to 2.5 km, it is preferable to use data transmission at a wavelength of 0.85 μm using Si-APD, and for longer fibers it is necessary to use InGaAs-APD operating at a wavelength of 1.55 μm.

It has been established that the docking losses can lead to a decrease in the rate of quantum key distribution generation up to two times. This must be taken into account when designing fiber-optic quantum cryptography systems.