ПРОГРАММА
повышения квалификации

Теоретические основы и прикладные аспекты квантовой криптографии

Москва - 2018

1. Цель реализации программы

Цель курса - сформировать у слушателей знания о теоретических основах квантовой криптографии и практических аспектах ее использования.

Цели также включают в себя:

1) Освоение математического аппарата, используемого для задач квантовой криптографии.

2) Освоение принципов работы базовых квантовых криптографических протоколов распределения ключей.

3) Освоение принципов работы волоконно-оптических систем квантового распределения ключей, а также систем квантовой криптографии, работающих через открытое пространство.

4) Получение навыков разработки и доказательства криптографической стойкости систем квантовой криптографии.

5) Подготовка шлушателей к чтению современной научной литературы в данной области.

.

2. Формализованные результаты обучения

Обучение в МГУ имени М.В. Ломоносова направлено на подготовку работника высокой квалификации, который:

в полной мере обладает профессиональными и личностными качествами, обеспечивающими ему приоритетную востребованность и устойчивую конкурентоспособность на российском и международном рынке труда и широкие возможности самореализации, в том числе в новейших областях знаний, наиболее значимых сферах профессиональной деятельности и общественной жизни;

стремится к продолжению образования и самообразованию в течение всей жизни, способен максимально продуктивно использовать свой творческий потенциал в интересах личности, общества и государства;

сознает ответственность за результаты своей профессиональной и научной деятельности перед страной и человечеством, обладает активной гражданской позицией, основанной на демократических убеждениях и гуманистических ценностях;

умеет порождать новые идеи, расширять сферу собственной компетентности, вырабатывать оптимальные стратегии своей деятельности; готов решать проблемы в новых и нестандартных профессиональных и жизненных ситуациях с учетом социальной и этической ответственности за принимаемые решения.

Выпускник МГУ имени М.В. Ломоносова, завершивший обучение по программе повышения квалификации «Квантовая обработка информации и квантовые технологии», должен обладать следующими универсальными и профессиональными компетенциями.

Универсальные компетенции

а) инструментальные:

способность использовать базовые знания и навыки управления информацией для решения исследовательских профессиональных задач, соблюдать основные требования информационной безопасности (ИК-1);

способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности, расширять и углублять свое научное мировоззрение (ИК-2);

б) системные:

способность к творчеству, порождению инновационных идей, выдвижению самостоятельных гипотез (СК-1);

способность к поиску, критическому анализу, обобщению и систематизации научной информации, к постановке целей исследования и выбору оптимальных путей и методов их достижения (СК-2);

способность к самостоятельному обучению и разработке новых методов исследования, к изменению научного и научно-производственного профиля деятельности; к инновационной научно-образовательной деятельности (СК-3).

Профессиональные компетенции

способность свободно владеть разделами физики, необходимыми для решения научно-исследовательских и научно-инновационных задач (ПК-1);

способность использовать знания современных проблем и новейших достижений физики в своей профессиональной деятельности (ПК-2);

способность и готовность применять на практике навыки составления и оформления научно-технической документации, научных отчётов, обзоров, докладов и статей (ПК-4);

способность использовать профессиональные знания в области информационных технологий, современных компьютерных сетей, программных продуктов и ресурсов интернета для решения задач профессиональной деятельности, в том числе находящихся за пределами профильной подготовки (ПК-5);

способность свободно владеть профессиональными знаниями для анализа и синтеза физической информации (ПК-6);

Результатом освоения дисциплины является формирования у слушателей специализированных компетенций по профессиональным

знаниям в области квантовой криптографии.

3. Содержание программы

Учебно-тематический план
программы повышения квалификации
«Теоретические основы и прикладные аспекты квантовой криптографии»

Объем – 72 часа.
Форма обучения – очно-заочная.

Наименование и краткое содержание разделов и тем дисциплины, **форма промежуточной аттестации по дисциплине**	**Всего, часы**	В том числе	
		Контактная работа (работа во взаимодействии с преподавателем), часы из них	**Самостоятельная работа обучающегося,** **часы** из них

		Занятия лекционного типа	Занятия семинарского типа	Учебные занятия, направленные на проведение текущего контроля успеваемости коллоквиумы, практические контрольные занятия и др.*	**Всего**	Выполнение домашних заданий	Подготовка рефератов и т.п.	**Всего**
Введение в квантовую криптографию. Одноразовые ключи. Критерий Шеннона абсолютной секретности. Квантово-механические запреты на копирование неизвестного квантового состояния. Основные стадии квантовых протоколов распределения ключей. Источники, детекторы, носители. Существующие достижения в квантовой криптографии.		2			**2**	2		**2**
Основные протоколы квантового распределения ключей: BB84, B92, E91, SARG04 и их реализации: фазово-временное кодирование, дифференциально-фазовое кодирование, релятивистское квантовое распределение ключей через открытое пространство с синхронизацией и без синхронизации часов на приемной и передающей стороне. Релятивистские квантово-механические запреты на копирование квантовых состояний.		6			**6**	6		**6**
Основы математического аппарата. Определение и критерии секретности. Критическая ошибка протоколов		2			**2**	2		**2**

квантового распределения ключей.								
Достижимая информация подслушивателя. Связь с квантовыми пропускными способностями.		2			**2**	2		**2**
.Индивидуальные и коллективные измерения в квантовой криптографии. Множественность атак подслушивателя, связь атак с пропускными способностями квантового канала.		2			**2**	2		**2**
Фундаментальная граница Холево для достижимой классической информации.		2			**2**	2		**2**
Исправление ошибок в первичных ключах в квантовой криптографии. Классические энтропии Реньи и их роль в квантовой криптографии. Усиление секретности – классический вариант. Универсальные хэш-функции второго рода, использование в процедурах усиления секретности и коррекции ошибок.		4			**4**	2		**2**
Доказательство секретности квантового распределения ключей для различных протоколов. Пример протокола BB84. Первые доказательства секретности для атак: прием-перепосыл, прозрачной атаки с индивидуальными и коллективными измерениями. Критические ошибки протокола для различных видов атак в асимптотическом пределе бесконечно длинных последовательностей передаваемых ключей.		2			**2**	2		**2**

Пример двухпараметрического протокола квантовой криптографии. Доказательство секретности квантового распределения ключей для квантовой криптографии с фазово-временным кодирование (асимптотический предел)). Критическая ошибка протокола при коллективной атаке.		2			**2**	2		**2**
Анализ стойкости протокола квантового распределения ключей SARG04.		2			**2**	2		**2**
Квантовые протоколы распределения ключей, использующие когерентные состояния. Необходимые сведения из теории когерентных состояний. Преобразование на линейных оптических элемента, детектирование когерентных состояний, включая гомодинное детектирование.		2			**2**	2		**2**
Анализ стойкости протокола квантового распределения ключей на геометрически однородных когерентных состояниях.		2			**2**	2		**2**
Квантовая криптография на непрерывных переменных.		2			**2**	2		**2**
Промежуточная аттестация - зачет			4		**4**	4 Подготовка к промежуточной аттестации (за-чету).		**4**

Итого		30	4	2	**36**			**36**

4. Материально-технические условия реализации программы

Реализация программы планируется на базе физического факультета МГУ. Для реализации программы есть необходимый аудиторный фонд, позволяющий работать с меловой (маркерной) доской, проектором, персональным компьютером, доступ в кабинет физических демонстраций и лаборатории общего физического практикума.

Аттестация участников осуществляется в форме зачета.

5. Учебно-методическое обеспечение программы

Основная литература:

1. А.С.Холево. Квантовые системы, каналы, информация, Москва. МЦМО, сс.327 (2010); S. Holevo, Introduction to Quantum Information Theory, (MTNMO, Moscow, 2002) [in Russian]; Usp. Mat. Nauk, 53, 193 (1998); А.С.Холево, Введение в квантовую теорию информации, серия Современная математическая физика, вып.5}, МЦНМО, Москва, 2002
2. М.Нильсен, И.Чанг, Квантовые вычисления и информация, изд. Мир, Москва, (2006).
3. Дж. Прескилл, Квантовая информация и квантовые вычисления, том 1, изд. R&C Dynamics, Ижевск, (2008).
4. C.E.Shannon, Mathematical Theory of Communication, Bell Syst. Tech. Jour., 27, 397; 27, 623 (1948).
5. Р.Галлагер, Теория информации и надежная связь, (Советское радио, 1974);
6. R. G. Gallager, Information Theory and Reliable Communication, (Wiley, New York, 1968)
7.

Дополнительная литература:

1. W.K.Wootters, W.H.Zurek, A single quantum cannot be cloned, Nature, {299, 802 (1982).
2. C.H.Bennett, G.Brassard, Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, 175 (1984).
3. C.H.Bennett, Phys. Rev. Lett., 68, 3121 (1992).
4. R.Renner, Security of Quantum Key Distribution, PhD Thesis, ETH Z\"urich, Dec. 2005. arXiv/quant-ph: 0512258.
5. V.Scarani, H.Bechmann-Pasquinucci, N.J.Cerf, M.Dusek, N.Lutkenhaus,
6. M.Peev, Rev. Mod. Phys., 81, 1301 (2009).

7. D.Mayers, Journal ACM, 48 351 (2001).
8. H.-K.Lo, H.F.Chau, Science, 283 2050 (1999).
9. P.Shor, J.Preskill, Phys. Rev. Lett., 85 441 (2000).
10. M.Koashi, J. Phys. Conf. Ser., 36, 98 (2006).
11. M.Tomamichel. R.Renner, The Uncertainty Relation for Smooth Entropies, arXiv/quant-ph: 10092015.
12. M.Tomamichel, C.Ci Wen Lim, N.Gisin, R.Renner, Tight Finite-Key Analysis for Quantum Cryptography, arXiv/quant-ph: 11034130.
13. С.П.Кулик, А.П.Маккавеев, С.Н.Молотков, Письма в ЖЭТФ. 85, 354 (2007).
14. С.Н.Молотков, ЖЭТФ. 133, 5 (2008).
15. Д.А.Кронберг, С.Н.Молотков, ЖЭТФ, 136, 650 (2009); ЖЭТФ, 138, 33 (2010).
16. H.P.Robertson, Phys. Rev., 34, 163 (1929).
17. D.Deutsch, Phys. Rev. Lett., 50, 631 (1983).
18. K.Kraus, Phys. Rev., D 35, 3070 (1987).
19. H.Maassen, J.B.M.Uffink, Phys. Rev. Lett., {\bf 60}, 1103 (1988).
20. J.M.Renes, J.-C. Boileau, Phys. Rev. Lett., 103, 020402-1 (2009).
21. M.Berta, M.Chritlandl, R.Colbeck, J.M.Renes, R.Renner, The Uncertainty Principle in the Presence of Quantum Memory, arXiv/quant-ph: 0909.0950.
22. M.Cover J.A.Thomas. Elements of Information Theory. Wiley, (1991).
23. M.Berta, M.Christandl, R.Colbeck, J.M.Renes, R.Renner, Nature Physics, 6, 659 (2010).
24. M.Tomamichel, R.Renner, The Uncertainty Relation for Smooth Entropies, arXiv/quant-ph: 10092015.
25. J.M.Renes, R.Renner, One-Shot Classical Data Compression withQuantum Side Information and the Distillation of Common Randomness or Secret Keys, arXiv/quant-ph: 10080452.
26. J.L.Carter, M.N.Wegman Universal Classes of Hash Functions, J. Comp. Syst. Sci., 18, (1979) 143.
27. M.N.Wegman, J.L.Carter, New Hash Functions and Their Use Authentication and Set Euqality, J. Comp. Syst. Sci., 22, 265 (1991).
28. C.H.Bennett, G.Brassard, C.Crepeau, U.M.Maurer, Generalized Privacy Amplication, IEEE Trans. on Inf. Theory, 41 (1995) 1915.
29. M.Tomamichel, C.Schaffner, A.Smith, R.Renner, Leftover Hashing Against Quantum Side Information, arXiv/quant-ph: 10022436.
30. D.R.Stinson, On the Connections Between Universal Hashing, Combinatorial Designs and Error-Correcting Codes, ECCC TR95-052, Electronic Colloquium on Computational Complexity - Reports Series (1995).
31. W.Hoeffding, Probability Inequalities for Sums of Bounded Random Variables, J. Amer. Statistical Assoc., 58 (1963) 13.
32. R. J. Serfling, Probability Inequalities for the Sum in Sampling without Replacement ,Ann. Stat., 2 (1974) 39.
33. L.Lydersen, C.Wiechers, C.Wittmann, D.Elser, J.Skaar, V.Makarov,
34. Hacking commercial quantum cryptography systems by tailored bright illumination, Nature Photonics, 4, 686 (2010).
35. С.Н.Молот ков, “Энтропийные соотношения неопределенностей и стойкость фазово-временной квантовой криптографии при конечных длинах передаваемых последовательностей” Журнал экспериментальной и теоретической физики, т. 142 (2012) 1-19.

36. С.Н.Молотков, “О стойкости релятивистской квантовой криптографии в открытом пространстве при конечных ресурсах”.Письма в журнал экспериментальной и теоретической физики, т. 96 (2012) 374.
37. С.П.Кулик, С.Н.Молотков, И.В.Радченко, “О квантовом распределении ключей на композитных фотонах -- поляризационных кутритах.” Письма в журнал экспериментальной и теоретической физики, т. 96 (2012) 367.
38. С.Н.Молотоков, “О геометрически однородных когерентных состояниях в квантовой криптографии”, Письма в журнал экспериментальной и теоретической физики, т. 95 (2012) 361.
39. С.Н.Молотков, “Об уязвимости базовых протоколов квантового распределения ключей и о трех протоколах, устойчивых к атаке с “ослеплением” лавинных детекторов”, Журнал экспериментальной и теоретической физики, т. 141 (2012) 812-831.
40. С.Н.Молотков,“О решении проблемы обеспечения стойкости квантовой криптографии для канала связи со сколь угодно большой длиной”, Письма в журнал экспериментальной и теоретической физики, т. 93 (2011) 830.
41. С.Н.Молотков,“Квантовое распределение ключей без передачи квантового состояния как целого через канал связи”, Письма в журнал экспериментальной и теоретической физики, т. 93 (2011) 389.
42. С.Н.Молотков, “Релятивистская квантовая криптография для открытого пространства без синхронизации часов на передающей и приемной стороне”, Письма в журнал экспериментальной и теоретической физики, т. 94 (2011) 504.
43. С.Н.Молотков, “Энтропийные соотношения неопределенностей и предельно допустимая критическая ошибка в квантовой криптографии”. Письма в журнал экспериментальной и теоретической физики, т. 94 (2011) 900.
44. Молотков, “Квантовое распределение ключей с эталонным квантовым состоянием”, Журнал экспериментальной и теоретической физики, т. 140 (2011) 857.
45. С.Н.Молотков, Релятивистская квантовая криптография, Журнал экспериментальной и теоретической физики, т. 139 (2011) 139.
46. Д.А.Кронберг, С.Н.Молотков, Усиление стойкости фазово-временной квантовой криптографии блочным исправлением ошибок,, Письма в ЖЭТФ, т.92, (2010) 539.
47. Д.А.Кронберг, С.Н.Молотков, Квантовая схема для оптимального подслушивания фазово-временной квантовой криптографии ,ЖЭТФ, т.138 (2010) 33.

6. Требования к результатам обучения

Приводится перечень вопросов, выносимых на аттестацию в форме зачета, а также рекомендуемые темы рефератов.
Оценка уровня освоения программы осуществляется аттестационной комиссией по пятибалльной системе.

Оценка качества освоения программы осуществляется на зачете посредством защиты доклада с презентацией по теме, соответствующей программе и согласованной с преподавателем. Результаты защиты определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают сдачу зачета.

Критерии оценивания защиты доклада:

1. Авторская самостоятельность.
2. Четкость, обоснованность, конкретность и ясность изложения содержания системы заданий, лабораторных работ, тем исследований, соответствие действующим нормативным требованиям.
3. Умение обосновать и отстаивать как предложенные задачи, лабораторные работы, темы исследований так и систему на их основе.
4. Использование современных методов диагностики образовательных результатов.
5. Возможность индивидуализации разработанной программы.
6. Использование навыков, полученных на практических занятиях курса.

Форма защиты доклада – очная (презентация проекта перед членами аттестационной комиссии, авторами и слушателями программы).

7. Составители программы

Молотков Сергей Николаевич, доктор. физ.-мат. наук, профессор кафедры квантовой электроники физического факультета МГУ имени М.В. Ломоносова.