Ведущий: **Антон Первушин**

ЗА МЕСЯЦ ПРОЧИТАЛ:

Дэвид Хоун «Хроники тираннозавра. Биология и эволюция самого известного хищника в мире»
Тираннозавр — самый популярный динозавр, но о нём мало известно. Хоун представил в своей книге новые сведения о древнем хищнике. Образ, реконструированный учёными, совсем не похож на то, что мы привыкли видеть на картинках и в кино: так, тираннозавры были покрыты перьями!

МАШИНА ВРЕМЕНИ

Фантасты не сумели предсказать появление квантовой связи. Возможно, им просто не хватило воображения. Квантовые эффекты вообще выглядят настолько странно, что вызывают инстинктивное неприятие как на уровне разума, так и на уровне чувств. Тем не менее они существуют и могут быть использованы в различных технологиях.

Квантовая связь основывается на довольно известном принципе «квантовой запутанности», при котором два или несколько квантов (скажем, фотонов) оказываются взаимозависимыми. При этом связь между ними сохраняется, даже если они разнесены в пространстве на расстояние, на котором невозможны любые другие физические взаимодействия — например, с помощью электромагнитного или гравитационного поля. При этом измерение параметра одного кванта тут же приводит к мгновенному прекращению запутанного состояния другого кванта. Считается, что, используя эффект запутанности, можно преодолеть ограничения природы и организовать передачу информации со скоростью выше световой.

Если бы такая технология появилась, она, конечно, сильно повлияла бы на наш мир. Однако в действительности квантовая связь не может нарушать базовые законы физики, согласно которым информация не может распространяться со скоростью, превышающей скорость света. Как же в таком случае использовать эту связь?

Жуткое дальнодействие

Квантовая запутанность родилась, что называется, на кончике пера. В 1927 году ведущие европейские физики собрались на Пятом Сольвеевском конгрессе в Брюсселе, чтобы в очередной раз обсудить фундаментальные вопросы, которые возникают по мере дальнейшего проникновения науки в тайны макрокосма и микрокосма. В тот момент наиболее важной проблемой стала объективность наблюдаемого мира, ведь новая квантовая теория бросала прямой вызов её фундаментальным принципам. Она утверждала, что результат наблюдения квантового явления зависит от наблюдателя. Альберт Эйнштейн, сам недавно совершивший революцию в физике своей теорией относительности, отказывался это принять. Одним из сторонников квантовой теории был не менее авторитетный физик Нильс Бор. Обмен колкостями между ними стал легендарным. «Бог не играет в кости!» — заявил Эйнштейн. «Альберт, не указывай Богу, что ему делать», — ответствовал Бор.

В результате споров победили последователи Бора, что не только многое поменяло в физике, но и открыло перед ней принципиально новые возможности, в том числе дало способ обмануть ограничения, диктуемые законами природы. В то же время теоретические построения не могли быть использованы на практике, поэтому целые десятилетия учёные рассматривали их исключительно как игру для ума. Например, знаменитый Эрвин Шрёдингер, прославившийся мысленным экспериментом с живой/мёртвой кошкой в ящике, ввёл термин «запутанность» для иллюстрации взаимного влияния квантов, находящихся в непосредственном контакте, но не хотел признавать существование взаимодействия на больших расстояниях. Эйнштейн называл эффект квантовой запутанности «жутким дальнодействием» и всячески издевался над коллегами, описывавшими его в своих моделях.

Альберт Эйнштейн и Нильс Бор

Тем не менее уравнения, предложенные Шрёдингером, работали, его предсказания совпадали с результатами экспериментов, поэтому со временем теория, обосновывавшая квантовые эффекты,

Peter Potrowl | CC BY SA 3.0

Ален Аспе

получала всё больше сторонников. Новое поколение учёных оказалось готово признать, что наш мир устроен куда безумнее, чем предполагал даже Нильс Бор. Своеобразный прорыв в этой области совершил ирландский физик Джон Белл, который в 1964 году вывел неравенства, получившие впоследствии его имя. Они обеспечивали теоретическую основу для экспериментов с запутанными квантами. Однако реальные технические возможности для проверки его выкладок появились намного позже: только в 1981 году французский физик Ален Аспе провёл хитроумный опыт с двумя потоками поляризованных фотонов, который в явной форме доказывал, что «жуткое дальнодействие» действительно существует и точно согласуется с неравенствами Белла.

В 2010 году Ален Аспе и другие учёные, работавшие над практическим обоснованием квантовой запутанности, получили за свой вклад в науку премию Вольфа. С этого момента в прессе начали активно

муссироваться слухи, будто бы физики открыли «квантовую телепортацию» — способ передавать информацию быстрее скорости света. Журналисты сразу вспомнили, что многие из фантастов описывали телепортацию и другие виды мгновенного перемещения в пространстве как передачу информации обо всём множестве атомов и субатомных частиц перемещаемого объекта (или субъекта) с последующим его восстановлением в месте назначения. И сделали вывод, что передача квантовых состояний — первый шаг к открытию настоящей телепортации. Однако журналисты ошибались: таким способом нельзя передать сколько-нибудь осмысленную информацию. Зато можно создать нечто другое — универсальный шифр!

Главная проблема современной криптографии состоит в том, что она основана на математических расчётах. Алгоритмы шифрования могут быть сколь угодно сложными и запутанными, однако, располагая достаточными вычислительными мощностями, рано или поздно можно взломать любой код. Разумеется, потенциальных хакеров в данном случае интересует не личная переписка влюблённых юзеров и даже не страшные тайны «Зоны 51», а ключи к банковским операциям. Поэтому нет ничего удивительного в том, что к «жуткому дальнодействию» проявляют интерес именно финансовые структуры, которые видят в нём один из способов защититься от взломов.

Квантовая криптография основана на разрушении квантовой запутанности. Сначала в специальном устройстве генерируется пара фотонов, запутанных, например, через поляризацию. Затем один из них передаётся по оптоволоконному кабелю или лазерному лучу на другой конец канала связи. Там поляризацию фотона измеряют, что, согласно законам квантового мира, приводит к разрушению запутанности. В результате на дальнем конце канала связи становится известным значение поляризации, а на исходном — значение базиса поляризации. Если выразить эти значения через нули и единицы, мы получим сочетание цифр, которое заранее, то есть до измерения, определить не можем. При достаточно интенсивном потоке запутанных фотонов на обоих концах канала связи образуются последовательности случайных чисел, которые можно использовать как две части ключа к одному и тому же шифру.

Благодаря взаимосвязи спутанных квантов пользователи на разных концах сети всегда будут получать одну и ту же информацию о состоянии носителя. Если некие злоумышленники попытаются перехватить ключ (фактически — измерить квантовое состояние одного из носителей), то из-за принципа неопределённости Гейзенберга (невозможно измерить одно свойство квантовой частицы, не повлияв на другое) запутанность будет нарушена непредсказуемым образом. В результате взломщики получат лишь бессвязный набор цифр, а пользователи шифра в тот же момент заметят, что их «взломали».

Преимущества квантовой криптографии настолько очевидны, что банковские структуры заинтересовались ею сразу, как только появились первые прототипы передачи ключа через запутанность. Первый протокол квантового распределения ключа под названием BB84 был предложен в 1984 году, а первый опыт такого рода был проведён в 1997 году. С тех пор технология активно развивается, причём основным каналом для трансляции запутанных фотонов служат оптоволоконные сети. К сожалению, даже лучшие из них могут непредсказуемо изменить состояние фотона, тем самым нарушив связность генерации ключа, поэтому физики разрабатывают способы борьбы с «помехами», возникающими на материальном уровне. Сначала речь шла о двух-трёх километрах, сегодня нормой считается передача на две сотни километров. То есть внутри среднего мегаполиса вполне можно обмениваться криптографическими ключами, обеспечивая функционирование информационной сети, которая принципиально защищена от взлома.

Интересно, что в деле квантового шифрования наша страна занимает одну из ведущих позиций. Например, в 2016 году сотрудники Казанского квантового центра и Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики запустили первую в стране многоузловую квантовую сеть. Они добились скорости генерирования случайных последовательностей в 117 кбит/с на линии протяжённостью 2,5 километра. В нынешнем году Российский квантовый центр связал коммерческой линией связи, созданной на принципах квантовой криптографии, офисы «Газпромбанка», находящиеся на расстоянии 30 километров. Аналогичные работы ведутся в Московском государственном университете и в Фонде перспективных исследований. До конца 2017 года российские учёные обещают выпустить первую модель отечественного квантового распределителя криптоключа, рассчитанную на массового потребителя. Используя это устройство, можно проектировать информационную сеть любой сложности, будучи уверенным в её защищённости.

Впрочем, нашим физикам ещё есть куда расти. В июне китайские специалисты заявили об успешной передаче запутанных фотонов с помощью специальных лазеров и околоземного спутника «Мо-цзы» (QUESS, Quantum Science Satellite), запущенного 15 августа 2016 года. Расстояние передачи составило от 500 до 1400 километров. Таким образом было показано, что квантовую криптографию можно использовать вне оптоволоконных сетей и даже в космическом пространстве.

Что это даёт? Прежде всего — новую высокотехнологичную основу для организации обмена данными. Однако в перспективе можно надеяться, что сумма квантовых технологий даст и новое качество — например, в непосредственном управлении материей на уровне частиц, которые вполне можно назвать «кирпичиками» мироздания. Но ни учёным, ни фантастам пока не хватает воображения, чтобы представить, как будет выглядеть подобная управляемая Вселенная.

Varsha Y S | CC BY SA 4.0