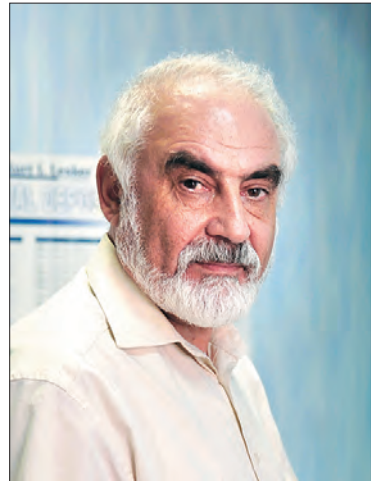




Что сказала Alice?

В педагогическом университете разрабатываются уникальные квантово-криптографические системы связи

Два года назад мы познакомили читателей "Поиска" с исследованиями, которые ведутся на кафедре общей и экспериментальной физики Московского педагогического государственного университета под руководством профессора, доктора физико-



математических наук Григория Гольцмана. Тогда поводом для публикации послужила небольшая заметка об успешных космических экспериментах зарубежных ученых в области квантовой коммуникации. Как оказалось, достижения российских исследователей были даже "круче", о чем мы с удовольствием и рассказали ("Поиск" №36, 2013). Выяснилось, что на физическом факультете МПГУ не только готовят будущих преподавателей физики, но и создают науку мирового уровня, свидетельством чему - многочисленные статьи в зарубежных рецензируемых журналах, таких как *Nature Photonics*, *Nature Communications*, *Scientific Reports*, *Applied Physics Letters* и др. Одновременно здесь работают и над решением вполне практических задач - тонкопленочные сверхпроводящие однофотонные детекторы, созданные под руководством Григория Гольцмана, стали визитной карточкой кафедры общей и экспериментальной физики и открытой на ее базе радиофизической лаборатории МПГУ, а также компании "Сверхпроводниковые нанотехнологии" ("Сконтел"), которая поставляет системы и приборы на базе этих детекторов во многие исследовательские центры мира.

В конце 2014 года очередной проект коллектива ученых МПГУ - "Разработка и исследование нового поколения квантово-криптографических систем на основе сверхбыстрых и сверхчувствительных гибридных сверхпроводниково-нанодетекторов" - получил поддержку Минобрнауки в рамках ФЦП "Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014-2020 годы" по мероприятию 2.2 "Поддержка исследований в рамках сотрудничества с государствами - членами Европейского союза". Руководит реализацией этой работы с российской стороны Григорий Гольцман, а выполняется она в сотрудничестве с коллегами из Технологического института г. Карлсруэ (*Karlsruhe Institute of Technology*), Германия.

Целью исследований является ни много ни мало - создание действующего прототипа квантово-криптографической системы связи (предельная дальность - 320 км) с использованием волно-

водных сверхпроводящих однофотонных детекторов (WSSPD) с улучшенными характеристиками.

О деталях проекта корреспондент "Поиска" расспросил Григория Гольцмана.

- Григорий Наумович, как получилось, что вы занялись квантовой криптографией?

- Это произошло не случайно. Как вы знаете, созданная на базе кафедры компания "Сконтел" не первый год выводит на рынок детекторы - счетчики фотонов, которые являются результатом наших предыдущих фундаментальных исследований. Как выяснилось, покупатели из разных стран используют эти детекторы для систем квантовой криптографии. Это обстоятельство и нас мотивировало обратить более пристальное внимание на такую область. В квантовой криптографии характеристики систем приема-передачи данных в значительной мере определяются детекторами, а уж их-то мы научились делать!

- Тогда в чем новизна работы, поддержанной грантом Минобрнауки?

- Новизна кроется во второй части названия проекта. Нами выбрано направление исследований волноводных сверхпроводниковых однофотонных детекторов на чипе для создания на их основе лабораторной модели системы распределения квантового ключа с поляризационным кодированием сигнала и использованием ловушечных состояний. Работа в этом направлении началась не сегодня и не вчера. Первая публикация на эту тему появилась в декабре 2012 года. Тогда мы начали сотрудничество с Иельским университетом, одна из научных групп которого занималась устройствами на оптических волноводах. Вообще волноводная техника очень давно и хорошо развита в микроволновом диапазоне. Волноводы в оптике - это по сути наноструктуры, которые с успехом используются в фотонике. Я предложил коллегам сделать следующую работу:

поставить наш детектор (счетчик фотонов) на волновод. Мы эту задачу выполнили, и в декабре 2012 года в *Nature Communications* была опубликована совместная статья. Ее первым автором был молодой немецкий ученый Вольфрам Пернайс (*Wolfram Pernice*), в то время аспирант Иельского университета. Впоследствии, уже в качестве профессора, он вернулся в Германию и продолжил исследования в Технологическом институте города Карлсруэ. Вместе с ним в Европу "переехала" и наша совместная работа. Мы увидели тогда, что если одно устройство разместить на волноводе, то и другие элементы, которые обычно делают на большом оптическом столе (с линзами, зеркалами и пр.), можно сделать в виде

малых структур на чипе. То есть это уже даже не просто оптика, а фотоника, но тоже на чипах. И тогда мы поняли, что может возникнуть новый тип устройств в нанопотонике - однофотонное устройство на чипе. Справедливости ради надо отметить, что с подобными устройствами сегодня работают и другие научные группы, но первыми были наша группа и группа из Голландии.

- То есть идея родилась из практики?

- Это, с одной стороны, техническая задача. Но часто при решении таких задач возникают фундаментальные вопросы, работа над которыми, в свою очередь, приводит к разработке новых технологий. В данном случае "сыграла" техническая идея перенести оптические схемы в квантовой оптике на чип и максимально их миниатюризировать. В дальнейшем, я думаю, и квантовые вычисления, и квантовый компьютер на чипе на одиночных фотонах получат распространение.

- Как вы делите сферы влияния с немецкими партнерами?

- Мы их не делим. Есть один элемент, который делается только у нас, поскольку материал, на основе которого изготовлен детектор, - это только наш вклад. Но в других вещах обе группы работают сообща. Мы сопоставляем полученные результаты, обмениваемся мнениями, люди ездят туда и сюда, ведут исследования там и здесь... Другими словами, обе группы умеют все и делают работу поровну.

- Квантовая криптография - молодое научное направление. Время от времени сообщается

о том, что в оптоволокну этот результат был повторен на расстояние 250 км. Квантовая криптография - это передача квантового ключа, который зашифрован в квантовых состояниях фотонов и передается по волоконной линии. Дальность передачи зависит от характеристик детектора, который в идеале должен принимать каждый фотон. Но он пропускает, поэтому приходится сокращать расстояния... Мы же обнаружили, что гораздо проще получить 100-процентную квантовую эффективность не на оптоволокну, а на волноводе, чтобы каждый фотон считался, детектировался. Идея состоит в том, чтобы совместить детектор на волноводе с волоконном, по которому распространяется квантовый ключ. Но само сопряжение волокна и волновода все еще представляет собой трудную техническую задачу. Необходимо добиться того, чтобы фотоны не терялись в месте соединения, где всегда происходит рассеяние, то есть потери.

- И все же, есть ли в этой области впечатляющие результаты, которые может оценить реальный потребитель?

- С этим как раз проблема. Прежде всего, потребитель должен убедиться, что ему нужна именно такая степень секретности. А может быть, достаточно той, что есть? Думаю, пока криптографические устройства не вышли на рынок в полной мере по маркетинговым причинам. С другой стороны, подобные системы необходимы для государственных нужд и не покупаются за рубежом... Пока мы не видели в России, что-

где один из наших сотрудников получил новую лабораторию. Вот они - главное наше богатство.

- Ваш грант рассчитан на три года. Что происходит сейчас и что должно получиться по истечении его срока?

- Система квантовой криптографии - это, как я уже говорил, система секретной передачи ключа. Ее принцип может обеспечить абсолютную секретность, но техническая реализация может иметь дефекты. Как проверить секретность, как убедиться, что ключ невозможно взломать? Практически это делается путем привлечения к работе профессионального хакера. В информационных системах безопасности происходит своеобразная борьба, развитие идет путем совершенствования систем защиты и взлома. Некоторое время назад мы решили изучить этот вопрос и выяснить, кто занимается взламыванием систем передачи квантового ключа, кто больше всего публикуется по этому поводу. Оказалось, что есть известный специалист с русским именем Вадим Макаров, который сейчас работает в Канаде и достиг в своем деле больших успехов. Мы его пригласили поработать с нами, взломать нашу систему.

- Не смог?

- Нет, смог, но мы поняли, какие методы он использует. Он воздействует на детектор мощным импульсом, детектор "слепнет", в этот момент он "втаскивает" туда свой ключ. Но выяснилось, что если слепнет наш детектор, то он ничего больше не принимает и не дает возможности что-либо передать, то есть "втаскивать" ему ничего не удастся. Скоро результаты этой работы будут опубликованы в нашей совместной статье. Если кратко - мы научились хакерские взломы эффективно отражать.

- Просто детектив какой-то! Григорий Наумович, всякий раз, когда разговариваю с вами, не покидает ощущение, что идей у вас столько, что могли бы обеспечить работой целый институт, не только лабораторию или кафедру. По-настоящему, что с таким потенциалом вы никогда не будете сидеть сложа руки, вне зависимости от того, выиграете вы деньги по гранту или нет. Так все же, какую роль в вашей работе играет факт финансирования от министерства?

- Наличие грантов для нас - вопрос жизни и смерти. То есть, куда вы приходите, - это научно-образовательный центр. Здесь делается наука, дается образование, создаются наукоемкие компании. Не будет финансирования - вся деятельность остановится. Взять хотя бы расходные материалы: мы работаем с низкими температурами, используем криогенные жидкости, прежде всего дороговую жидкий гелий. Для создания наноструктур снова требуются уникальные расходные материалы. Стоимость капли электронного резиста (специальный полимер, который используется для создания наноструктур) несопоставима даже со стоимостью золота! Но главное, грант позволяет привлекать к работе талантливых молодежь, дает ей шанс надолго закрепиться в российской науке.

Фото Николая СТЕПАНЕНКОВА



об интересных экспериментах и каких-то значимых результатах в области передачи данных или квантовой телепортации сообщений между находящимися на значительном расстоянии друг от друга условными "партнерами" Alice и Bob (например, на противоположных берегах Женевского озера), когда один правильно трактует "послания" другого. Но по большому счету о серьезных прорывах пока не слышно...

- Мы участвовали в подобных экспериментах вместе с группой ученых из Женевского университета. Тогда удалось протестировать наш однофотонный детектор и передать квантовый ключ на расстояние в 150 км, а в лабораторных условиях при использова-

нии оптоволокну этот результат был повторен на расстояние 250 км. Квантовая криптография - это передача квантового ключа, который зашифрован в квантовых состояниях фотонов и передается по волоконной линии. Дальность передачи зависит от характеристик детектора, который в идеале должен принимать каждый фотон. Но он пропускает, поэтому приходится сокращать расстояния... Мы же обнаружили, что гораздо проще получить 100-процентную квантовую эффективность не на оптоволокну, а на волноводе, чтобы каждый фотон считался, детектировался. Идея состоит в том, чтобы совместить детектор на волноводе с волоконном, по которому распространяется квантовый ключ. Но само сопряжение волокна и волновода все еще представляет собой трудную техническую задачу. Необходимо добиться того, чтобы фотоны не терялись в месте соединения, где всегда происходит рассеяние, то есть потери.

- Кто занят в работах над проектом?

- Студенты, аспиранты, магистры. Многие делают бакалаврские работы, пишут диссертации. Причем работают над проектом не только студенты МПГУ. Сюда приходят и ребята из МИЭМ НИУ ВШЭ, где мы открыли базовую кафедру от компании, и из Физтеха,