УЧЕНЫЕ ЗАПИСКИ КАЗАНСКОГО УНИВЕРСИТЕТА
*Том 155, кн. 1* Физико-математические науки *2013*

УДК 535.8

# СИСТЕМА КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА НА ПОДНЕСУЩИХ ЧАСТОТАХ МОДУЛИРОВАННОГО ИЗЛУЧЕНИЯ С КОМПЕНСАЦИЕЙ ИСКАЖЕНИЙ СИГНАЛА

*В.И. Егоров, А.В. Глейм, А.В. Рупасов*

**Аннотация**

Создана принципиальная схема системы распространения криптографического ключа на поднесущих частотах модулированного света, обеспечивающая безусловно безопасную передачу информации. Предложены механизмы компенсации поляризационной зависимости фазовых модуляторов и негативного влияния двулучепреломления в волокне.

**Ключевые слова:** квантовая криптография, безопасное распределение ключа, поднесущие частоты.

---

В современных линиях связи проблема защиты передаваемых данных является весьма актуальной. В работе [1] было показано, что коммуникационные методы, опирающиеся на квантовые свойства света (при использовании одиночных фотонов в технологии передачи), позволяют передавать по незащищенному каналу связи последовательность случайных символов таким образом, что вторжение злоумышленника в канал связи неизбежно обнаруживается легитимными пользователями (традиционно именуемыми Алиса и Боб). Тем самым квантовая механика позволяет реализовать надежное распределение абсолютно стойкого ключа [1]. Сам процесс передачи принято называть квантовым распределением ключа (КРК). В существующих системах КРК наиболее распространен метод кодирования состояний одиночных фотонов с помощью модуляции оптической фазы [2–4].

При практической реализации волоконно-оптических фазовых систем КРК возникают две проблемы: проблема синхронизации фазы оптического излучения и проблема двулучепреломления в оптических элементах системы. Первая связана с тем, что оптические фазы сигналов, вводимые Алисой и Бобом, должны быть согласованы с высокой точностью. Вторая заключается в том, что используемые электрооптические фазовые модуляторы чувствительны к поляризации излучения. Вместе с тем стандартное оптическое волокно обладает двулучепреломлением, которое носит случайный характер, в том числе зависит случайным образом от времени. В обоих случаях результатом становится искажение квантового сигнала, что недопустимо по нескольким причинам, в частности, потому что протоколы квантовой криптографии используют уровень сигнала и частоту ошибок в качестве критерия наличия перехвата. Одним из возможных решений обеих проблем является использование Plug-and-Play систем КРК [3], однако конструкционные особенности такой системы накладывают ограничение на скорость генерации криптографического ключа, что является существенным недостатком.

Разработанная система квантового распределения криптографического ключа на поднесущих частотах модулированного излучения (КРКПЧ) решает проблемы

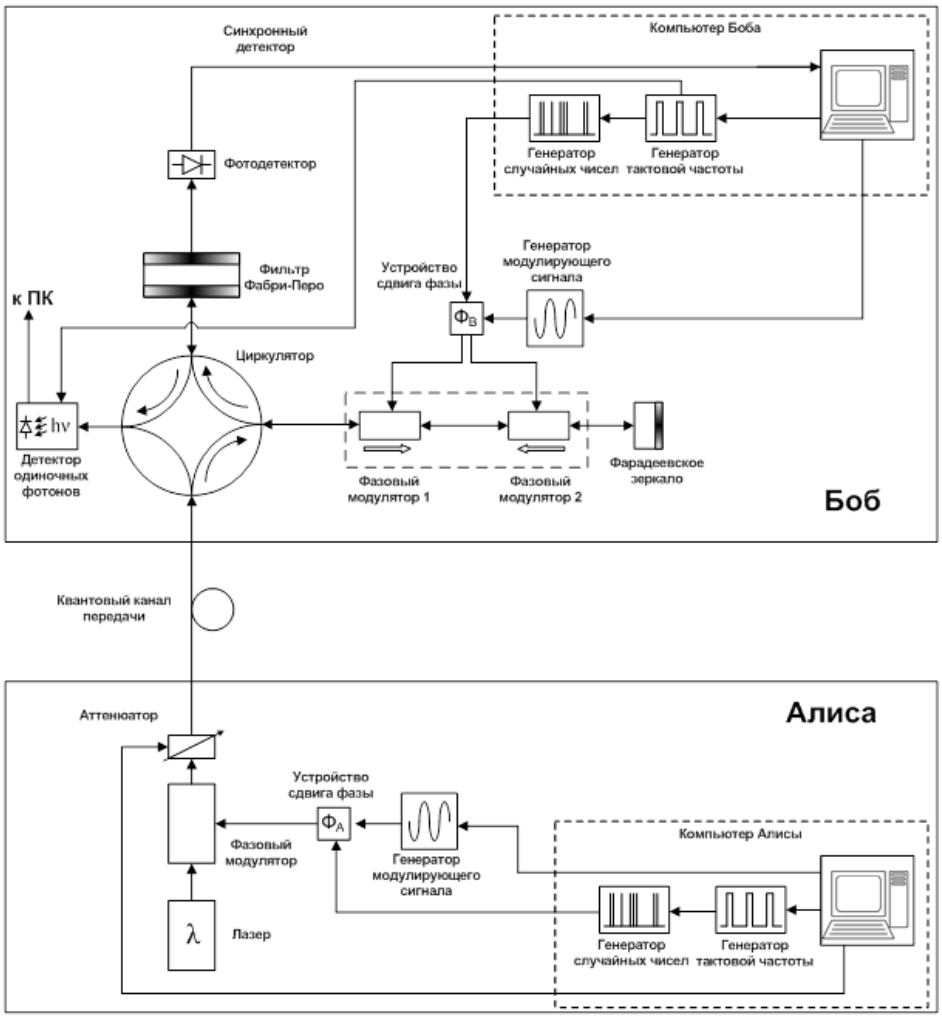


Рис. 1. Схема системы квантовой рассылки криптографического ключа на поднесущей частоте модулированного излучения

двулучепреломления и синхронизации фазы, предотвращая искажения сигнала, а также не имеет ограничений на скорость генерации криптографического ключа, присущих интерферометрическим Plug-and-Play системам [4–7]. На рис. 1 приведена схема установки, используемой в работе.

Лазер генерирует непрерывный сигнал на длине волны 1550 нм. Излучение подвергается фазовой модуляции. Генератор модулирующего сигнала 2.5 ГГц подключен к фазовому модулятору через устройство сдвига фазы. В результате фазовой модуляции в спектре сигнала появляются две боковые частоты, отстоящие от основной частоты оптического сигнала на величину частоты модулирующего радиочастотного сигнала. Генерация ключа осуществляется в соответствии с протоколом B92 [8]. Каждый бит кодируется путем внесения в модулирующий сигнал некоторого фазового сдвига $\Phi_A$. Фазовый сдвиг регулируется устройством сдвига фазы и принимает два возможных значения: 0 и $\pi$. К устройству сдвига фазы подключен генератор случайных чисел, на который подается управляющий сигнал от генератора тактовой частоты, управляемого компьютером.

Мощность сигнала на боковых частотах регулируется изменением амплитуды модулирующего сигнала. Далее модулированный сигнал ослабляется с помощью аттенюатора, управляемого компьютером. Величина затухания, вносимого аттенюатором, вычисляется из условия, что мощность сигнала на боковых частотах должна соответствовать уровню 0.2 фотона в одном тактовом интервале. Таким образом, излучение на поднесущих частотах является квантовым сигналом (используются так называемые «когерентные состояния»), а излучение на центральной частоте представляет собой опорный сигнал. Модулированный сигнал направляется в канал оптической связи.

На приемном устройстве (у Боба) сигнал следует к первому порту оптического циркулятора. Из первого порта циркулятора сигнал направляется во второй порт и поступает на фазовые модуляторы Боба и фарадеевское зеркало. Отразившись от фарадеевского зеркала, сигнал следует в обратном направлении. На этом этапе сигнал, пришедший от Алисы, подвергается повторной модуляции. Чтобы модуляция излучения не зависела от состояния его поляризации, эффективность модуляции не должна зависеть от направления распространения излучения. Для получения такой независимости модуляторы Боба устанавливают последовательно таким образом, что направления распространения бегущих электрических волн в этих модуляторах противоположны. После отражения от фарадеевского зеркала вертикальная и горизонтальная компоненты поляризации меняются местами, а излучение, отраженное от фарадеевского зеркала, проходит через модуляторы Боба в обратном направлении. Таким образом, все изменения состояния поляризации излучения на его пути от Алисы к Бобу при двойном прохождении излучения через модуляторы Боба компенсируются. Кроме того, благодаря встречному расположению модуляторов Боба при двойном проходе сигнала через них поляризационная чувствительность модуляции также компенсируется.

Боб на приемном устройстве использует свой генератор радиочастотного сигнала. Независимо от Алисы он также вносит фазовый сдвиг $\Phi_B$ в модулирующий сигнал, используя свое устройство фазового сдвига. К устройству фазового сдвига подключен генератор случайных чисел, который управляется сигналом от генератора тактовой частоты.

Мощность излучения на поднесущих частотах зависит от значений фазового сдвига, внесенных Алисой ($\Phi_A$) и Бобом ($\Phi_B$). В случае, когда модулирующие радиочастотные сигналы Алисы и Боба синфазны, то есть разность фаз двух модулирующих радиочастотных сигналов равна нулю ($\Phi_A - \Phi_B = 0$), на поднесущих частотах наблюдается конструктивная интерференция, и мощность оптического сигнала отлична от нуля. В случае, когда модулирующие радиочастотные сигналы Алисы и Боба находятся в противофазе, то есть разность фаз модулирующих сигналов равна $\pi$ ($\Phi_A - \Phi_B = \pi$), наблюдается деструктивная интерференция, и мощность сигнала на поднесущих частотах равняется нулю.

Далее сигнал вновь попадает на циркулятор и из второго порта направляется в третий, на выходе которого установлен спектральный фильтр Фабри–Перо. Излучение на основной частоте и поднесущих частотах детектируется отдельно. Сигнал на основной частоте проходит сквозь фильтр Фабри–Перо и попадает на фотодетектор. Сигнал на поднесущих частотах отражается от фильтра Фабри–Перо и следует обратно в циркулятор, где направляется из третьего в четвертый порт и затем регистрируется детектором одиночных фотонов. Синхронизация «ворот» детектора одиночных фотонов с тактовой частотой квантового сигнала осуществляется управляющим сигналом от генератора тактовой частоты.

Анализируя результаты измерений, Алиса и Боб получают «сырой» ключ. После расчета коэффициента ошибок в «сыром» ключе Алиса и Боб делают

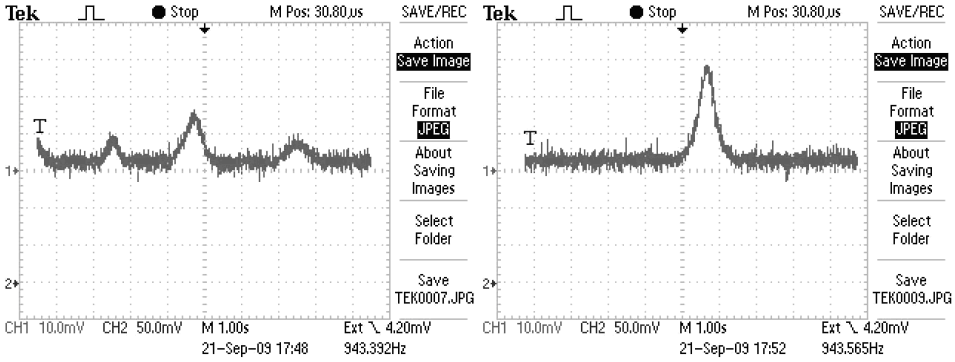


Рис. 2. Спектр оптического сигнала при конструктивной (слева) и деструктивной (справа) интерференции боковых частот

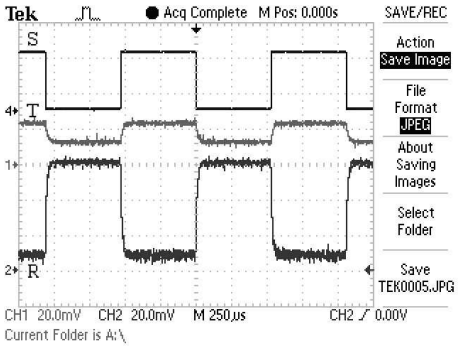


Рис. 3. Осциллограмма сигналов, передаваемых на центральной частоте ($T$) и боковых частотах ($R$) при периодическом и скачкообразном изменениях разности фаз модулирующих сигналов (кривая $S$) на величину $\pi$

вывод о присутствии подслушивающего злоумышленника. В случае отсутствия злоумышленника проводится коррекция ошибок, в результате которой Алиса и Боб получают секретный криптографический ключ.

Явления конструктивной и деструктивной интерференции были прежде всего продемонстрированы в экспериментах со сканированием частоты лазера при одновременной записи на осциллографе спектров излучения, прошедших через спектральный фильтр. Соответствующие осциллограммы приведены на рис. 2.

На лабораторном макете системы КРКПЧ была проведена имитация процесса генерации криптографического ключа. Частота излучения лазера настраивалась точно на центр полосы пропускания спектрального фильтра. С помощью электроники управления модуляторами разность фаз модулирующих сигналов Алисы и Боба переключалась между значениями 0 и $\pi$ с частотой 1 кГц. Полученные осциллограммы представлены на рис. 3. Зависимость разности фаз $\Phi_A - \Phi_B$ от времени имела вид меандра (кривая $S$). При этом зависимость мощности сигнала на боковых частотах также имела вид меандра с той же частотой (кривая $R$).

Характерные зависимости от времени оптических сигналов $T$ и $R$, формирующиеся в результате интерференции боковых частот Алисы и Боба при периодическом изменения разности $\Phi_A - \Phi_B$, могут быть названы интерференционными картинами. Вертикальный масштаб кривых $T$ и $R$ различен. Основной интерес представляют зависимости от времени интенсивности боковых частот (кривая $R$), имитирующие генерацию криптографического ключа. При переключении разност-

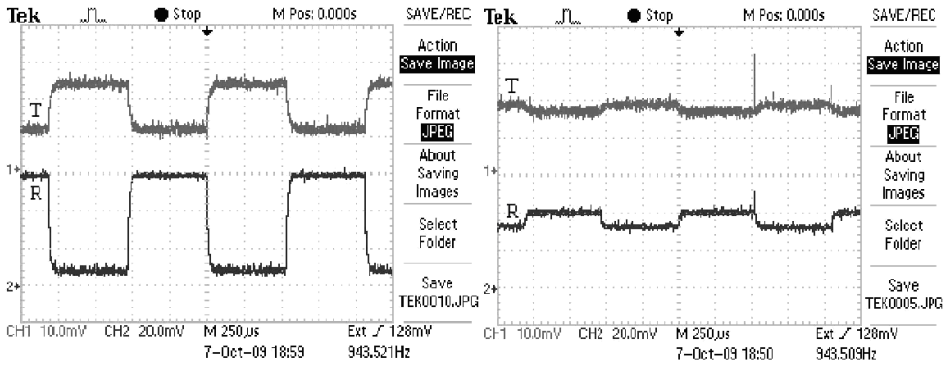


Рис. 4. Сравнение интерференционных картин при осцилляции разности фаз поднесущих частот в схеме с зеркалом Фарадея (слева) и с обычным зеркалом (справа). Исходное состояние

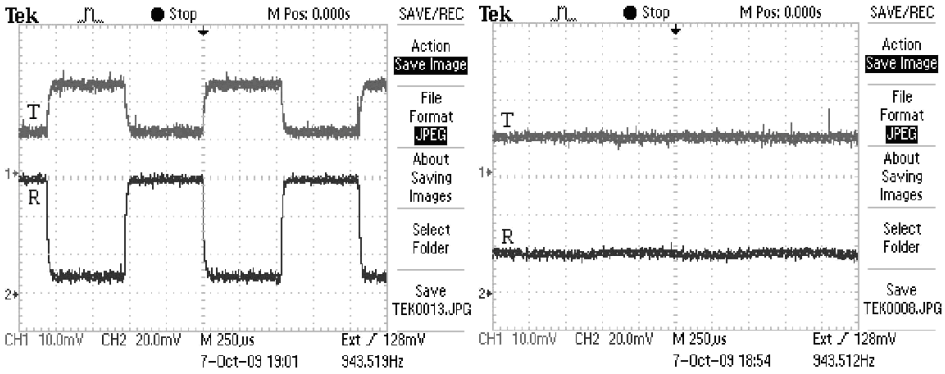


Рис. 5. Сравнение интерференционных картин при осцилляции разности фаз поднесущих частот в схеме с зеркалом Фарадея (слева) и с обычным зеркалом (справа). После преобразования поляризации

ной фазы от 0 до $\pi$ интенсивность излучения боковых частот изменяется от нуля до максимального значения.

В ходе эксперимента при интерференции боковых частот контраст интерференционной картины достигал значения $K = 10$, что соответствует видности $V = 82\%$. Результаты опытов свидетельствуют о корректной работе системы квантового распределения криптографического ключа в режиме высокоинтенсивного излучения. Понижение мощности сигнала на основной частоте, повышение качества зеркал спектрального фильтра Фабри–Перо, а также использование антиотражающих покрытий для линз коллиматоров и поверхности фотодиода позволят значительно уменьшить коэффициент шумов в сигнале на боковых частотах и осуществить функционирование системы КРКПЧ в режиме одиночных фотонов.

Компенсация поляризационной зависимости электрооптических модуляторов подтверждается следующим опытом. В оптическом волокне на участке между Алисой и Бобом состояние поляризации передаваемого сигнала произвольно изменялось. Для этого применялся волоконный контроллер поляризации. В исходном случае подобные манипуляции не должны вызывать какие-либо изменения интерференционной картины. Если же в схеме лабораторного образца фарадеевское зеркало заменить обычным зеркалом, то интерференционная картина должна заметно исказиться. На рис. 4, 5 приведены результаты этого опыта.

Очевидно, что интерференционная картина в случае с обычным зеркалом сильно искажается по сравнению с зеркалом Фарадея. Эксперимент подтвердил, что в случае с зеркалом Фарадея интерференционная картина остается стабильной и никакие внешние воздействия, влияющие на состояние поляризации распространяющегося сигнала, не повлияют на конечный результат интерференции.

Таким образом, в предлагаемой схеме происходит автоматическая динамическая компенсация двулучепреломления волоконно-оптической линии связи и компенсация поляризационной зависимости электрооптических модуляторов, что было подтверждено экспериментально. Это делает данный класс систем более предпочтительным для практического применения в волоконно-оптических линиях связи.

**Summary**

*V.I. Egorov, A.V. Gleim, A.V. Rupasov.* A System of Quantum Key Distribution on the Subcarrier Frequencies of a Modulated Emission with Signal Distortion Compensation.

We have created a schematic diagram for the system of cryptographic key distribution on the subcarrier frequencies of modulated light, which provides absolutely safe transmission of information. We have developed mechanisms of compensation for the polarization dependence of the phase modulators and for the negative impact of birefringence in the fiber.

**Keywords:** quantum cryptography, safe key distribution, subcarrier frequencies.

**Литература**

1. *Bennett C.H., Brassard G.* Quantum cryptography: public key distribution and coin tossing // Proc. IEEE Int. Conf. on Computers Systems and Signal Processing. – 1984. – P. 175–179.
2. *Scarani V., Bechmann-Pasquinucci H., Cerf N.J., Dusek M., Lutkenhaus N., Peev M.* The security of practical quantum key distribution // Rev. Mod. Phys. – 2009. – V. 81, No 3. – P. 1301–1350.
3. *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, No 7. – P. 793–795.
4. *Мазуренко Ю.Т., Мероллa Ж.-М., Годжебюр Ж.-П.* Квантовая передача информации с помощью поднесущей частоты. Применение к квантовой криптографии // Оптика и спектроскопия. – 1999. – Т. 86, № 2. – С. 181–183.
5. *Merolla J.-M., Mazurenko Y., Goedgebuer J.-P., Porte H., Rhodes W.T.* Phase-modulation transmission system for quantum cryptography // Opt. Lett. – 1999. – V. 24, No 2. – P. 104–106.
6. *Merolla J.-M., Mazurenko Y., Goedgebuer J.-P., Rhodes W.T.* Single-photon interference in sidebands of phase-modulated light for quantum cryptography // Phys. Rev. Lett. – 1999. – V. 82, No 8. – P. 1656–1659.
7. *Duraffourg L., Merolla J.-M., Goedgebuer J.-P., Mazurenko Y., Rhodes W.T.* Compact transmission system using single-sideband modulation of light for quantum cryptography // Opt. Lett. – 2001. – V. 26, No 18. – P. 1427–1429.
8. *Bennett C.H., Bessette F., Brassard G., Salvail L., Smolin J.* Experimental quantum cryptography // J. Cryptology. – 1992. – V. 5, No 1. – P. 3–28.

Поступила в редакцию
04.04.11

**Егоров Владимир Ильич** – студент, Санкт-Петербургский государственный университет информационных технологий, механики и оптики, г. Санкт-Петербург, Россия.
E-mail: *egorovvl@gmail.com*

**Глейм Артур Викторович** – студент, Санкт-Петербургский государственный университет информационных технологий, механики и оптики, г. Санкт-Петербург, Россия.
E-mail: *aglejm@yandex.ru*

**Рупасов Андрей Викторович** – студент, Санкт-Петербургский государственный университет информационных технологий, механики и оптики, г. Санкт-Петербург, Россия.
E-mail: *sadbender@yandex.ru*