УДК 535.8

УСТАНОВКА КВАНТОВОЙ КРИПТОГРАФИИ С ИСТОЧНИКОМ ОДИНОЧНЫХ ФОТОНОВ, ОСНОВАННЫМ НА ЯВЛЕНИИ СПОНТАННОГО ПАРАМЕТРИЧЕСКОГО РАССЕЯНИЯ СВЕТА

В.И. Егоров, И.З. Латыпов, А.В. Рупасов, А.В. Глейм, С.А. Чивилихин

Предложены схема однофотонного источника, основанного на явлении спонтанного параметрического рассеяния света, для приложений квантовой информатики и схема установки квантовой криптографии, содержащая такой источник. Проводится сравнение характеристик этой системы с альтернативными, оперирующими критически ослабленным классическим излучением.

Ключевые слова: квантовая криптография, спонтанное параметрическое рассеяние, бифотоны, поднесущие частоты.

Введение

Технология квантовой криптографии, опирающаяся на квантовые свойства света, позволяет передавать по незащищенному каналу связи случайную последовательность бит таким образом, что вмешательство злоумышленника (именуемого Ева) в процесс передачи неизбежно порождает дополнительный шум в канале и обнаруживается легитимными пользователями (именуемыми Алиса и Боб) [1].

Одним из важных элементов любой системы квантовой рассылки ключа является источник однофотонного излучения. В современных работах различают два основных подхода к пониманию квантового сигнала: одиночные фотоны и когерентные состояния [2, 3]. Известно несколько механизмов генерации одиночных фотонов, в частности, с использованием квантовых точек [4] и спонтанного параметрического рассеяния (СПР) [5]. К сожалению, на сегодняшний день не существует широкого выбора коммерческих продуктов, основывающихся на этих принципах. Используемой в экспериментах [2] и коммерческих образцах [6] альтернативой являются короткие лазерные импульсы, ослабленные до критического уровня так, чтобы среднее число фотонов в них было меньше единицы. В квантовой криптографии в связи с этим часто употребляется выражение «одна десятая фотона», подразумевающее, что одиночный фотон присутствует в среднем лишь в одном из десяти временных отсчетов.

Системы, использующие ослабленное классическое излучение («когерентные состояния») значительно более просты и доступны, а также имеют ряд других преимуществ, но обладают уязвимостью к определенным типам атак Евы. Кроме того, однофотонные источники необходимы для других приложений квантовой информатики (например, квантовой телепортации), поэтому их создание является важной задачей.

Оценка уязвимости систем квантовой криптографии с классическим источником

Безусловная безопасность систем квантовой рассылки ключа основывается на предположении, что в каждом рабочем импульсе содержится не более одного фотона [3]. Если это не так, у злоумышленника появляется возможность провести эффективную атаку, называемую beamsplitting (разделение пучка). Суть ее состоит в том, что Ева может отвести по одному фотону из каждого импульса, не тронув остальные, и сохранить их до того момента, как Алиса и Боб начнут обсуждение по открытому каналу, а затем провести измерения в соответствии с полученной информацией. Подобная тактика не требует проведения измерения квантовых состояний непосредственно в процессе передачи, а потому никак не влияет ни на статистику получателя, ни на уровень шума в канале. В случае если Ева способна хранить фотоны в течение времени, затрачиваемого на генерацию ключа (для современных систем оно может не превышать нескольких секунд), эффективность этой атаки составляет 100% и не зависит от типа системы. Следует отметить, что, хотя число фотонов в пучке носит статистический характер, у Евы существует несколько возможностей для успешного определения импульсов, содержащих более одного фотона. Во-первых, теоретически перехватчик может обладать устройством, определяющим количество фотонов во временном интервале без их непосредственного измерения. Во-вторых, известно, что внутри каждого отсчета квантовые частицы идут с задержкой, а ворота счетчика в устройстве Боба, как правило, настроены таким образом, чтобы пропускать только первый фотон [2]. Этот подход значительно снижает уровень шума, но также позволяет Еве безнаказанно использовать запаздывающие компоненты импульса.

Для оценки эффективности атаки beamsplitting рассмотрим статистику излучения источника когерентных состояний [2]. Известно, что она описывается следующим выражением

$$P(n,\mu) = \frac{\mu^n}{n!} \cdot e^{-\mu} \quad ,$$

где n – число фотонов в импульсе; μ – среднее число фотонов в импульсе. Долю ключа, известную Еве, можно получить, отнеся количество импульсов с числом фотонов больше единицы к количеству непустых импульсов, из которых будет формироваться ключ

$$P(n>1 \mid n>0,\mu) = \frac{1-P(0,\mu)-P(1,\mu)}{1-P(0,\mu)}.$$

На рис. 1 приведены графики зависимости количества импульсов, содержащих более одного фотона (I), и доли ключа, известной Еве (II), от величины μ в диапазоне 0,1–1.

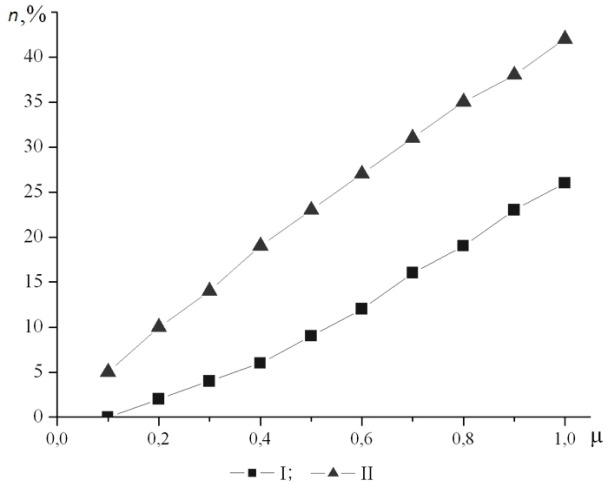

Рис. 1. Зависимость доли импульсов, содержащих более одного фотона (I) и доли ключа, известной Еве (II), от величины μ для источника когерентных состояний

Из графика видно, что хотя при значении μ порядка 0,1 число состояний с несколькими фотонами не превышает 1%, доля ключа, полученная Евой с применением атаки beamsplitting, составляет уже около 5%. Это связано с тем, что пустые отсчеты ($n = 0$), которых при низком значении μ большинство, не участвуют в процессе формирования ключа. Следует отметить, что разделение пучка может быть легко совмещено с другими типами атак, например, intercept-resend [2, 3]. В этом случае доли ключа, полученные Евой от атак разных типов, будут суммироваться. Хотя многие стратегии перехвата подразумевают повышение уровня шума в канале, Ева при определенных условиях может эффективно маскироваться под него, жертвуя информацией о ключе. Отметим также, что значение μ на практике ограничено снизу характеристиками приемника, так как отношение сигнал/шум линейно зависит от этого параметра [2].

Из этого следует, что использование источников когерентных состояний в реальных системах сопряжено с опасностью утечки секретных данных, которая может быть точно оценена в зависимости от характеристик применяемого пользователями оборудования.

Схема однофотонного источника для систем квантовой криптографии

Одним из возможных методов приготовления однофотонных состояний является СПР [5]. На основе СПР можно построить источник с вероятностным испусканием фотонов, обладающий высокой эффективностью, стабильностью и имеющий возможность перестройки в зависимости от задачи. Принципиальная схема источника, предлагаемого авторами, изображена на рис. 2.

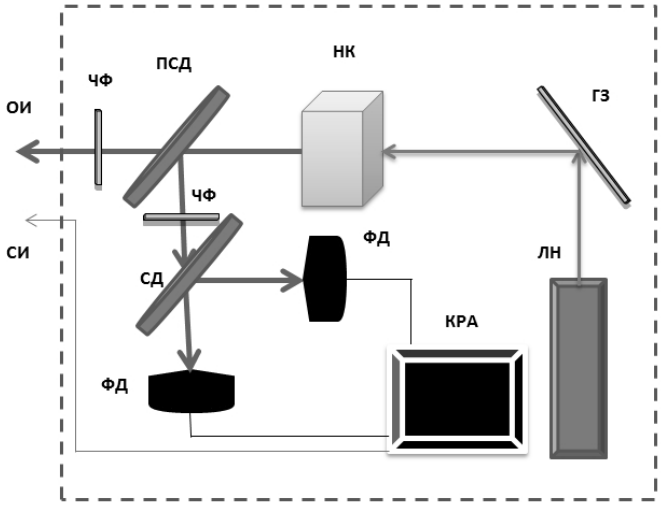

Рис. 2. Принципиальная схема однофотонного источника на основе СПР

Рассмотрим принцип работы такого источника. Излучение накачки генерируется непрерывным лазером (ЛН). Может быть использован как газовый лазер, так и диодный, с мощностью в диапазоне 10–100 мВт. Длина волны лазера определяет длины волн генерируемых фотонов. Фотон накачки, отра-

жаясь от глухого зеркала (ГЗ) с определенной вероятностью (10^{-7}–10^{-11}) рассеивается на нелинейном кристалле (НК), в результате чего рождается пара коррелированных фотонов (бифотон). Частоты пары фотонов могут быть одинаковыми (частотно-вырожденный режим СПР) и меняются при изменении ориентации нелинейного кристалла. Свойства нелинейного кристалла и ориентация его оптической оси относительно пучка накачки подбираются таким образом, что пара фотонов рождается с линейной и взаимно-ортогональной поляризацией (II тип синхронизма СПР). Далее бифотоны делятся по поляризации с помощью полупрозрачного светоделителя (ПСД). Один фотон (сигнальный) идет в оптический тракт (ОИ), а другой (холостой) проходит в боковой канал через частотный фильтр (ЧФ), используемый для отсечения излучения накачки и паразитных засветок, и светоделитель (СД). Затем холостой фотон регистрируется одним из лавинных фотодиодов (ФД), а сигнал о детектировании поступает на комплекс регистрирующей аппаратуры (КРА), включающий счетчики импульсов, электрическую линию задержки, схему совпадений, а также генератор синхроимпульсов (СИ). Наличие СД в холостом канале обусловлено необходимостью отсечения двухфотонных состояний света, представляющих наибольшую угрозу для безопасности квантового канала.

В процессе юстировки один из ФД ставится на выход ОИ, а схема совпадений соединяет прямой (сигнальный) и боковой каналы. При правильной настройке установки, когда выполняется условие ортогональности поляризации, регистрируется высокий уровень совпадений детектирования фотонов в двух каналах. После этого схема совпадений перемещается в холостой канал, а регистрация совпадения в нем будет означать присутствие двухфотонного состояния света, и такой импульс не будет использоваться. Когда в холостом канале фотон детектируется только на одном из приемников, в сигнальном канале также присутствует ровно один фотон. В этом случае КРА посылает синхроимпульс на затвор однофотонного источника либо на затвор детектора на принимающей стороне криптографической схемы.

Частота генерации бифотонов настолько мала, что излучение даже при непрерывной накачке невысокой мощности носит импульсный характер и может регистрироваться счетчиками одиночных фотонов без предварительного ослабления излучения. Это позволяет получить надежный инструмент для отсеивания паразитных многофотонных состояний света, что делает данную схему «истинным» однофотонным источником.

Принципиальная схема системы квантовой криптографии с СПР-источником

На рис. 3 приведена предлагаемая схема системы квантовой рассылки ключа с рассмотренным выше однофотонным источником. Схема во многом повторяет классическую систему Plug-and-play [5], однако имеет и важные отличия. В частности, из-за заложенной в источнике возможности отсеивания холостых импульсов синхроимпульс может быть выведен из волокна и пущен по отдельной (не обязательно оптической) линии связи, что значительно снизит уровень шума засветки в системе. Это отличие выражается в отсутствии дополнительного источника лазерного излучения у Алисы, СД и детектора классического излучения в блоке Боба. Синхронизация может быть выполнена при передаче сигнала от холостого детектора в СПР-источнике Алисы на модулятор Боба.

Следует отметить, что жесткая привязка синхронизационного сигнала к детектированию фотона в холостом канале имеет и негативный эффект: при использовании легитимными пользователями протокола двух состояний (например, B92 [2]) Ева будет обладать выигрышной стратегией, так как всегда будет знать, был ли в импульсе фотон. Однако при использовании протоколов с большим числом состояний (например, BB84 [2]) с учетом понижения уровня шума такой возможностью перехватчик обладать не будет. Этот вопрос нуждается в дополнительном теоретическом исследовании.

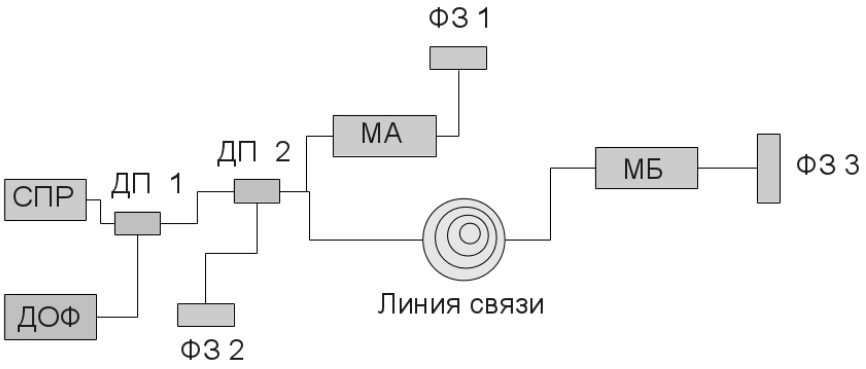

Рис. 3. Принципиальная схема Plug-and-Play системы квантовой криптографии с СПР-источником одиночных фотонов

Рассмотрим алгоритм работы этой схемы. Отправитель-Алиса запускает процесс генерации ключа, подавая на кристалл источника СПР излучение накачки. После рождения фотонной пары и детектирования «холостого» фотона импульс проходит через первый делитель (ДП 1) и разделяется на втором

(ДП 2) на компоненты P1 и P2. Первая компонента, P1, сразу идет по линии связи к получателю-Бобу, а вторая, P2, предварительно задерживается в специальном («задерживающем») отрезке волокна между фарадеевскими зеркалами ФЗ 1 и ФЗ 2. Система из трех фарадеевских зеркал (ФЗ 1, ФЗ 2 и ФЗ 3) позволяет сохранить поляризацию импульсов P1 и P2 в момент их интерференции [7]. После прохождения света по линии связи Боб без изменений отражает обратно P1 и вносит фазовый сдвиг в P2 на модуляторе Боба (МБ), чтобы закодировать бит. При обратном проходе Алиса, в свою очередь, задерживает P1 и модулирует его фазу на модуляторе Алисы (МА), после чего P1 и P2 интерферируют, одновременно оказываясь на выходе из делителя ДП 2. Результат интерференции P1 и P2 наблюдается с помощью счетчика одиночных фотонов ДОФ.

Преимущества и недостатки систем с однофотонным источником

Установка квантовой криптографии с СПР-источником обладает как преимуществами, так и недостатками по сравнению с другими современными типами систем квантовой рассылки ключа.

К недостаткам можно отнести высокую стоимость и сложность, низкую скорость работы (связанную с малой вероятностью генерации бифотонов) по сравнению с технологиями Plug-and-play [3] и квантовой рассылки криптографического ключа на поднесущей частоте модулированного света (КРКПЧ) [8], технические сложности с детектированием сигнального и холостого фотонов при определенных соотношениях их частот и частоты накачки. Для предложенной схемы установки актуальны проблемы, характерные для большинства Plug-and-play схем: увеличение потерь и снижение скорости за счет использования двунаправленной схемы распространения излучения, необходимость точного контроля фазы излучения. Кроме того, отсутствует возможность простой реализации мультиплексирования и интеграции в существующие линии оптической связи, присущая системам КРКПЧ [8].

Тем не менее, системы с СПР-источниками обладают фундаментально важными преимуществами: в них достигается значительно более высокая чистота состояний, требующаяся для достижения уровня секретности, описываемого в теории квантовой криптографии. Эти источники применимы для экспериментов в других областях квантовой информатики, демонстрируют низкий уровень шума и позволяют при необходимости легко отсекать пустые отсчеты.

Заключение

В работе продемонстрирована принципиальная возможность создания системы квантовой криптографии с бифотонным источником. Несмотря на то, что они позволяют достичь значительно более высокой чистоты квантовых состояний, целесообразность их применения должна оцениваться в зависимости от задачи. В частности, известные успешные эксперименты по взлому доступных на рынке систем квантовой криптографии базируются на уязвимостях аппаратуры принимающей стороны, а не атаке типа beamspliting [6].

Работа выполнена в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 годы, ГК №16.513.11.3070.

Работа выполнена при поддержке ГК №14.740.12.08.41 «Использование излучения ультракороткой длительности для биомедицины, промышленности и защищенных коммуникаций», выполняемого в рамках мероприятия «Проведение поисковых научно-исследовательских работ в целях развития общероссийской мобильности в области физики и астрономии».

Литература

1. Bennett C.H., Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing // Proceedings of IEEE International Conference on Computers Systems and Signal Processing. – 1984. – P. 175–179.
2. Gisin N., Ribordy G., Tittel W., Zbinden H. Quantum cryptography // Rev. Mod. Phys. – 2002. – V. 74. – № 1. – P. 145–190.
3. Scarani V., Bechmann-Pasquinucci H., Cerf N.J. et al. The security of practical quantum key distribution // Rev. Mod. Phys. – 2009. – V. 81. – P. 1301–1350.
4. Unitt D.C., Bennett A.J., Atkinson P. et.al. Quantum dots as single-photon sources for quantum information processing // Journal of optic. – 2005. – V. 7. – № 7. – P. 129–134.
5. Калачев А.А., Калашников Д.А., Калинкин А.А., Митрофанова Т.Г., Самарцев В.В., Шкаликов А.В. Бифотонная спектроскопия кристалла рубина // Учен. зап. Казан. гос. ун-та. Сер. физ.-матем. науки. – 2008. – Т. 150. – Кн. 2. – С. 125–130.
6. Feihu Xu, Bing Qi, Hoi-Kwong Lo. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system // New J. Phys. – 2010. – V. 12. – P. 113026.
7. Muller A., Herzog T., Huttner B., Tittel W., Zbinden H., Gisin N. «Plug and play» systems for quantum cryptography // Appl. Phys. Lett. – 1997. – V. 70. – P. 793–795.
8. Рупасов А.В., Глейм А.В., Егоров В.И., Мазуренко Ю.Т. Согласованная система квантовой рассылки криптографического ключа на поднесущей частоте модулированного света // Научно-технический вестник СПбГУ ИТМО. – 2011. – № 2 (72). – С. 95–99.

Егоров Владимир Ильич – Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, аспирант, egorovvl@gmail.com

Латыпов Ильнур Зиннурович – КФТИ КазНЦ РАН, мл. научный сотрудник, ilnur.latypov@gmail.com

Рупасов Андрей Игоревич – Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, аспирант, sadbender@yandex.ru

Глейм Артур Викторович – Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, студент, aglejm@yandex.ru

Чивилихин Сергей Анатольевич – Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, кандидат физ.-мат. наук, ст. научный сотрудник, доцент, sergey.chivilikhin@gmail.com