БУДУЩЕЕ КВАНТОВЫХ ВЫЧИСЛЕНИЙ: ОТ ОДНОАТОМНЫХ ТВЕРДОТЕЛЬНЫХ ЭЛЕМЕНТОВ ДО СТЕГАНОГРАФИЧЕСКИХ СИСТЕМ

FUTURE OF QUANTUM COMPUTING: FROM MONOATOMIC SOLID ELEMENTS TO STEGANOGRAPHIC SYSTEMS

DOI: 10.22184/1993-8578.2018.80.1.40.43

*Л.Раткин**
*L.Ratkin**

Осенью 2017 года суперкомпьютерный консорциум российских университетов, Федеральное агентство научных организаций (ФАНО) и Российский фонд фундаментальных исследований (РФФИ) провели в Москве международную конференцию Russian Supercomputing Days. В преддверии 30-летия Физико-технологического института РАН (ФТИАН) и 85-летия Физического факультета МГУ им. М.В.Ломоносова на суперкомпьютерном форуме был проведен семинар по квантовым вычислениям.

In the autumn of 2017, a supercomputer consortium of Russian universities, the Federal Agency for Scientific Organizations (FASO) and the Russian Foundation for Basic Research (RFBR) held an international conference Russian Supercomputing Days in Moscow. On the eve of the 30th anniversary of the Physical Technological Institute of the Russian Academy of Sciences (FTIAN) and the 85th anniversary of the Faculty of Physics of the Lomonosov Moscow State University at the supercomputer forum held a seminar on quantum computing.

Семинару предшествовало пленарное заседание международной конференции Russian Supercomputing Days с программным выступлением С.Кулика, доцента кафедры квантовой электроники Физического факультета МГУ им. М.В.Ломоносова, представившего доклад о современном состоянии и перспективах развития квантовой обработки информации.

На семинаре был представлен совместный доклад Ю.Богданова (ФТИАН, МИФИ, МИЭТ), Б.Бантыша, Н.Богданова (оба – ФТИАН и МИЭТ), А.Квасного (МИФИ) и директора ФТИАН, члена-корреспондента РАН В.Лукичёва о нечетких измерениях в задачах квантовой томографии. В частности, идеальный случай томографии квантовых состояний предполагает формирование аппаратной матрицы протокола квантовых состояний. Методом максимального правдоподобия можно получить уравнение правдоподобия, в котором потери точности описываются обобщенным распределением. С помощью квантовой томографии можно восстановить значения амплитуд квантового состояния: после проведения множественных замеров выявляются оптимальные схемы измерений.

Текущему состоянию и перспективам развития одноатомных твердотельных элементов и устройств было посвящено выступление В.Шорохова, научного сотрудника кафедры атомной физики, физики плазмы и микроэлектроники Физического факультета МГУ им. М.В.Ломоносова. Был рассмотрен одноэлектронный параметрон, клеточные зарядовые автоматы, компоненты твердотельного квантового компьютера на примесных атомах, логические элементы на неупорядоченной системе наночастиц. В частности, была представлена система золотых наночастиц, являющаяся

* ООО "АРГМ" / ARGM LLC.

С.Кулик
S.Kulik

Б.Бантыш
B.Bantysh

совокупностью одноэлектронных транзисторов, которые в зависимости от соседних частиц находятся в закрытом или открытом состояниях. На электроды подается изменяемый во времени сигнал, а с одного из электродов снимается выходной ток-сигнал. В докладе отмечалось, что при построении резервуарных нейронных сетей возникают особые требования к вычислениям. Например, пространство состояний резервуарной сети должно содержать множество неустойчивых точек (так называемых точек бифуркации), для перемешивания полученных в различные моменты времени сигналов резервуар должен обладать затухающей памятью, а входные сигналы должны трансформироваться нелинейным образом. Идеальной основой для конструирования резервуарной сети является одноэлектронная сеть на примесных атомах. В качестве примера была представлена резервуарная вычислительная сеть на примесных атомах с диаметром круга около 200 нм, шириной электродов 50 нм, расстоянием между электродами 15–25 нм, содержащая 500 неглубоких примесных атомов и 3000 глубоких примесных атомов. Правила отбора при туннелировании наряду с дискретным энергетическим спектром электронов обуславливают появление множества устойчивых состояний в многопараметрическом пространстве (много больше 10^{100}). Резервуарная нейронная сеть на примесных атомах может применяться одновременно как обработчик полезного сигнала (при соответствующей настройке) и как наносенсор электрического поля. Сенсорные функции позволяют измерять величину поля и его градиент с возможным пространственным разрешением до 10 нм.

Государственно-частное партнерство и научно-техническая кооперация производственного предприятия и ведущего российского вуза на примере разработки квантово-криптографического комплекса защиты информации для крупных дата-центров рассматривались в докладе В.Елисеева в соавторстве с А.Жиляевым и А.Климовым (все – "ИнфоТеКС") и А.Уривским (МГУ им. М.В.Ломоносова). Отмечено, что при передаче данных в открытую среду основными угрозами являются утечка и подмена, что может привести не только к несанкционированному доступу, взлому паролей и получению конфиденциальной информации, но также к техногенной катастрофе – например, в случае перехвата каналов

В.Шорохов
V.Shorokhov

С.Молотков
S.Molotkov

управления беспилотным летательным аппаратом и его направления на стратегически важный объект. Вследствие намеренных воздействий операторов или ошибок настройки возможно выведение из строя критически важных компонентов инфраструктуры управления предприятий, отраслей или регионов.

Разработанный квантово-криптографический комплекс для защиты данных применим для информационных хранилищ и репозиторных систем оборонно-промышленных предприятий и банковских структур. Комплекс может использоваться в корпоративных информационных системах (ИС) и дата-центрах, а также в дата-центрах федеральных и региональных органов законодательной и исполнительной власти. Развитием квантово-криптографических комплексов вследствие появления квантовых компьютеров являются стеганографические системы. В отличие от криптографических систем, шифрующих сообщения, стеганографические системы скрывают сам факт передачи сообщения, многократно усложняя задачу их поиска в различных потоках данных и значительно повышая устойчивость ко взлому и уровень защиты корпоративных информационных сетей и систем связи.

Научный сотрудник Лаборатории квантовой радиофизики Физического факультета МГУ им. М.В.Ломоносова М.Сайгин развил тему безопасности данных. Докладчик обратил внимание участников семинара на рост объемов публикаций по квантово-компьютерной тематике в России и за рубежом. Лидерами в публикационной активности по проблемам разработки квантовых компьютеров являются США: в ближайшие годы ожидается создание квантового компьютера с более чем 100 кубитами. Присутствие в научно-промышленном секторе квантовых вычислений преимущественно предприятий американского ВПК формирует социальный заказ на разработку нового поколения систем защиты данных. Традиционных криптографических комплексов для обеспечения информационной безопасности и противодействия взломам ИС с применением квантовых компьютеров уже недостаточно, поэтому разрабатываются стеганографические системы данных, позволяющие скрывать факт передачи, приема или обработки данных в специальных стеганографических контейнерах (стегоконтейнерах) и совмещенные крипто-стеганографические системы. Высокая степень устойчивости стегоконтейнеров к эвристическому стеганографическому анализу для выявления скрытых "информационных закладок" позволяет применять их в военном и гражданском промышленном производстве, в частности на предприятиях ОПК, для противодействия хакерским атакам с использованием ресурсов высокопроизводительных вычислительных систем и комплексов, в том числе суперкомпьютеров и квантовых компьютеров.

Доклад С.Молоткова (Институт физики твердого тела РАН, Академия криптографии РФ, Факультет вычислительной математики и кибернетики МГУ им. М.В.Ломоносова) в соавторстве с А.Климовым, К.Балыгиным и С.Куликом (Физический факультет МГУ им. М.В.Ломоносова, Лаборатория квантовых оптических технологий) затрагивал вопросы конструирования и принципов работы квантового генератора случайных чисел. Особое внимание было уделено физическим генераторам, в которых случайная последовательность формируется при регулярном измерении состояний физической системы через фиксированные промежутки времени. В отличие от эволюции системы, описываемой законами классической физики, фактор случайности зависит только от степени неопределенности начальных условий. Поскольку начальные условия могут быть восстановлены даже при сложном законе классической эволюции, после чего изменение системы становится предсказуемым, последовательности также являются псевдослучайными. Представляет интерес использование счетчика фотонов в качестве источника физической случайности (квантового генератора случайных чисел), который благодаря лавинным однофотонным детекторам, регулируемым от сильно ослабленного до квазиоднородного уровней, генерирует излучение с пуассоновским

В.Погосов
V.Pogosov

распределением числа фотонов. В этом случае дискретной случайной величиной может рассматриваться акт фотодетектирования, то есть отсчет в фиксированный временной интервал. К clock-генератору регистрирующей электроники привязаны моменты дискретизации сигнала, что позволяет выбирать разные способы группировки фотографических отсчетов (фотоотсчетов). В частности, функция распределения временных интервалов между последовательными фотоотсчетами имеет экспоненциальный характер.

В завершение семинара прозвучало выступление В.Погосова (ВНИИ автоматики им. Н.Л.Духова, МФТИ, Институт теоретической и прикладной электродинамики РАН) о проблемах коррекции ошибок и стабилизации квантовой запутанности в искусственных квантовых системах. В соавторстве с С.Ремизовым (ВНИИ автоматики им. Н.Л.Духова, Институт радиотехники и электроники им. В.А.Котельникова РАН), Д.Шапиро, А.Жуковым (оба – ВНИИ автоматики им. Н.Л.Духова, МИФИ) и Ю.Лозовиком (ВНИИ автоматики им. Н.Л.Духова, МФТИ, Институт спектроскопии РАН) он представил результаты научных исследований, которые могут использоваться при построении отечественных квантовых компьютеров.

В завершение отметим, что в программе "Цифровая экономика Российской Федерации", утвержденной распоряжением Правительства РФ от 28.07.2017 г. № 1632-р, квантовые технологии – наряду с технологиями обработки и хранения больших данных, нейротехнологиями и искусственным интеллектом, системами распределенного реестра, новыми индустриальными технологиями, промышленным Интернетом, компонентами робототехники и сенсорикой, беспроводной связью, а также технологиями виртуальной и дополненной реальности – определены как "основные сквозные цифровые технологии" (ОСЦТ). На четвертый квартал 2018 года намечено создание системы "мер, стимулирующих крупные компании, в том числе государственные компании и государственные корпорации, участвовать в работе центров компетенции, включая среди прочих меры финансового стимулирования и механизмы государственно-частного партнерства по таким направлениям, как квантовые вычисления, искусственный интеллект, робототехника и др.". В конце 2017 – начале 2018 года были утверждены планы мероприятий по направлениям "Нормативное регулирование", "Формирование исследовательских компетенций и технологических заделов", "Информационная инфраструктура" и "Информационная безопасность". По итогам заседания Правительственной комиссии по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, в частности, принято решение о разработке "дорожных карт" по направлениям программы.

ЗАКЛЮЧЕНИЕ

Реализация программы "Цифровая экономика Российской Федерации" позволит сформировать условия для развития цифровой инфраструктуры, создать благоприятный инвестиционный климат для выполнения отраслевых проектов и обеспечить государственную поддержку цифровых технологий.

В апреле 2018 года отмечается 85-летие Физического факультета МГУ им. М.В.Ломоносова. На Физическом факультете проводится широкий спектр фундаментальных и прикладных научных исследований с участием представителей академического сообщества. Разработки факультета применяются в ведущих российских и зарубежных вузах, научно-производственных и финансово-промышленных корпорациях. Среди выпускников – пять лауреатов Нобелевской премии и свыше 30 лауреатов Государственной премии. Весной 2018 года в МГУ запланировано проведение серии конференций, посвященных юбилею.

Также в текущем году отмечается 30-летие ФТИАН – одного из лидеров в сфере разработки отечественных квантовых компьютеров. К юбилею приурочено проведение ФТИАН международной конференции "Микро- и наноэлектроника" и симпозиума "Квантовая информатика" осенью 2018 года. ■