17:04 03 Окт. 2016

Источник: https://nplus1.ru/news/2016/10/03/bit-commitment-24-hours

Физики передали бит с рекордно отложенным прочтением

Капсула времени в Монтроуз, Колорадо
Chuckcars / Flickr.com

Физики из Университета Женевы поставили эксперимент, в котором бит, переданный Алисой Бобу, стал «доступен для чтения» лишь спустя рекордные 24 часа. Как отмечают авторы, главная сложность эксперимента — сделать невозможной «подделку» бита Алисой или третьим лицом или преждевременное его прочтение Бобом. Подобная техника может использоваться для секретной связи между двумя не доверяющими друг другу сторонами или, например, при голосовании. Ученые сравнивают этот эксперимент с передачей конверта с именем обладателя Оскара. Теоретически такая же схема эксперимента позволяет увеличить время задержки между отправкой и прочтением до года.
Исследование опубликовано в журнале *Physical Review Letters*(препринт), кратко о нем сообщает *Physics*.

В основе техники для передачи бита с «отложенным прочтением» лежит существование двух агентов Алисы и двух агентов Боба, попарно находящихся в разных точках земного шара. Первый агент Боба отправляет расположенному неподалеку первому агенту Алисы случайное число. Агент Алисы суммирует его с другим заранее заготовленным секретным числом с помощью известного обоим метода, зависящего от передаваемого бита («ноль» или «единица»). Затем второй агент Алисы раскрывает второму агенту

Боба передаваемый бит и секретное число. Второй агент Боба сверяет информацию с первым агентом Боба и убеждается, что за время между передачей первого и второго сообщений Алиса не совершила подлог, поменяв значение передаваемого бита.

Задержка между моментом передачи и прочтением информации в такой схеме зависит от расстояния между первым и вторым агентом Алисы. К примеру, если первый агент Алисы передает информацию агенту Боба из Москвы, а второй — из Сиднея или Веллингтона, то безопасное время, за которое Алиса не успеет подменить бит, составит около 20 миллисекунд. Для увеличения задержки необходимо либо значительно увеличивать расстояние между парами агентов (например, поместив одну из пар на Плутоне, тогда безопасное время достигнет пары часов), либо потребовав для расшифровки использования нескольких циклов связи между агентами.

Последний подход был предложен в 1999 году. Чтобы быть уверенным в невозможности «подмены» со стороны Алисы, каждый новый цикл (а они происходят поочередно в каждой паре) должен начинаться до того, как агенты Алисы успеют связаться друг с другом. Чтобы у Боба не было возможности надежно угадать передаваемый бит до окончания всех циклов передачи, требуется большой объем информации — чем больше время задержки, тем экспоненциально больше длина сообщений.

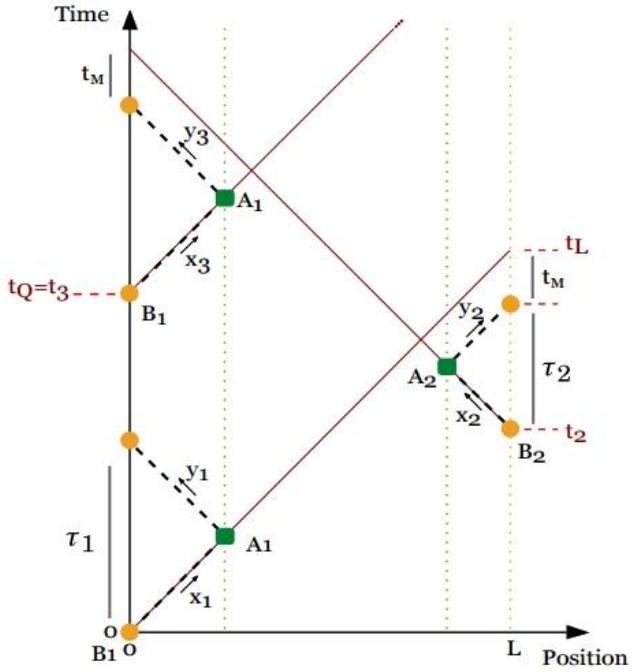

Схема эксперимента. Вертикальная ось — ось времени, горизонтальная — ось расстояний между агентами. В начале координат первый агент Боба (B1) передает агенту Алисы (A1) случайное сообщение (x1). Путь распространения сообщения имеет наклон, который ограничен скоростью света. Красные линии показывают пути сообщений, которыми могут пытаться обмениваться агенты Алисы для подмены бита. Как видно, они оказываются там, где физически расположены агенты Алисы, уже после того, как произошел очередной сеанс связи.
Ephanielle Verbanis et al / arXiv.org, 2016

В 2015 году схему реализовали на практике — шесть циклов обмена сообщениями при расстоянии между парами агентов в 131 километр привели к суммарной задержке в две миллисекунды. Для масштабов расстояний,

сопоставимых с размерами Земли, это соответствует задержке в 200 миллисекунд. Новая работа улучшает этот результат в полмиллиона раз — до 24 часов, сохраняя безопасность сообщений от преждевременной дешифровки Бобом.

В новом эксперименте расстояние между парами агентов составляло всего 7 километров — обе пары находились в пределах Женевы. У агентов Алисы есть заранее сгенерированный и пронумерованный массив 128-битных строк. В первом сеансе связи первый агент Боба передавал Алисе случайное 128-битное сообщение. Если Алиса изначально задумывала передать «ноль», то в ответ агент отправлял Бобу первую строчку из массива. Если же сообщением была «единица», то агент Алисы складывал (вернее, выполнял XOR) сообщение Боба с первой строкой. Второй сеанс связи начинался до того, как свет мог долететь от одного агента Алисы к другому, сообщая о результатах первого сеанса.

Во время второго сеанса второй агент Боба отправлял второе случайное сообщение второму агенту Алисы. Агент математически комбинировал это сообщение (выполнял умножение в поле Галуа) с первой строкой массива, а затем суммировал со второй. После этого третий сеанс связи происходил уже между первыми агентами и так далее.

Последний сеанс связи (всего в эксперименте их было пять миллиардов) завершался тем, что агент Алисы отдавал Бобу в явном виде последнюю строку массива. Боб использовал ее для того, чтобы вычислить предпоследнюю строку, предпредпоследнюю и так далее. Всего за 24 часа эксперимента было передано 162 гигабайта сообщений, а на полную их дешифровку с использованием обычного компьютера ушло около 72 часов.

По оценкам ученых, если увеличить расстояние между агентами до 10 тысяч километров, то с помощью такого же метода можно добиться годовых задержек между отправкой и прочтением. Важно, что с высокой надежностью используемая методика не позволит Бобу раскрыть сообщение раньше времени или позволить Алисе изменить решение и сменить передаваемый бит. Кроме того, полный процесс передачи бита управлялся с помощью двух компьютеров, каждый из которых обладал процессором уровня Core i3 и четырьмя гигабайтами оперативной памяти.

Ранее мы сообщали о других важных достижениях в безопасной передаче данных. Так, этим летом физики запустили первую в России линию межбанковского квантового шифрования. Также недавно американские физики впервые реализовали на практике абсолютно стойкую систему квантового шифрования.

Владимир Королёв