«УТВЕРЖДАЮ»

Председатель Научного совета РАН «Квантовые технологии»,
академик-секретарь ОНИТ РАН,
академик РАН

Г.Я. Красников

« 16 » марта 2022 г.

ПРОТОКОЛ
заседания Научного совета РАН «Квантовые технологии»
(далее — «Совет»)
по теме «Квантовые и постквантовые алгоритмы»

МЕСТО И ДАТА ПРОВЕДЕНИЯ: г. Москва, Ленинский пр-т, 32А, здание РАН, Синий зал. 3 марта 2021 г. с 10:00 до 15:53.

ФОРМАТ ПРОВЕДЕНИЯ: смешанный – очный и дистанционный (онлайн в Zoom).

ПРЕДСЕДАТЕЛЬСТВОВАЛ:

Председатель Совета, академик-секретарь Отделения нанотехнологий и информационных технологий (далее – ОНИТ) РАН, академик РАН Г.Я. Красников.

УЧАСТВОВАЛИ:

Члены Бюро Совета

1. Красников Геннадий Яковлевич, академик РАН	председатель Совета, руководитель приоритетного технологического направления по электронным технологиям, академик-секретарь ОНИТ РАН, генеральный директор АО «НИИМЭ» (очно)
2. Горбацевич Александр Алексеевич, академик РАН	заместитель председателя Совета, заведующий лабораторией ФИАН, заведующий кафедрой квантовой физики и наноэлектроники НИУ МИЭТ, заведующий лабораторией АО «НИИМЭ» (очно)
3. Холево Александр Семёнович, академик РАН	заместитель председателя Совета, заведующий отделом, главный научный сотрудник МИАН (очно)

4. Александров Евгений Борисович, академик РАН	руководитель лаборатории атомной радиоспектроскопии ФТИ им. А.Ф. Иоффе (онлайн)
5. Латышев Александр Васильевич, академик РАН	директор ИФП СО РАН (онлайн)
6. Сурис Роберт Арнольдович, академик РАН	главный научный сотрудник ФТИ им. А.Ф. Иоффе (онлайн)
7. Волович Игорь Васильевич, член-корреспондент РАН	заведующий отделом, главный научный сотрудник МИАН (онлайн)
8. Горнев Евгений Сергеевич, член-корреспондент РАН	заместитель руководителя приоритетного технологического направления АО «НИИМЭ» (онлайн)
9. Колачевский Николай Николаевич, член-корреспондент РАН	директор ФИАН (очно)
10. Махлин Юрий Генрихович, член-корреспондент РАН	главный научный сотрудник ИТФ им. Л.Д. Ландау РАН, заведующий лабораторией физики конденсированного состояния НИУ ВШЭ (очно)
11. Богданов Юрий Иванович, доктор физико-математических наук	главный научный сотрудник, руководитель лаборатории физики квантовых компьютеров ФТИАН им. К.А. Валиева РАН (онлайн)
12. Кулик Сергей Павлович, доктор физико-математических наук	научный руководитель Центра квантовых технологий физического факультета МГУ имени М.В. Ломоносова (очно)
13. Фельдман Эдуард Беньяминович, доктор физико-математических наук	заведующий лабораторией ИПХФ РАН (онлайн)
14. Тельминов Олег Александрович, кандидат технических наук	ученый секретарь Совета, начальник лаборатории АО «НИИМЭ», доцент базовой кафедры микро- и наноэлектроники МФТИ (очно)

Члены Совета

15. Глазов Михаил Михайлович, член-корреспондент РАН	ведущий научный сотрудник ФТИ им. А.Ф. Иоффе (онлайн)
16. Двуреченский Анатолий Васильевич, член-корреспондент РАН	заведующий лабораторией неравновесных полупроводниковых систем ИФП СО РАН, профессор кафедры «Физика полупроводников» Новосибирского государственного университета (очно)
17. Ивченко Евгениюс Левович, член-корреспондент РАН	заведующий сектором ФТИ им. А.Ф. Иоффе (онлайн)
18. Лукичев Владимир Федорович, член-корреспондент РАН	директор ФТИАН им. К.А. Валиева РАН (очно)

19. Никитов Сергей Аполлонович, член-корреспондент РАН	директор ИРЭ им. В.А. Котельникова РАН (очно)
20. Рябцев Игорь Ильич, член-корреспондент РАН	заведующий лабораторией ИФП СО РАН (онлайн)
21. Турлапов Андрей Вадимович, член-корреспондент РАН, PhD	заведующий лабораторией ультрахолодных квантовых систем ИПФ РАН, руководитель научной группы РКЦ (онлайн)
22. Устинов Виктор Михайлович, член-корреспондент РАН	директор НТЦ микроэлектроники РАН (онлайн)
23. Шеремет Игорь Анатольевич, член-корреспондент РАН	заместитель директора по науке РФФИ (онлайн)
24. Калачёв Алексей Алексеевич, профессор РАН, доктор физико-математических наук	директор ФИЦ КазНЦ РАН (онлайн)
25. Печень Александр Николаевич, профессор РАН, доктор физико-математических наук	заведующий отделом МИАН (очно)
26. Аблаев Фарид Мансурович, доктор физико-математических наук	заведующий кафедрой теоретической кибернетики Казанского (Приволжского) федерального университета, главный научный сотрудник Физико-технического института ФИЦ КазНЦ РАН (очно)
27. Звездин Анатолий Константинович, доктор физико-математических наук	главный научный сотрудник ИОФ РАН (онлайн)
28. Сысоев Николай Николаевич, доктор физико-математических наук	декан физического факультета МГУ имени М.В. Ломоносова (онлайн)

От Государственной корпорации по содействию разработке, производству и экспорту высокотехнологичной промышленной продукции «Ростех», г. Москва

29. Стоянов Сергей Викторович	директор по развитию Центра суперкомпьютерного моделирования Госкорпорации «Ростех» (онлайн)

От Общества с ограниченной ответственностью «Совместное предприятие «Квантовые технологии» (Госкорпорация «Росатом»), г. Москва

30. Борисов Ярослав Михайлович	руководитель направления по новым проектам ООО «СП «Квант» (Госкорпорация «Росатом») (онлайн)

От Проектного офиса по реализации программы «Цифровая экономика Российской Федерации» – аналитического центра при Правительстве Российской Федерации

31. Ганеев Константин Альбертович	заместитель руководителя направления Проектного офиса по реализации программы «Цифровая экономика Российской Федерации» - аналитического центра при Правительстве Российской Федерации (онлайн)

От Российского квантового центра, г. Москва

32. Киктенко Евгений Олегович, кандидат физико-математических наук	главный научный сотрудник РКЦ, старший научный сотрудник МИАН (очно)
33. Федоров Алексей Константинович, кандидат физико-математических наук	руководитель проекта «Квантовые информационные технологии» РКЦ (онлайн)
34. Мастюкова Алена Сергеевна	младший научный сотрудник РКЦ (онлайн)

От Федерального государственного казенного научного учреждения «Академия криптографии Российской Федерации», г. Москва

35. Корольков Андрей Вячеславович, кандидат технических наук	начальник Научно-исследовательского центра Академии криптографии Российской Федерации, заведующий кафедрой БК-252 РТУ МИРЭА (очно)

От Фонда перспективных исследований, г. Москва

36. Ремнев Михаил Анатольевич, кандидат физико-математических наук	руководитель проекта Центра перспективной электроники направления информационных исследований Фонда перспективных исследований (онлайн)

От Государственного научного учреждения «Институт физики имени Б.И. Степанова Национальной академии наук Беларуси», г. Минск

37. Килин Сергей Яковлевич, иностранный член РАН, академик НАН Беларуси	заведующий центром Института физики НАН Беларуси, заместитель Председателя Президиума НАН Беларуси (онлайн)

От Института проблем лазерных и информационных технологий — филиала Федерального государственного учреждения «Федеральный научно-исследовательский центр «Кристаллография и фотоника» Российской академии наук», г. Шатура Московской обл.

38. Панков Михаил Александрович, кандидат физико-математических наук	старший научный сотрудник ИПЛИТ РАН – филиала ФНИЦ «Кристаллография и фотоника» РАН (онлайн)
39. Притоцкий Егор Михайлович	научный сотрудник ИПЛИТ РАН – филиала ФНИЦ «Кристаллография и фотоника» РАН (онлайн)

От Института систем обработки изображений РАН — филиала Федерального государственного учреждения «Федеральный научно-исследовательский центр «Кристаллография и фотоника» Российской академии наук», г. Самара

40. Сойфер Виктор Александрович, академик РАН	научный руководитель ИСОИ РАН – филиала ФНИЦ «Кристаллография и фотоника» РАН, президент Самарского университета (онлайн)

От Института теоретической физики им. Л.Д. Ландау Российской академии наук, г. Москва

41. Мальцев Андрей Яковлевич, профессор РАН, доктор физико-математических наук	старший научный сотрудник ИТФ им. Л.Д. Ландау РАН (онлайн)

От Института физики микроструктур РАН — филиала Федерального государственного бюджетного научного учреждения «Федеральный исследовательский центр Институт прикладной физики Российской академии наук», г. Нижний Новгород

42. Гапонов Сергей Викторович, академик РАН	советник ИФМ РАН – филиала ИПФ РАН (онлайн)

От Научного совета РАН по материалам и наноматериалам, г. Москва

43. Алдошин Сергей Михайлович, академик РАН	председатель Научного совета РАН по материалам и наноматериалам, научный руководитель ИПХФ РАН (онлайн)

От Самарского филиала Федерального государственного бюджетного учреждения науки Физический институт им. П.Н. Лебедева Российской академии наук, г. Самара

44. Котова Светлана Павловна, кандидат физико-математических наук	ведущий научный сотрудник, заведующий лабораторией моделирования и автоматизацией лазерных систем, и.о. заместителя директора по научной работе СФ ФИАН, профессор Самарского университета (онлайн)

От Федерального государственного автономного научного учреждения Институт сверхвысокочастотной полупроводниковой электроники имени В.Г. Мокерова Российской академии наук, г. Москва

45. Мальцев Петр Павлович, доктор технических наук	научный руководитель ИСВЧПЭ РАН (очно)

От Федерального государственного бюджетного учреждения «Российская академия наук», г. Москва

46. Ситник Леонид Леонидович	главный специалист Управления научно-информационной деятельности РАН (очно)

От Федерального государственного бюджетного учреждения высшего образования и науки «Санкт-Петербургский национальный исследовательский академический университет Российской Академии Наук», г. Санкт-Петербург

47. Мухин Иван Сергеевич, кандидат физико-математических наук	заведующий лабораторией возобновляемых источников энергии СПбАУ РАН им. Ж.И. Алферова (онлайн)

От Федерального государственного бюджетного учреждения науки Институт нанотехнологий микроэлектроники Российской академии наук, г. Москва

48. Сауров Александр Николаевич, академик РАН	директор ИНМЭ РАН (онлайн)

От Федерального государственного бюджетного учреждения науки Институт общей физики им. А.М. Прохорова Российской академии наук, г. Москва

49. Гусейн-заде Намик Гусейнага оглы, доктор физико-математических наук	заведующий отделом ИОФ РАН (очно)

От Федерального государственного бюджетного учреждения науки Институт проблем проектирования в микроэлектронике Российской академии наук, г. Москва, г. Зеленоград

50. Русаков Сергей Григорьевич, член-корреспондент РАН	главный научный сотрудник ИППМ РАН (онлайн)
51. Ульянов Сергей Леонидович, доктор технических наук	главный научный сотрудник ИППМ РАН (онлайн)

От Федерального государственного бюджетного учреждения науки Институт проблем технологии микроэлектроники и особочистых материалов Российской академии наук, г. Черноголовка Московской обл.

52. Зайцев Сергей Иванович, доктор физико-математических наук	главный научный сотрудник ИПТМ РАН (онлайн)
53. Рощупкин Дмитрий Валентинович, доктор физико-математических наук	директор ИПТМ РАН (очно)
54. Тулин Вячеслав Александрович, доктор физико-математических наук	главный научный сотрудник ИПТМ РАН (онлайн)
55. Фомин Лев Александрович, кандидат физико-математических наук	заведующий лабораторией ИПТМ РАН (онлайн)
56. Шабельникова Яна Леонидовна, кандидат физико-математических наук	научный сотрудник ИПТМ РАН (онлайн)

От Федерального государственного бюджетного учреждения науки Институт проблем химической физики Российской академии наук, г. Черноголовка Московской обл.

57. Коплак Оксана Вячеславовна, доктор физико-математических наук	заведующий лабораторией ИПХФ РАН (онлайн)
58. Доронин Сергей Иванович, кандидат физико-математических наук	старший научный сотрудник ИПХФ РАН (онлайн)
59. Зенчук Александр Иванович, кандидат физико-математических наук	ведущий научный сотрудник ИПХФ РАН (онлайн)
60. Кузнецова Елена Игоревна, кандидат физико-математических наук	старший научный сотрудник ИПХФ РАН (онлайн)
61. Пырков Алексей Николаевич, кандидат физико-математических наук	научный сотрудник ИПХФ РАН (онлайн)

62. Бочкин Георгий Алексеевич	научный сотрудник ИПХФ РАН (онлайн)
63. Лазарев Илья Дмитриевич	инженер ИПХФ РАН (онлайн)

От Федерального государственного бюджетного учреждения науки Институт радиотехники и электроники им. В.А. Котельникова Российской академии наук, г. Москва

64. Кузнецова Ирен Евгеньевна, профессор РАН, доктор физико-математических наук	главный научный сотрудник, заведующий отделом аспирантуры ИРЭ им. В.А. Котельникова РАН (очно)
65. Логунов Михаил Владимирович, доктор физико-математических наук	ведущий научный сотрудник ИРЭ им. В.А. Котельникова РАН (онлайн)

От Федерального государственного бюджетного учреждения науки Институт физики полупроводников им. А.В. Ржанова Сибирского отделения Российской академии наук, г. Новосибирск

66. Ковалев Вадим Михайлович, доктор физико-математических наук	заведующий лабораторией ИФП СО РАН (онлайн)
67. Попов Владимир Павлович, доктор физико-математических наук	заведующий лабораторией физических основ материаловедения кремния ИФП СО РАН, научный консультант АО «НЗПП с ОКБ» (онлайн)
68. Бетеров Илья Игоревич, кандидат физико-математических наук	старший научный сотрудник ИФП СО РАН (онлайн)
69. Ненашев Алексей Владимирович, кандидат физико-математических наук	старший научный сотрудник ИФП СО РАН (онлайн)

От Федерального государственного бюджетного учреждения науки Институт физики твердого тела Российской академии наук, г. Черноголовка Московской обл.

70. Тулина Наталья Алексеевна, кандидат физико-математических наук	старший научный сотрудник ИФТТ РАН (онлайн)

От Федерального государственного бюджетного учреждения науки Институт физической химии и электрохимии им. А.Н. Фрумкина Российской академии наук, г. Москва

71. Мартынов Александр Германович, доктор химических наук	ИФХЭ РАН (очно)

От Федерального государственного бюджетного учреждения науки Институт химии высокочистых веществ им. Г.Г. Девятых Российской академии наук, г. Нижний Новгород

72. Созин Андрей Юрьевич, доктор химических наук	заведующий лабораторией аналитической химии высокочистых веществ ИХВВ РАН (онлайн)

От Федерального государственного бюджетного учреждения науки Института лазерной физики Сибирского отделения Российской академии наук, г. Новосибирск

73. Тайченачев Алексей Владимирович, член-корреспондент РАН	директор ИЛФ СО РАН, профессор НГУ (онлайн)

От Федерального государственного бюджетного учреждения науки Математический институт им. В.А. Стеклова Российской академии наук, г. Москва

74. Амосов Григорий Геннадьевич, доктор физико-математических наук	ведущий научный сотрудник МИАН, профессор МФТИ (онлайн)
75. Подольский Владимир Владимирович, доктор физико-математических наук	ведущий научный сотрудник отдела математической логики МИАН, доцент НИУ ВШЭ (очно)
76. Трушечкин Антон Сергеевич, доктор физико-математических наук	ведущий научный сотрудник МИАН (очно)
77. Широков Максим Евгеньевич, доктор физико-математических наук	ведущий научный сотрудник МИАН, профессор кафедры высшей математики МФТИ (онлайн)
78. Теретёнков Александр Евгеньевич, кандидат физико-математических наук	научный сотрудник МИАН (очно)

От Федерального государственного бюджетного учреждения науки Физико-технический институт им. А.Ф. Иоффе Российской академии наук, г. Санкт-Петербург

79. Торопов Алексей Акимович, доктор физико-математических наук	заведующий лабораторией квантовой фотоники ФТИ им. А.Ф. Иоффе (онлайн)
80. Шамрай Александр Валерьевич, доктор физико-математических наук	заведующий лабораторией квантовой электроники ФТИ им. А.Ф. Иоффе (онлайн)
81. Шубина Татьяна Васильевна, доктор физико-математических наук	главный научный сотрудник ФТИ им. А.Ф. Иоффе (онлайн)

82. Анисимов Андрей Николаевич, кандидат физико-математических наук	научный сотрудник ФТИ им. А.Ф. Иоффе (онлайн)

От Федерального государственного бюджетного учреждения науки Физико-технологический институт имени К.А. Валиева Российской академии наук, г. Москва

83. Богданова Надежда Александровна, кандидат физико-математических наук	старший научный сотрудник ФТИАН им. К.А. Валиева РАН (онлайн)
84. Федичкин Леонид Евгеньевич, кандидат физико-математических наук	ведущий научный сотрудник ФТИАН им. К.А. Валиева РАН, доцент кафедры теоретической физики МФТИ (очно)
85. Хорин Иван Анатольевич, кандидат физико-математических наук	ученый секретарь ФТИАН им. К.А. Валиева РАН, доцент РТУ МИРЭА (онлайн)
86. Чернявский Андрей Юрьевич, кандидат физико-математических наук	старший научный сотрудник ФТИАН им. К.А. Валиева РАН (очно)
87. Фастовец Дмитрий Владиславович	младший научный сотрудник ФТИАН им. К.А. Валиева РАН (онлайн)

От Федерального государственного бюджетного учреждения науки Физический институт им. П.Н. Лебедева Российской академии наук, г. Москва

88. Шубин Николай Михайлович, кандидат физико-математических наук	старший научный сотрудник ФИАН, старший научный сотрудник АО «НИИМЭ» (онлайн)

От Федерального государственного унитарного предприятия Экспериментальный завод научного приборостроения со Специальным конструкторским бюро Российской академии наук, г. Черноголовка Московской обл.

89. Бородин Владимир Алексеевич, член-корреспондент РАН	заместитель генерального директора ФГУП ЭЗАН (онлайн)

От Федерального государственного учреждения «Федеральный исследовательский центр «Информатика и управление» Российской академии наук», г. Москва

90. Безродных Сергей Игоревич, профессор РАН, доктор физико-математических наук	ведущий научный сотрудник ФИЦ ИУ РАН, начальник отдела — заместитель академика-секретаря по научно-организационной работе ОМН РАН (онлайн)
91. Зацаринный Александр Алексеевич, доктор технических наук	заместитель директора по научной работе ФИЦ ИУ РАН (онлайн)

92. Бажанов Дмитрий Игоревич, кандидат физико-математических наук, PhD	старший научный сотрудник ФИЦ ИУ РАН, старший преподаватель Физического факультета МГУ имени М.В. Ломоносова (очно)

От Федерального государственного учреждения «Федеральный научный центр научно-исследовательский институт системных исследований Российской академии наук», г. Москва

93. Привезенцев Владимир Владимирович, кандидат технических наук	ведущий научный сотрудник ФГУ ФНЦ НИИСИ РАН (онлайн)
94. Фирсов Анатолий Александрович, кандидат физико-математических наук	ведущий научный сотрудник ФГУ ФНЦ НИИСИ РАН (онлайн)
95. Дорофеев Владислав Петрович	научный сотрудник ФГУ ФНЦ НИИСИ РАН (онлайн)

От Фрязинского филиала Федерального государственного бюджетного учреждения науки Институт радиотехники и электроники им. В.А. Котельникова Российской академии наук, г. Фрязино Московской обл.

96. Гольдман Евгений Иосифович, кандидат физико-математических наук	ведущий научный сотрудник ФИРЭ им. В.А. Котельникова РАН (онлайн)

От Технического комитета по стандартизации ТК 26 «Криптографическая защита информации», г. Москва

97. Матюхин Дмитрий Викторович, кандидат физико-математических наук	заместитель председателя ТК 26 (очно)

От Федерального государственного бюджетного научного учреждения «Научно-исследовательский институт - республиканский исследовательский научно-консультационный центр экспертизы», г. Москва

98. Беневоленский Сергей Борисович, доктор технических наук	главный научный сотрудник ФГБНУ НИИ РИНКЦЭ (онлайн)

От Федерального государственного бюджетного научного учреждения «Научно-производственный комплекс «Технологический центр», г. Москва, г. Зеленоград

99. Веселов Владимир Федорович	начальник отдела НПК «Технологический центр» (онлайн)

От Федерального государственного бюджетного научного учреждения Федеральный научный агроинженерный центр ВИМ, г. Москва

100. Толоконников Георгий Константинович, кандидат физико-математических наук	научный сотрудник ФГБНУ ФНАЦ ВИМ (очно)

От Федерального государственного бюджетного учреждения «Национальный исследовательский центр «Курчатовский институт», г. Москва

101. Демин Вячеслав Александрович, кандидат физико-математических наук	заместитель главного ученого секретаря, и.о. начальника лаборатории технологий искусственного интеллекта НИЦ «Курчатовский институт» (онлайн)

От Федерального государственного унитарного предприятия «Всероссийский научно-исследовательский институт автоматики им. Н.Л. Духова»

102. Сатанин Аркадий Михайлович, доктор физико-математических наук	главный научный сотрудник ФГУП «ВНИИА» (онлайн)

От Федерального государственного унитарного предприятия «Всероссийский научно-исследовательский институт физико-технических и радиотехнических измерений», г.о. Солнечногорск Московской обл.

103. Фатеев Вячеслав Филиппович, доктор технических наук	начальник научно-технического центра ФГУП «ВНИИФТРИ», профессор аспирантуры ПАО «МАК «Вымпел» (онлайн)
104. Хромов Максим Николаевич, кандидат физико-математических наук	заместитель начальника ГМЦ ГСВЧ по научной работе ФГУП «ВНИИФТРИ» (очно)

От Федерального государственного унитарного предприятия «Российский федеральный ядерный центр - всероссийский научно-исследовательский институт экспериментальной физики», г. Саров Нижегородской обл.

105. Степаненко Сергей Александрович, доктор физико-математических наук	главный научный сотрудник ФГУП «РФЯЦ - ВНИИЭФ» (онлайн)

От Автономной некоммерческой образовательной организации высшего образования «Сколковский институт науки и технологий», г. Москва

106. Кабатянский Григорий Анатольевич, доктор физико-математических наук	вице-президент по академическому сотрудничеству Сколтеха (очно)

От Автономной некоммерческой организации «Университет Иннополис», г. Иннополис

107. Тормасов Александр Геннадьевич, доктор физико-математических наук	ректор АНО ВО «Университет Иннополис» (онлайн)

От Научно-исследовательского физико-технического института Федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского», г. Н. Но

108. Бастракова Марина Валерьевна, кандидат физико-математических наук	заведующий лабораторией теории наноструктур НИФТИ ННГУ им. Н.И. Лобачевского, доцент кафедры физического материаловедения физического факультета ННГУ им. Н.И. Лобачевского (онлайн)

От Федерального государственного автономного образовательного учреждения высшего образования «Крымский федеральный университет имени В.И. Вернадского», г. Симферополь

109. Полулях Сергей Николаевич, доктор физико-математических наук	заведующий кафедрой экспериментальной физики Физико-технического института Крымского федерального университета имени В.И. Вернадского (онлайн)

От Федерального государственного автономного образовательного учреждения высшего образования «Московский физико-технический институт (государственный университет)», г. Долгопрудный Московской обл.

110. Бугаев Александр Степанович, академик РАН	заведующий кафедрой МФТИ (очно)
111. Николаев Евгений Николаевич, член-корреспондент РАН	профессор кафедры молекулярной медицины МФТИ (очно)
112. Мизгинов Дмитрий Сергеевич	аспирант МФТИ, научный сотрудник АО «НИИМЭ» (онлайн)

113. Шарапов Андрей Анатольевич	аспирант базовой кафедры «Микро- и наноэлектроника» МФТИ, научный сотрудник АО «НИИМЭ» (очно)

От Федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского», г. Н. Новгород

114. Ежевский Александр Александрович, доктор физико-математических наук	профессор кафедры физики полупроводников, электроники и наноэлектроники физического факультета ННГУ им. Н.И. Лобачевского (онлайн)

От Федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС», г. Москва

115. Капуткина Наталия Ефимовна, доктор физико-математических наук	профессор НИТУ «МИСиС» (очно)
116. Кобелева Светлана Петровна, кандидат физико-математических наук	доцент кафедры полупроводниковой электроники и физики полупроводников НИТУ «МИСиС» (онлайн)
117. Курочкин Владимир Леонидович, кандидат физико-математических наук	заведующий лабораторией НИТУ «МИСиС», ведущий исследователь РКЦ (онлайн)
118. Курочкин Юрий Владимирович, кандидат физико-математических наук	директор Центра компетенций по квантовым коммуникациям НИТУ «МИСиС» (онлайн)

От Федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский университет «Высшая школа экономики», г. Москва

119. Лубенец Елена Рубеновна, доктор физико-математических наук	профессор-исследователь НИУ ВШЭ (онлайн)
120. Иванов Федор Ильич, кандидат физико-математических наук	доцент, академический руководитель образовательной программы «Информационная безопасность», старший научный сотрудник НИУ ВШЭ, научный сотрудник ИППИ РАН (онлайн)

От Федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский университет ИТМО», г. Санкт-Петербург

121. Алоджанц Александр Павлович, доктор физико-математических наук	профессор Института перспективных систем передачи данных, старший научный сотрудник национального центра когнитивных разработок Университета ИТМО (онлайн)
122. Козлов Сергей Аркадьевич, доктор физико-математических наук	декан факультета фотоники и оптоинформатики Университета ИТМО (онлайн)
123. Царёв Дмитрий Владимирович, кандидат физико-математических наук	ассистент Института перспективных систем передачи данных, младший научный сотрудник Лаборатории однофотонных детекторов и генераторов Университета ИТМО (онлайн)
124. Осипов Степан Валерьевич	студент магистратуры Университета ИТМО (онлайн)

От Федерального государственного автономного образовательного учреждения высшего образования «Новосибирский национальный исследовательский государственный университет», г. Новосибирск

125. Ашкарин Иван Николаевич	аспирант НГУ, инженер-исследователь лаборатории № 32 ИФП СО РАН (онлайн)

От Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)», г. Санкт-Петербург

126. Устинов Алексей Борисович, доктор физико-математических наук	доцент кафедры физической электроники и технологии СПбГЭТУ «ЛЭТИ» (онлайн)

От Федерального государственного бюджетного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых», г. Владимир

127. Аракелян Сергей Мартиросович, доктор физико-математических наук	заведующий кафедрой физики и прикладной математики ВлГУ (очно)

128. Крылов Владимир Павлович, доктор технических наук	профессор кафедры «Электроника, приборостроение и биотехнические системы» Института информационных технологий и радиоэлектроники ВлГУ, руководитель научно-образовательного центра «CALS в электронике» ВлГУ, главный научный сотрудник Управления научно-исследовательской деятельности ВлГУ (онлайн)

От Федерального государственного бюджетного образовательного учреждения высшего образования «Кубанский государственный университет», г. Краснодар

129. Строганова Елена Валерьевна, доктор физико-математических наук	декан физико-технического факультета Кубанского государственного университета (онлайн)

От Федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)», г. Москва

130. Денисенко Денис Витальевич	преподаватель МГТУ им. Н.Э. Баумана (очно)

От Федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет имени М.В. Ломоносова», г. Москва

131. Ожигов Юрий Игоревич, доктор физико-математических наук	профессор факультета вычислительной математики и кибернетики МГУ имени М.В. Ломоносова (онлайн)
132. Черепнев Михаил Алексеевич, доктор физико-математических наук	доцент факультета ВМК МГУ имени М.В. Ломоносова, научный сотрудник АО «Концерн «Автоматика» (очно)
133. Чижов Иван Владимирович, кандидат физико-математических наук	доцент факультета вычислительной математики и кибернетики МГУ имени М.В. Ломоносова, заместитель по научной работе руководителя лаборатории криптографии АО «НПК «Криптонит» (очно)
134. Ли Ваньшунь	аспирант факультета вычислительной математики и кибернетики МГУ имени М.В. Ломоносова (онлайн)
135. Мяо Хуэйхуэй	аспирант факультета вычислительной математики и кибернетики МГУ имени М.В. Ломоносова (онлайн)
136. Ю Цзянчуань	студент факультета вычислительной математики и кибернетики МГУ имени М.В. Ломоносова (онлайн)

От Федерального государственного бюджетного образовательного учреждения высшего образования «Петрозаводский государственный университет», г. Петрозаводск

137. Корзун Дмитрий Жоржевич, кандидат физико-математических наук	заместитель директора по науке Центра искусственного интеллекта, доцент Кафедры информатики и математического обеспечения Института математики и информационных технологий Петрозаводского государственного университета (онлайн)

От Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский политехнический университет Петра Великого», г. Санкт-Петербург

138. Рудской Андрей Иванович, академик РАН	ректор Санкт-Петербургского политехнического университета Петра Великого (очно)

От Федерального государственного бюджетного образовательного учреждения высшего образования «Тюменский государственный университет», г. Тюмень

139. Писарев Александр Дмитриевич, кандидат технических наук	доцент кафедры прикладной и технической физики, заведующий лабораторией пучково-плазменных технологий НОЦ «Нанотехнологии» ТюмГУ (онлайн)

От Федерального государственного бюджетного образовательного учреждения высшего образования «Ульяновский государственный университет», г. Ульяновск

140. Фотиади Андрей Александрович, кандидат физико-математических наук	ведущий научный сотрудник НИТИ Ульяновского государственного университета, старший научный сотрудник ФТИ им. А.Ф. Иоффе, senior scientist, Prof. University of Mons (Бельгия) (онлайн)

От Ферганского государственного университета (Узбекистан), г. Фергана

141. Отажонов Салим Мадрахимович, доктор физико-математических наук	профессор кафедры физики Ферганского государственного университета (онлайн)

От Центра квантовых технологий физического факультета МГУ имени М.В. Ломоносова, г. Москва

142. Сайгин Михаил Юрьевич, кандидат физико-математических наук, PhD	старший научный сотрудник Центра квантовых технологий физического факультета МГУ имени М.В. Ломоносова (очно)

От Terra Quantum AG (Швейцария)

143. Мельников Алексей Андреевич, PhD	руководитель научной группы Terra Quantum AG (Швейцария), научный сотрудник лаборатории микроструктурирования и субмикронных приборов ФТИАН им. К.А. Валиева РАН (онлайн)

От Акционерного общества «Информационные технологии и коммуникационные системы», г. Москва

144. Елисеев Владимир Леонидович, кандидат технических наук	руководитель Центра научных исследований и перспективных разработок АО «ИнфоТеКС», доцент кафедры Управления и интеллектуальных технологий ФГБОУ ВО «НИУ «МЭИ» (онлайн)
145. Растрыгин Сергей Евгеньевич	технический писатель АО «ИнфоТеКС» (онлайн)

От Акционерного общества «Концерн «Автоматика», г. Москва

146. Москвичев Андрей Иванович	заместитель генерального конструктора АО «Концерн «Автоматика» (онлайн)

От Акционерного общества «Научно-исследовательский институт микроэлектронной аппаратуры «Прогресс», г. Москва

147. Завалин Юрий Викторович	директор по производству АО «НИИМА «Прогресс» (онлайн)

От Акционерного общества «Научно-исследовательский институт молекулярной электроники», г. Москва, г. Зеленоград

148. Бокарев Валерий Павлович, доктор технических наук	начальник отдела службы главного конструктора АО «НИИМЭ», доцент базовой кафедры «Микро- и наноэлектроника» МФТИ (онлайн)
149. Исляйкин Андрей Михайлович, кандидат химических наук	начальник отдела разработки технологических процессов АО «НИИМЭ» (онлайн)

150. Колдаев Игорь Михайлович, кандидат физико-математических наук	ведущий специалист аппарата генерального директора АО «НИИМЭ» (онлайн)
151. Матюшкин Игорь Валерьевич, кандидат физико-математических наук	старший научный сотрудник АО «НИИМЭ» (онлайн)
152. Патюков Сергей Иванович, кандидат технических наук	начальник лаборатории отдела разработки технологических процессов АО «НИИМЭ» (онлайн)
153. Дорошин Владимир Викторович	инженер-конструктор разработки схем для источников питания АО «НИИМЭ» (онлайн)

От Акционерного общества «Научно-производственная компания «Криптонит», г. Москва

154. Шишкин Василий Алексеевич, кандидат физико-математических наук	руководитель лаборатории криптографии АО «НПК «Криптонит» (очно)

От Акционерного общества «Центральное конструкторское бюро «ДЕЙТОН», г. Москва, г. Зеленоград

155. Юдахин Юрий Анатольевич, доктор исторических наук	директор по научно-техническому развитию АО «ЦКБ «Дейтон» (онлайн)

От Акционерного общества «Экспериментальное научно-производственное объединение специализированные электронные системы», г. Москва

156. Давыдов Георгий Георгиевич, кандидат технических наук	ведущий научный сотрудник, и.о. заместителя начальника НТК-3 АО «ЭНПО СПЭЛС», старший научный сотрудник Центра экстремальной прикладной электроники НИЯУ МИФИ (онлайн)

От Акционерного общества «Юл-Ком Медиа», г. Москва

157. Ершов Андрей Владимирович, кандидат физико-математических наук	генеральный директор АО «Юл-Ком Медиа», доцент МФТИ (онлайн)

От Компании «Иннопрактика», г. Москва

158. Одиноков Алексей Васильевич	руководитель департамента по управлению интеллектуальной собственностью Компании «Иннопрактика» (очно)

От Некоммерческой организации Фонд развития центра разработки и коммерциализации новых технологий, г. Москва

159. Суетин Николай Владиславович, доктор физико-математических наук	вице-президент по науке и образованию Фонда «Сколково», ведущий научный сотрудник НИИЯФ МГУ (онлайн)

От Общества с ограниченной ответственностью «Газпромнефть - цифровые решения», г. С.-Петербург

160. Исмагилов Нияз Салаватович, кандидат физико-математических наук	руководитель развития технологий квантовых вычислений Дирекции цифрового инжиниринга ООО «Газпромнефть-ЦР» (онлайн)

От Общества с ограниченной ответственностью «Колибри», г. Москва, Сколково

161. Галицын Алексей Александрович, кандидат технических наук	генеральный директор ООО «Колибри» (очно)

От Общества с ограниченной ответственностью «Коннектор Оптикс», г. Санкт-Петербург

162. Карачинский Леонид Яковлевич, кандидат физико-математических наук	генеральный директор ООО «Коннектор Оптикс», старший научный сотрудник ФТИ им. А.Ф. Иоффе, старший научный сотрудник Университета ИТМО (онлайн)

От Общества с ограниченной ответственностью «КуРейт»

163. Петров Иван Витальевич	младший научный сотрудник Отдела теоретических исследований ООО «КуРэйт», студент магистратуры кафедры РКЦ ЛФИ МФТИ (онлайн)
164. Хыдырова Селби	научный сотрудник ООО «КуРэйт», аспирант кафедры МТ11 «Электронные технологии в машиностроении» МГТУ им. Н.Э. Баумана (онлайн)

От Общества с ограниченной ответственностью «НТ-МДТ Спектрум Инструментс», г. Москва, г. Зеленоград

165. Быков Виктор Александрович, доктор технических наук	почетный президент ООО «НТ-МДТ С.И.», научный консультант ООО «НТ-МДТ», президент Общероссийской общественной организации «Нанотехнологическое общество России» (ООО «НОР») (онлайн)

ПОВЕСТКА ДНЯ:

Академик РАН Красников Геннадий Яковлевич (АО «НИИМЭ»). Открытие заседания.
(1) д.ф.-м.н. Подольский Владимир Владимирович (МИАН; НИУ ВШЭ). Задачи теории сложности вычислений и алгоритм Гровера.
(2) к.ф.-м.н. Чернявский Андрей Юрьевич, Фастовец Дмитрий Владиславович, д.ф.-м.н. Богданов Юрий Иванович (ФТИАН им. К.А. Валиева РАН). Разработка квантовых алгоритмов в эпоху NISQ.
(3) к.ф.-м.н. Бетеров Илья Игоревич (ИФП СО РАН), Ашкарин Иван Николаевич, Журавлев Никита Алексеевич (НГУ; ИФП СО РАН), к.ф.-м.н. Дучков Антон Альбертович (ИНГГ СО РАН; НГУ), член-корр. РАН Рябцев Игорь Ильич (ИФП СО РАН). Проблемы квантового ускорения для алгоритмов, реализуемых на NISQ-процессорах.
(4) к.ф.-м.н., PhD Сайгин Михаил Юрьевич (Центр квантовых технологий Физического факультета МГУ имени М.В. Ломоносова). Квантовые алгоритмы для решения задач материаловедения.
(5) к.ф.-м.н. Федоров Алексей Константинович (РКЦ). Устойчивость квантовых вычислений к шумам: вариационные алгоритмы и коррекция ошибок.
(6) PhD Мельников Алексей Андреевич (ФТИАН им. К.А. Валиева РАН, Terra Quantum AG (Швейцария)), к.ф.-м.н. Федичкин Леонид Евгеньевич (МФТИ, ФТИАН им. К.А. Валиева РАН). Методы машинного обучения для решения задач квантовой информатики.
(7) д.ф.-м.н. Трушечкин Антон Сергеевич (МИАН). Квантовая и постквантовая криптография.
(8) д.ф.-м.н. Черепнев Михаил Алексеевич (МГУ имени М.В. Ломоносова; АО «Концерн «Автоматика»). Квантовые алгоритмы и постквантовая криптография.
(9) к.ф.-м.н. Чижов Иван Владимирович (МГУ имени М.В. Ломоносова; АО «НПК «Криптонит»), к.ф.-м.н. Шишкин Василий Алексеевич (АО «НПК «Криптонит»). Постквантовая криптография. Задачи, перспективы, стандартизация.
(10) д.ф.-м.н. Кабатянский Григорий Анатольевич (Сколтех). Постквантовая криптография на кодах и решетках: общее и различия.
(11) д.ф.-м.н. Аблаев Фарид Мансурович (Казанский федеральный университет; ФИЦ КазНЦ РАН), профессор РАН, д.ф.-м.н. Калачёв Алексей Алексеевич (ФИЦ КазНЦ РАН). Квантовое хеширование для безопасной передачи информации. Реализация квантовых хеш-функций на основе состояний высокой размерности.

(12) к.ф.-м.н. Киктенко Евгений Олегович (РКЦ; МИАН). Теоретически стойкие алгоритмы на основе квантового распределения ключей.
(13) д.ф.-м.н. Ожигов Юрий Игоревич (МГУ имени М.В. Ломоносова). О фундаментальной роли проекта квантового компьютера для России.
Общая дискуссия. Подведение итогов заседания Научного совета.

(академик РАН Г.Я. Красников; академик РАН А.А. Горбацевич;
академик РАН А.С. Холево; академик РАН А.И. Рудской;
академик РАН В.А. Сойфер; академик РАН Р.А. Сурис;
член-корр. РАН И.В. Волович; член-корр. РАН Е.С. Горнев;
член-корр. РАН Е.Н. Николаев; профессор РАН, д.ф.-м.н. А.А. Калачёв;
профессор РАН, д.ф.-м.н. А.Н. Печень; д.ф.-м.н. Ф.М. Аблаев;
д.ф.-м.н. С.М. Аракелян; д.ф.-м.н. А.К. Звездин; д.ф.-м.н. Г.А. Кабатянский;
д.х.н. А.Г. Мартынов; д.ф.-м.н. Ю.И. Ожигов; д.ф.-м.н. В.В. Подольский;
д.ф.-м.н. Н.В. Суетин; д.ф.-м.н. А.С. Трушечкин; д.ф.-м.н. Э.Б. Фельдман;
д.ф.-м.н. М.А. Черепнев; к.ф.-м.н. И.И. Бетеров; к.ф.-м.н. Е.О. Киктенко;
к.ф.-м.н. И.В. Матюшкин; PhD А.А. Мельников; к.ф.-м.н. И.С. Мухин;
к.ф.-м.н. М.А. Ремнев; к.ф.-м.н., PhD М.Ю. Сайгин; к.ф.-м.н. А.К. Федоров;
к.ф.-м.н. А.Ю. Чернявский; к.ф.-м.н. И.В. Чижов; Д.В. Фастовец)

1. В заседании приняли участие 28 из 53 членов Бюро Совета и членов Совета, а также 137 приглашенных ученых и специалиста – всего 165 человек из 102 организаций и их подразделений. В обсуждении повестки дня участвовало 33 человека.
2. Во вступительном слове при открытии заседания председатель Совета, академик РАН Г.Я. Красников отметил существенную роль теоретической разработки и практической реализации квантовых и постквантовых алгоритмов в развитии квантовых технологий.
3. (1) д.ф.-м.н. В.В. Подольский (МИАН; НИУ ВШЭ) привел обзор в области задач теории сложности вычислений – сложностные классы N и NP и алгоритма Гровера применительно к решению задач перебора и NP-полных задач. В результате выявлено, что алгоритм Гровера позволяет получить квадратичное ускорение перебора в модели с черным ящиком. При этом для модели черного ящика дальнейшее ускорение невозможно. Если использовать внутреннюю структуру полиномиального алгоритма A(x, y), то ящик перестает быть черным и для конкретной NP-полной задачи теоретически возможно дальнейшее ускорение. Для этого нужны новые идеи.
4. (2) к.ф.-м.н. А.Ю. Чернявский (ФТИАН им. К.А. Валиева РАН) доложил о том, что Топ-10 текущих квантовых процессоров содержат от 32 до 127 кубитов с точностью операций примерно до 99,9%, что относит их к так называемому классу NISQ (noisy intermediate-scale quantum). Такие параметры ещё не позволяют реализовать полномасштабные «классические» квантовые алгоритмы, такие как алгоритмы Шора и Гровера, в связи с чем активно развиваются альтернативные NISQ-подходы: например, квантовый отжиг, бозонный сэмплинг и квантовые вариационные алгоритмы (VQA).

   В основе VQA лежит минимизация (на классическом компьютере) целевых функций, получаемых как результат параметризованного квантового вычисления. К VQA могут быть сведены важные задачи из различных областей: многочастичная физика и химия, машинное обучение, комбинаторная

оптимизация, численные методы, финансы. Такие задачи «классических» квантовых алгоритмов, как факторизация и решение систем линейных алгебраических уравнений (СЛАУ), также перекладываются на VQA.

Несмотря на яркие перспективы, реалистичная оценка практической применимости квантовых алгоритмов является сложнейшей задачей, дающей иногда неожиданные результаты: так, например, для квантового превосходства HHL-алгоритма решения СЛАУ в задаче вычисления электромагнитного сечение рассеяния металлической цели могут понадобиться порядка 10^8 идеальных кубитов и 10^{28} тактов идеальных квантовых операций (Scherer, Artur, et al. «Concrete resource analysis of the quantum linear-system algorithm used to compute the electromagnetic scattering cross section of a 2D target.» Quantum Information Processing 16.3 (2017): 1-65). Для VQA алгоритмов появляются и новые трудности, связанные с классической оптимизацией: например, так называемые бесплодные равнины (barren plateaus), когда в силу экспоненциального роста размерности падает градиент целевой функции. Всё это говорит о критической важности реалистичных оценок ресурсов и экспериментов на текущих NISQ-устройствах. Во ФТИАН им. К.А. Валиева РАН ведутся такие работы по тестированию и анализу NISQ-алгоритмов, в том числе алгоритма TTN (Tree Tensor Networks), основанного на идеях нейронных сетей и классической многопараметрической оптимизации функции потерь.

На облачной платформе IBM Q 5 Tenerife был реализован квантовый алгоритм TTN для решения тестовой задачи (Fisher's Iris data set) классификации цветов ириса (Fastovets, D. V., et al. International Conference on Micro-and Nano-Electronics 2018. Vol. 11022. SPIE, 2019). Были обучены три бинарных классификатора для попарного разделения представленных в задаче классов, а также предложено многоклассовое обобщение алгоритма. Полученный высокий уровень точности классификации говорит о перспективе применения данного подхода для решения и более сложных задач. Однако стоит отметить, что данный алгоритм получает превосходство над классическим аналогом лишь на задачах, которым на вход подаются «квантовые» данные.

5. (3) к.ф.-м.н. И.И. Бетеров (ИФП СО РАН) сообщил, что в настоящее время ведутся интенсивные исследования квантовых алгоритмов, которые могут быть реализованы на уже существующих или создаваемых квантовых процессорах промежуточного масштаба с высоким уровнем шумов (так называемых NISQ-процессорах). Наиболее перспективны алгоритмы, относящиеся к так называемому BQP-типу – успешно реализуемых на квантовом компьютере с вероятностью получения правильного ответа более 2/3. Несмотря на разнообразие квантовых алгоритмов, большая их часть может быть сведена лишь к нескольким основным подходам – например, квантовому преобразованию Фурье, алгоритму Гровера или вариационному алгоритму. Большой интерес представляет решение оптимизационных задач с помощью квантового компьютера, например, ведутся работы по применению квантово-вычислительных подходов в геофизике.

   В докладе были также представлены оригинальные результаты по выполнению квантовой оценки фазы итерационным методом на процессоре IBM с последующей классической коррекцией вычислительных ошибок. В результате, удалось получить корректную последовательность из 25 битов, задающих собственное значение матрицы 2x2.

6. (4) к.ф.-м.н., PhD М.Ю. Сайгин (Центр квантовых технологий Физического факультета МГУ имени М.В. Ломоносова) сообщил, что методы решения прикладных задач материаловедения представляют собой область, требующую большие вычислительные мощности и специализированные подходы расчётов. Многие актуальные задачи в этой области не могут быть решены точно классическими методами и поэтому в последние несколько лет именно материаловедение притягивает большой интерес учёных, работающих в области квантовых вычислений. Примерами важных задач материаловедения являются расчёт электронных уровней энергий молекул и колебательных спектров.

   Для решения первой задачи на квантовых вычислителях среднего масштаба с шумами и ошибками, которые могут быть реализованы в ближайшие годы, предложено использовать вариационные квантовые алгоритмы. Были выполнены эксперименты по демонстрации работы вариационных квантовых алгоритмов для задач малой сложности, которые с лёгкостью могут быть решены классическими методами. Нерешённой проблемой использования вариационных алгоритмов для расчёта более сложных квантовых систем является принципиальная сложность оптимизации – так называемое бесплодное плато. На сегодняшний день исследования, направленные на решение этой проблемы, продолжаются.

   Для расчётов колебательных спектров молекул предложен квантового алгоритм, основанный модификации схемы, реализующей гауссовый бозонный сэмплинг. Вместе с тем, с развитием более совершенных классических алгоритмов, в т.ч. вдохновлённых квантовыми системами, целесообразность практической реализации квантового алгоритма на реальных квантовых устройствах и их масштаб остаётся неисследованной.

   Таким образом, использование квантовых подходов для решения прикладных задач материаловедения как на современном этапе развития технологий и алгоритмов, так и в ближайшем будущем вряд ли сможет быть более эффективным по сравнению с классическими методами. По этой причине научные разработки новых квантовых алгоритмов и принципиально инновационных подходов использования квантовых особенностей физических систем для решения задач материаловедения представляется наиболее важным наравне с совершенствованием квантового «железа».
7. (5) к.ф.-м.н. А.К. Федоров (РКЦ) привел обзор развития квантовых вычислений в контексте потенциальных приложений в области оптимизации, моделирования и машинного обучения. Были представлены полученные результаты по разработке вариационных квантовых алгоритмов для NISQ-устройств. В частности, были показаны примеры применения квантовых вычислений для решения задач по сборке генома, квантовой химии (моделирования реакций) и обучению генеративных нейронных сетей, применяемых в химии. Рассмотрены различные подходы к коррекции ошибок в квантовых вычислительных устройствах. Показан пример реализации семейства кодов коррекции ошибок, которые позволили продемонстрировать сохранение квантового состояния.
8. (6) PhD А.А. Мельников (ФТИАН им. К.А. Валиева РАН, Terra Quantum AG (Швейцария)) сообщил, что методы машинного обучения активно используются для решения задач квантовой информации. В докладе были продемонстрированы примеры такие задач из следующих областей: дизайн компонент квантового

компьютера, повышение устойчивости квантовой криптографии, и нахождение квантового преимущества. В задаче дизайна компонент квантового компьютера был рассмотрен дизайн фотонного квантового компьютера. Фотонный квантовый компьютер является перспективным направлением: он работает при комнатной температуре, сохраняет когерентность на больших временах и расстояниях, имеет высокие скорости генерации кубитов. Тем не менее, фотонный квантовый компьютер обладает существенным недостатком: существует сложность генерации запутанных многокубитных состояний. Чтобы преодолеть этот недостаток предложено использование запутанных трехфотонных состояний для создания запутанных состояний произвольного размера. Оптические элементы, расположенные в определенной последовательности, могут позволить создать такие состояния. В докладе показано, что нахождение новых экспериментов по созданию запутанных фотонов — планирование в сложной сети возможностей расположения оптических элементов. Наши результаты показали, что обучение с подкреплением автономно учится производить дизайн квантовых состояний по запросу. Параллельно, разработанный алгоритм обучения с подкреплением оптимизирует длину эксперимента. Также продемонстрировано, что обучение с подкреплением способно к трансферному обучению в задаче дизайна компонент квантового компьютера. Решение, предоставленное машинным обучением, позволило найти больше важных дизайнов экспериментов и найти компактные реализации квантовых экспериментов. Таким образом, разработанные нами алгоритмы машинного обучения позволяют участвовать в ускорении создания полномасштабного квантового компьютера.

9. (7) д.ф.-м.н. А.С. Трушечкин (МИАН) сообщил, что существенная часть традиционной криптографии окажется под угрозой после появления полномасштабного квантового компьютера. Существует два способа защиты информации от взлома в том числе и на квантовом компьютере: квантовая криптография и постквантовая криптография. Постквантовая криптография основана на вычислительных задачах, которые сложно решить даже на квантовом компьютере. Так, к постквантовой криптографии относят симметричную криптографию, так как хороший симметричный шифр не должен допускать анализ, существенно лучший, чем полный перебор ключей. Квантовый алгоритм Гровера дает лишь квадратичное ускорение при полном переборе, т. е. появление квантового компьютера нивелируется двукратным увеличением длины ключа. Ведутся исследования постквантовых криптографических систем с открытым ключом. Их преимущество по сравнению с квантовой криптографией заключается в том, что они не требуют нового дорогостоящего оборудования, такого как, например, однофотонные детекторы. Однако они сталкиваются с вызовами, связанными с большими длинами ключей, необходимостью работать над надежной реализацией, а также строгими доказательствами стойкости. Квантовая криптография предлагает защиту информации, основывающуюся на принципах квантовой механики. В отличие от систем постквантовой криптографии ее стойкость доказана строго и системы квантовой криптографии невозможно взломать задним числом. То есть, выполнив определенный объем вычислений, любой классический шифр (кроме одноразового блокнота) можно прочитать, пусть и спустя время. Но если сеанс квантовой криптографии не взломали за время этого сеанса, то созданный

в сеансе ключ является стойким навсегда, нет таких вычислений, проведя которые его возможно было бы узнать позже. Для случая идеального оборудования стойкость протокола квантовой криптографии BB84 строго доказана в ряде работ разных авторов 1996-2005 гг. Но для практического применения квантовой криптографии необходимо иметь доказанную стойкость при реалистичных предположениях об аппаратуре, над чем научное сообщество работает в настоящее время. Докладчик сообщил о своих результатах в области доказательства стойкости метода обманных состояний, который решает проблему многофотонных импульсов, а также стойкости протокола BB84 при однофотонных детекторах с отличающимися эффективностями, что потребовало создания принципиально новых методов. Указано, что на данный момент не существует доказательства стойкости, которое бы учитывало сразу все неидеальности оборудования (детекторов и источника). Развивается аппаратнонезависимая квантовая криптография, которая использует только самые базовые предположения об аппаратуре (например, отсутствие прямых каналов утечек), но требует условий, при которых можно подтвердить нарушение неравенств Белла без «лазеек». Таким образом, и в квантовой, и в постквантовой криптографии предстоит еще большая работа по устранению уязвимостей на уровне технического воплощения.

10. (8) д.ф.-м.н. М.А. Черепнев (МГУ имени М.В. Ломоносова; АО «Концерн «Автоматика») сообщил, что ситуация с квантовым компьютером сейчас отличается от ситуации с обычным компьютером в середине 20 века и ранее. Первые компьютеры хоть и медленно, но работали (например, суммирующая машина Паскаля 1642 г. осуществляла арифметические преобразования пятизначных десятичных чисел (около 50 машин было сделано, 15 из них продано), разностная машина Беббиджа 1822 г. вычисляла значения многочленов до 7 степени, ЭВМ “Bombe”, “Colossus” 1940-43 гг. осуществляли взлом немецких шифровальных машин Enigma и Lorenz), а первые квантовые – нет. Кроме того, имеются принципиальные нерешенные проблемы, препятствующие построению квантового компьютера (проблема исправления ошибок, связанная с невозможностью копирования состояния, влиянием кубитов и их содержания на вычислительную среду, проблема считывания состояния, неустойчивость физических устройств и вычислений). Если $1/k^s$ это вероятность успешного срабатывания одного кубита в s шагах программы для n кубитного процессора (вычисляющего функцию от n битного аргумента). Тогда для того, чтобы получить хотя бы один правильный (по всем кубитам) результат нам понадобиться в среднем произвести k^{sn} квантовых шагов. При $k^s > 2$, это больше, чем количество всех возможных аргументов данной задачи. Значительного выигрыша по сравнению с обычным компьютером, последовательно обрабатывающим эти аргументы, мы не получаем.

    Достоверность одного шага квантового компьютера (Fidelity) зависит от числа кубитов, их содержимого и от номера шага (не исследовано).

    Для реализации конкретных практических задач не нужен полноценный квантовый компьютер. (Jiuzhang 2020 фотоны более стабильны, не требуют охлаждения, лучше масштабируются).

    Представляется реализуемой технология «Выстрел»: Одна квантовая операция с последующим анализом результатов на обычном компьютере. Уменьшаются проблемы с нагревом, количеством ошибок, проще создать

идеальные условия. Практическая реализация одной операции на квантовой системе, принимающей 2^{500} состояний, была бы принципиальным прорывом для решения прикладных задач. Правда, при таком подходе известные квантовые алгоритмы Шора, Гровера остаются непрактичными. Нужны будут другие алгоритмы.

40 лет изучения свойств квантовых вычислителей привели к тому, что постквантовая эра в криптографии уже началась. Угрозы в ней связаны с лавинообразным ростом коммуникационного трафика среди всех людей. Для смягчения этих угроз предлагаются децентрализованные системы защиты информации. В децентрализованной системе методы защиты информации те же, но квантовый компьютер «к каждому не приставишь» (принцип распараллеленной защиты: чтобы сломать общую защиту надо сломать защиту каждого). Децентрализованное распределение ключей (хеш старого ключа с новой общей секретной информацией). Децентрализованное шифрование (разделение при помощи пороговых схем с последующей отправкой разными маршрутами через списки доверия). Децентрализованная аутентификация (каждый подписывает весь свой цифровой след в сетях).

В случае исключения получения практического результата как цели исследований, разрозненные усилия физиков и математиков будут наполнять знаниями международную базу знаний, увеличивая риски ее использования в деструктивных целях.

11. (9) к.ф.-м.н. И.В. Чижов (МГУ имени М.В. Ломоносова; АО «НПК «Криптонит») сообщил о текущих работах по стандартизации в области постквантовой криптографии в рамках рабочей группы «Постквантовые криптографические механизмы» Технического комитета № 26. Рабочая группа занимается вопросами стандартизации объектов, относящихся к постквантовым криптографическим механизмам (шифрование, аутентификация, имитозащита, электронная подпись и т.п.). Постквантовый криптографический механизм – такой криптографический механизм, который является стойким как в классической модели противника, так и в квантовой модели противника. Квантовая модель предполагает, что противник имеет доступ к квантовому вычислителю и способен на нём запускать эффективные (полиномиальные) алгоритмы.

Все криптографические механизмы можно разделить на два типа: с секретным ключом (симметричная криптография) и открытым ключом. К механизмам с секретным ключом относятся разного рода блочные, поточные шифры, криптографические хеш-функции.

Механизмы с открытым ключом на практике представлены схемами инкапсуляции ключа, и схемами электронной подписи.

Задачи синтеза постквантовых криптографических механизмов с секретным ключом не стоит, так как в случае для защиты от атак с использованием квантового компьютера достаточно будет увеличить длину секретного ключа.

В квантовой модели задачи целочисленной факторизации и дискретного логарифмирования, на сложности которых основана стойкость практически используемых криптографических механизмов с открытым ключом, имеют эффективное решение (алгоритм Питера Шора, 1997 г.). Снижение сложности принципиально, так как исчезнет экспоненциальный разрыв между вычислительной сложностью алгоритмов легального абонента и злоумышленника. Решить эту проблему увеличением ключа нельзя. Поэтому

стоит задача разработать схемы электронной подписи и обмена ключами, стойкие как в квантовой, так и в классической модели. В рамках группы «Постквантовые криптографические механизмы» ТК 26 как раз ведутся работы именно по этим направлениям: создание новых стандартов постквантовой электронной подписи и постквантового механизма инкапсуляции ключа.

Для постквантовых схем электронной подписи наиболее перспективными являются следующие направления: криптографические механизмы на основе кодов, исправляющих ошибки и алгебраических решёток.

Для постквантовых схем инкапсуляции ключа наиболее перспективными являются следующие направления: криптографические механизмы на основе кодов, исправляющих ошибки и алгебраических решёток, а также на основе изогений эллиптических кривых.

Можно выделить следующие основные направления и задачи в области постквантовой криптографии: (1) разработка стойких постквантовых схем электронной подписи с небольшой длиной ключа и размером подписи; (2) Развитие аппарата оценки стойкости постквантовых криптографических механизмов против атак по побочным каналам; (3) разработка постквантовых криптографических механизмов, устойчивых к атакам по побочным каналам; (4) развитие аппарата доказуемой стойкости для постквантовых криптографических механизмов; (5) интеграция в существующие приложения и сетевые протоколы.

12. (10) д.ф.-м.н. Г.А. Кабатянский (Сколтех) сообщил о сходстве и различиях постквантовой криптографии на кодах и решетках. Современная криптография ведет свое начало от двух работ конца 70-х годов прошлого века: «Новые направления в современной криптографии» Диффи и Хеллмана (1976) и RSA (1978). Идея, идущая от Диффи и Хелмана, состояла в том, чтобы взять NP-трудную задачу, у которой для некоторого достаточно большого множества входов есть простое (полиномиальное) решение и «замаскировать» эти входы как случайные. В качестве примера они взяли задачу о рюкзаке, но соответствующую криптосистему через несколько лет сломали. Тем интереснее, что система МакЭлиса (1978), также основанная на идее рюкзака, но только алгебраического, оказалась не только до сих пор не сломана, но остается одним из главных претендентов на стандарт пост-квантовой криптографии. Т.е. эта система появилась задолго до того, как квантовые компьютеры возникли как теоретическая угроза криптографии. Хотя у нее имеются довольно очевидные недостатки – большой размер ключа (и открытого, и закрытого) и превышение длины шифрованного сообщения над длиной секретной информации, но есть и два достоинства: быстрая обработка и, самое главное, неизвестно (пока?) как ее взламывать на квантовом компьютере. Сравнительно недавно возник похожий класс криптосистем – криптография на решетках. NP-трудные задачи, на которых основана «решетчатая» криптография это поиск ближайшего вектора решетки к данному евклидову вектору, и задача нахождения длины кратчайшего вектора решетки. Здесь имеются глубокие аналогии с проблемой декодирования случайных кодов, что также обсуждалось в докладе. Так же были выделены открытые задачи, представляющие интерес с точки зрения построения криптосистем, устойчивых к атакам на квантовом компьютере.

13. (11) д.ф.-м.н. Ф.М. Аблаев (Казанский федеральный университет; ФИЦ КазНЦ РАН), профессор РАН, д.ф.-м.н. А.А. Калачёв (ФИЦ КазНЦ РАН) доложили о об основных результатах исследования – разработке метода генерации квантовых хеш-функций и экспериментальной реализации конкретной квантовой хеш-функции.

1) Квантовая хеш-функция – это обобщение понятия криптографической хеш-функции на квантовый случай. Криптографическая хеш-функция – это функция: а) сжимающая, б) сложно обратимая и в) коллизия-устойчивая. Доказательство свойства «сложной обратимости» – открытая проблема. Доказательство свойства «сложной обратимости» для некоторой функции будет означать, что класс сложности P не совпадет с классом NP. Квантовая хеш-функция отображает исходную информацию (последовательности длины n) в квантовые s-кубитовые состояния и должна удовлетворять следующим двум требованиям:

а) Величина s должна быть значительно меньше n. Это обеспечивает (в силу теоремы Холево) свойство сложной обратимости в случае квантовой хеш-функции.

б) Требование попарной epsilon-ортогональности квантовых состояний (образов исходных последовательностей). Это требование обеспечивает свойство коллизия-устойчивости.

2) Разработан метод генерации квантовых хеш-функций с необходимыми свойствами. Проведен анализ свойств квантовых хеш-функций. Численные параметры (значения величин фаз квантового состояния) являются исходными параметрами для реализации квантовой хеш-функции.

3) Экспериментальная реализация квантовых хеш-функций выполнена с использованием последовательности однофотонных кубитов, генерируемых в процессе спонтанного параметрического рассеяния света. При этом управление состояниями кубитов в базисе орбитального углового момента света осуществлялось через пространственную модуляцию излучения накачки, что позволяет достичь максимальной эффективности условного приготовления фотонов. Получено хорошее согласие теории и эксперимента при исследовании зависимости вероятности коллизии хеш-функции от числа кубитов s. Результат практически не зависит от величины орбитального момента света, что открывает перспективу использования мультиплексирования для повышения скорости обработки информации.

4) Публикация: D. A. Turaykhanov, D. O. Akat'ev, A. V. Vasiliev, F. M. Ablayev, and A. A. Kalachev. Quantum hashing via single-photon states with orbital angular momentum // Physical Review A, 104, 052606(1-8) (2021).

5) Планы исследований (теоретические): (1) построение эффективных криптографических протоколов; (2) разработка эффективных квантовых алгоритмов на основе квантового хеширования; (3) разработка алгоритмов обработки больших данных на основе квантового хеширования. Наши первые результаты показывают, что методы квантового хеширования позволяют значительно экономить число используемых кубитов при квантовом поиске. Для разработки квантовых алгоритмов обработки больших данных ведется разработка квантового локально чувствительного хеширования (local sensitive hashing – LSH).

6) Планы исследований (экспериментальные): реализация разработанных протоколов, в том числе с использованием многомерных квантовых состояний (кудитов).

14. (12) к.ф.-м.н. Е.О. Киктенко (РКЦ; МИАН) сообщил, что на сегодняшний день достигнут ряд важных теоретических результатов в области построения алгоритмов, обладающих доказуемой теоретической стойкостью, построенных на основе технологии квантового распределения ключей. В частности, разработан протокол распределенного реестра, обладающего византийской отказоустойчивостью в случае, если количество злоумышленников внутри сети меньше трети от общего числа узлов в сети. Также разработан информационно теоретически стойкий протокол квантовой цифровой подписи, для которого в явном виде получены верхние границы на вероятности успешной подделки подписи и отказа от авторства. Были продемонстрированы величины потребления квантово-сгенерированный симметричных ключей для создания одной пары сообщение-подпись. Данные величины согласуются с показателями производительности современных устройств квантового распределения ключей. Сделаны общие выводы о важности информационно-теоретически стойких алгоритмов.
15. (13) д.ф.-м.н. Ю.И. Ожигов (МГУ имени М.В. Ломоносова) сообщил, что сложность квантового состояния F есть число кубитов в его запутанном ядре, редуцированное наиболее эффективным каноническим преобразованием. Точность квантового состояния — число его возможных копий. Сложность и точность связаны соотношением $A(F)\,C(F) < Q$, где Q – безразмерная константа, которую предстоит найти экспериментально, как наибольшее число кубитов, для которых алгоритм Гровера дает верный ответ. Судя по имеющимся экспериментам, Q не превосходит $20 – 30$. Малая величина Q не позволяет практически реализовать квантовое ускорение в духе Шора и Гровера, но открывает совершенно новые возможности для компьютерного моделирования сложных систем на квантовом уровне с предсказательной силой. Это особенно важно для нашей страны, так как позволяет преодолеть известное отставание.

16. При подведении итогов заседания Председатель Совета, академик-секретарь ОНИТ РАН, академик РАН Г.Я. Красников отметил высокий научно-технический уровень доложенных результатов, выразил уверенность в усилении сотрудничества между организациями и предприятиями в области совершенствования квантовых и постквантовых алгоритмов.

РЕШИЛИ:

1. Принять к сведению полученную в ходе заседания информацию.
2. Рекомендовать докладчикам предоставить презентации к докладам для размещения на сайте Совета.
3. По предложению к.ф.-м.н. А.К. Федорова (РКЦ) рассмотреть вопрос о новых задачах, проблемах и результатах в области реализации квантовых алгоритмов на одном из заседаний Совета.
4. Поддержать инициативы д.ф.-м.н. Ю.И. Ожигова (МГУ имени М.В. Ломоносова):

– организовать проект по реализации экспериментального определения границы применимости квантовой теории путем создания оптических полостей квантовой электродинамики для манипуляций с отдельными атомами ^{85}Rb и проверки первых принципов квантовой механики на числе кубитов, превосходящих 10;

– развивать проект создания квантового компьютера путем интенсификации междисциплинарное взаимодействие с химиками и биологами в части методов компьютерного моделирования сложных систем на квантовом уровне;

– организовать проект по реализации отечественного аналога архива препринтов arxiv.org, рекомендовать разработать программную оболочку факультету Вычислительной математики и кибернетики МГУ имени М.В. Ломоносова.

5. Вышеприведенные результаты передать в Президиум РАН, заинтересованным Научным советам РАН (отделений РАН) и в профильные Министерства.

Ученый секретарь Совета,
к.т.н. Тельминов О.А.