

Физики уместили 10 бит в одном фотоне

Источник: <https://nplus1.ru/news/2016/09/26/photonrecord-data-storage>

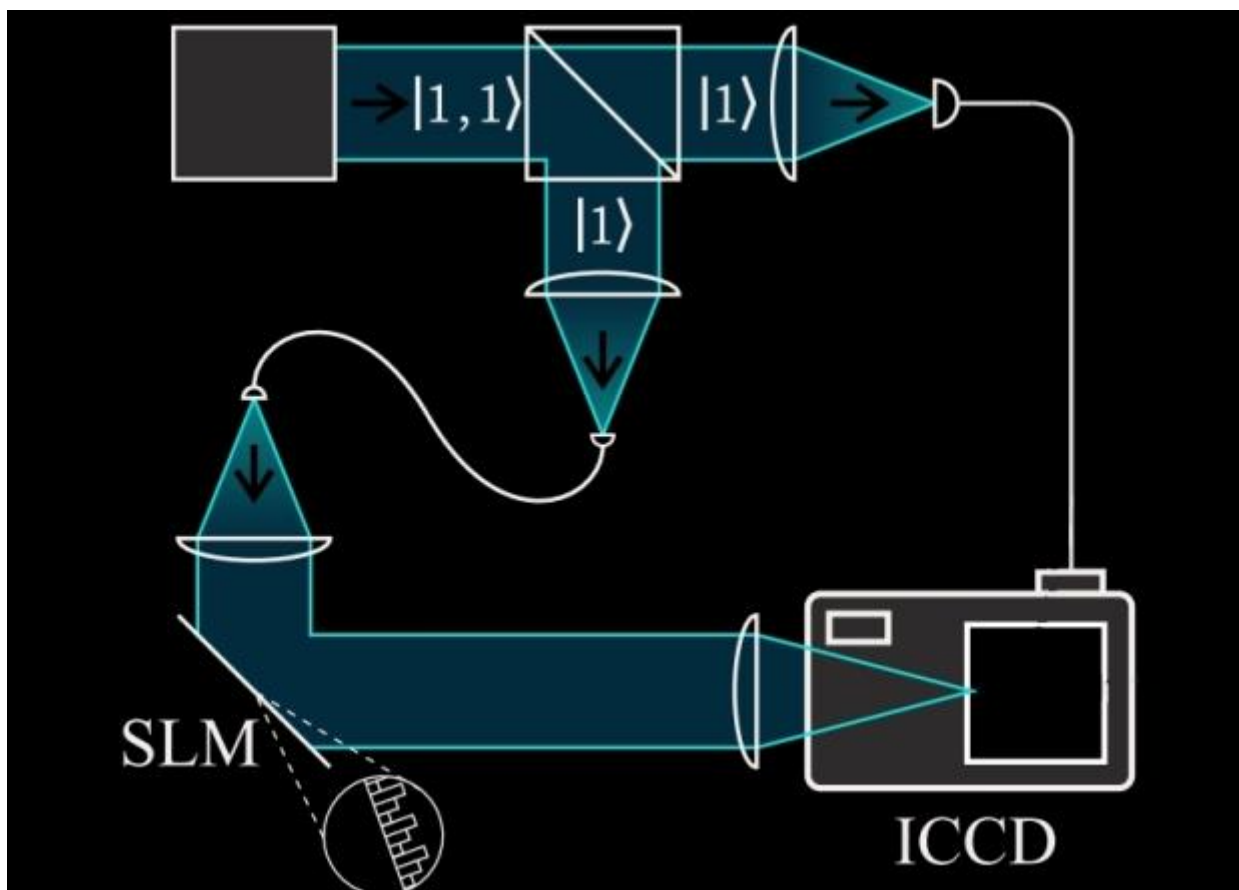


Схема эксперимента

T. B. H. Tentrup et al. / arXiv.org, 2016

Физики из нидерландского Университета Твента побили рекорд записи информации в одиночных фотонах, поместив в единичный квант света свыше 10 бит данных. Новый результат, по словам авторов, позволит значительно улучшить существующие методики квантовой криптографии — в современных устройствах фотон несет лишь один бит информации. Предыдущий рекорд для одиночных фотонов составлял семь бит. Эксперимент описан в [препринте](#) на arXiv.org, кратко о нем [сообщает](#) MIT Technology Review.

Традиционная методика квантовой криптографии — квантовое распределение ключа — основана на передаче фотонов, закодированных в одном из двух базисов. Например, фотоны могут быть поляризованы вертикально или горизонтально в первом базисе и по

одной из диагоналей во втором базисе. Базисы для подготовки и считывания каждого фотона выбираются каждый раз случайным образом, и лишь если они совпадут, информация считается переданной. Такой способ передачи данных в идеальной реализации защищен от атак злоумышленников — любое вмешательство в систему (измерение, например) необратимо изменит свойства фотона и будет обнаружено. Информация, переданная таким способом, будет в дальнейшем использоваться в роли ключа для шифрования данных, передаваемых в открытом канале.

В поляризации фотона можно записать лишь один бит информации — она несет либо «единицу», либо «ноль». Существуют техники, которые позволяют увеличить этот объем. Так, гораздо больше информации можно записать в форме волнового фронта фотона. Для этого используются пространственные модуляторы света (SLM). Эти устройства представляют собой сетки из ячеек, каждая из которых кодирует определенный символ. Если в сетке находится 8×8 ячеек, то она теоретически способна записать в фотон $\log_2(8 \times 8)$ — 6 бит информации. Считать этот фотон можно с помощью массива однофотонных детекторов 8×8 . На практике объем записываемой информации обычно меньше.

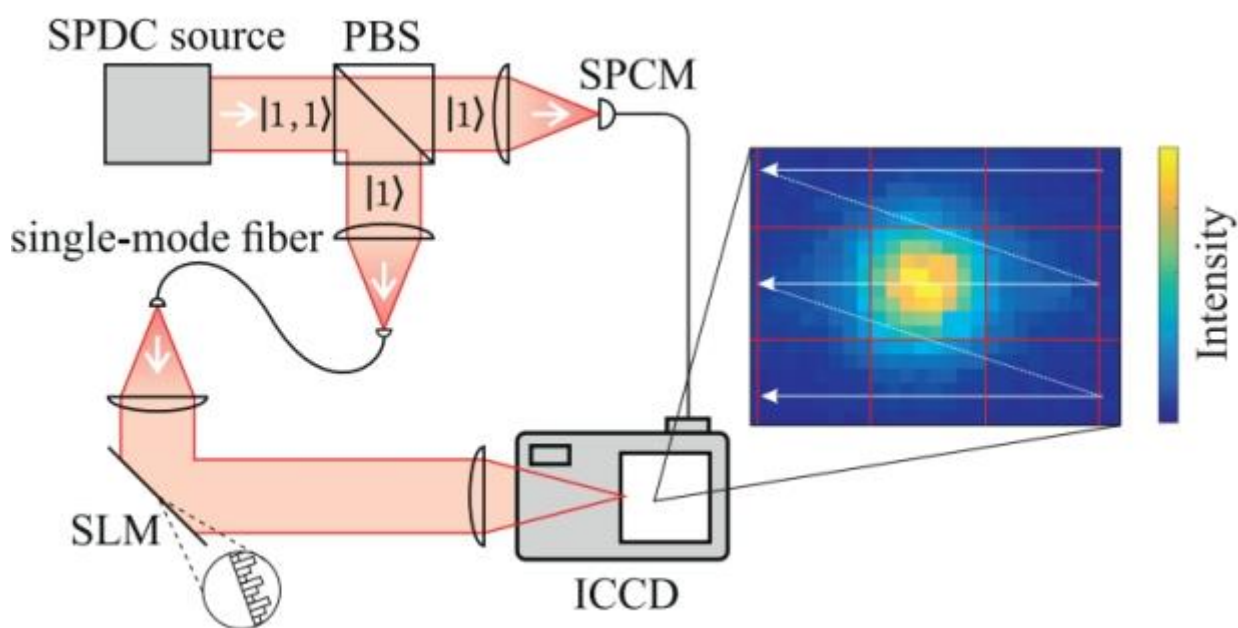


Схема эксперимента: SPDC — кристалл, в котором происходит спонтанное параметрическое рассеяние, SLM — пространственный модулятор света
T. B. H. Tentrup et al. / arXiv.org, 2016

В новой работе авторы использовали для подготовки фотона SLM, состоявший из 9072 ячеек (112×81). В идеальном случае ее было бы достаточно для того, чтобы закодировать в волновом фронте фотона более 13 бит информации. Подобная система очень чувствительна к

шумам от внешних фотонов, поэтому в эксперименте использовалась следующая система.

С помощью спонтанного параметрического рассеяния из фотона 395-нанометрового лазера физики получали запутанную пару фотонов с длиной волны 790 нанометров. Один из них играл роль «вестника», включавшего массив однофотонных детекторов. Второй фотон попадал на модулятор, перенаправлявший его на один из пикселей детектора. Благодаря фотону-«вестнику» исследователи избегали фиксации посторонних фотонов.

Даже несмотря на это, детектор все равно обладал ненулевым уровнем шумов, который приводил к потере информации. Для того чтобы сделать сигнал более выраженным, ученые понизили разрешение принимающего детектора, объединив несколько однофотонных детекторов в пиксель. В результате авторы добились кодирования 10,5 бит информации в одиночном фотоне.

Из-за неидеальности системы, с точки зрения практического использования емкость полученного канала передачи данных составляет лишь 0,1 бита в фотоне. Это связано с тем, что фотоны теряются в оптических узлах устройства. По словам физиков, эти потери можно устранить. Также авторы отмечают, что полученные результаты можно напрямую применять в современных системах для передачи данных.

Интересно, что именно благодаря использованию SLM американским ученым удалось впервые реализовать на практике систему абсолютно стойкого квантового шифрования. В ее основе лежал тот факт, что в одном фотоне можно записать шесть бит информации — 2,3 бита секретного ключа, 1 бит информации и 2,7 бита избыточной информации для того, чтобы понять, правильно ли расшифровано сообщение. Эта система позволяла передавать ключ для расшифровки сообщений одновременно с самими сообщениями, что невозможно в традиционных методах абсолютно стойкого шифрования.

Владимир Королёв