3 ФОТОНИКА И ОПТОИНФОРМАТИКА

УДК 535.8

СОГЛАСОВАННАЯ СИСТЕМА КВАНТОВОЙ РАССЫЛКИ КРИПТОГРАФИЧЕСКОГО КЛЮЧА НА ПОДНЕСУЩЕЙ ЧАСТОТЕ МОДУЛИРОВАННОГО СВЕТА

А.В. Рупасов, А.В. Глейм, В.И. Егоров, Ю.Т. Мазуренко

Создана принципиальная схема согласованной (plug-and-play) системы распространения криптографического ключа на поднесущей частоте модулированного света, обеспечивающая, безусловно, безопасную передачу информации. Предложены механизмы компенсации поляризационной зависимости фазовых модуляторов и негативного влияния двулучепреломления в волокне, приведены экспериментальные результаты.

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

Введение

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 надежную передачу абсолютно стойкого ключа. Этот процесс передачи принято называть квантовой рассылкой ключа (КРК) [2]. В существующих системах КРК наиболее распространен метод кодирования состояний одиночных фотонов с помощью модуляции оптической фазы [2, 3].

Технология квантовой рассылки ключа на поднесущей частоте модулированного света (КРКПЧ) была предложена в работе [4] и развита в работах [5–9]. Использование поднесущих частот позволяет облегчить введение оптической фазы в рабочие сигналы [4]. Однако в системах КРКПЧ возникают те же проблемы, что и при разработке других устройств КРК, использующих модуляцию фазы. Можно выделить следующие проблемы устройств КРК с фазовой модуляцией: проблема синхронизации фазы и проблема двулучепреломления в системах волоконной связи. Первая из них связана с тем, что оптические фазы сигналов, вводимые Алисой и Бобом, должны быть согласованы с высокой точностью; одно из возможных решений приводится в [9]. Вторая проблема заключается в том, что электрооптические фазовые модуляторы, в частности, используемые в волоконных линиях связи, в большом числе случаев чувствительны к поляризации излучения. Вместе с тем стандартное оптическое волокно обладает двулучепреломлением, которое носит случайный характер, в том числе зависит случайным образом от времени. С учетом этого обстоятельства простейшая схема КРКПЧ [4] в реальности может обладать существенными недостатками, как и другие схемы КРК с фазовой модуляцией, и не являться, таким образом, согласованной (plug-and-play) [10]. Действительно, Алиса может однозначно ввести фазу в сигнал, непосредственно излучаемый ее лазером. Однако при передаче этого сигнала по длинному волокну к Бобу состояние поляризации этого сигнала может непредсказуемо измениться. Поскольку модулятор Боба также чувствителен к состоянию поляризации падающего излучения, результат модуляции сигнала Бобом может случайным образом зависеть от времени. Предлагаемое техническое решение данной проблемы описывается ниже.

Система компенсации двулучепреломления волокна и поляризационной чувствительности модуляторов в установках квантовой рассылки ключа

Рис. 1 иллюстрирует используемый в системах КРК принцип компенсации двулучепреломления волокна и поляризационной чувствительности модулятора [10]. Излучение лазера Л после его модуляции с помощью модулятора Алисы МА проходит сквозь 3-портовый циркулятор и направляется на модулятор Боба МБ. В предлагаемой схеме модулированное Бобом излучение направляется не на детектор фотонов, а на фарадеевское зеркало ФЗ. После отражения от фарадеевского зеркала вертикальная и горизонтальная компоненты поляризации меняются местами. Все изменения состояния поляризации при прохождении излучения через модулятор МБ компенсируются. Кроме того, при двойном проходе через модулятор МБ поляризационная чувствительность модуляции также компенсируется. Иными словами, модулятор МБ становится поляризационно-независимым. Излучение, выходящее из модулятора МБ и попадающее вновь в 3-портовый циркулятор, направляется циркулятором в другой канал, ведущий к детектору фотонов ДФ.

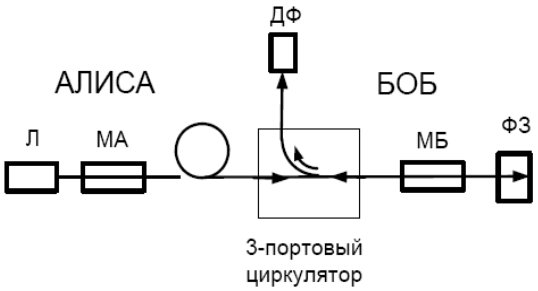


Рис. 1. Схема компенсации двулучепреломления в установках КРК

Схема (рис. 1) обладает следующим недостатком. При довольно высоких частотах модуляции (порядка ГГц), необходимых для реализации КРКПЧ, электрическое поле, накладываемое на электрооптический кристалл, формируется в виде бегущей волны. В этом случае распространение световой и электрической волн в кристалле модулятора может быть сделано синхронным, что приводит к существенному увеличению эффективности модуляции. Это означает, что электрооптические характеристики модулятора МБ в общем случае зависят от направления распространения света – слева направо или справа налево. Действительно, в одном случае распространение электрической и световой волны однонаправлено, а в другом случае – противоположно. Чтобы компенсировать такого рода невзаимность электрооптического модулятора, предлагается использовать вместо одного модулятора МБ на рис. 1 два идентичных модулятора, устанавливаемых последовательно таким образом, что направления распространения бегущих электрических волн в этих модуляторах противоположны. Полученная схема иллюстрируется рис. 2, на котором одинаковые модуляторы МБ1 и МБ2 установлены таким образом, что их бегущие электрические волны распространяются в противоположных направлениях (полые стрелки на рис. 2 указывают на направление распространения электрической волны).

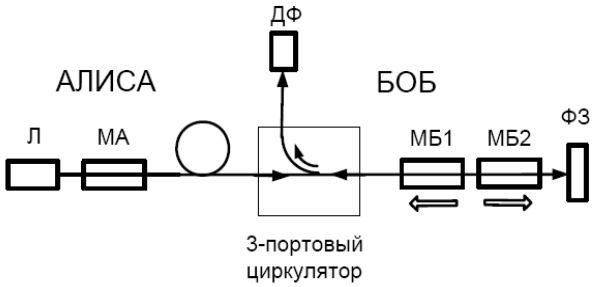


Рис. 2. Схема компенсации характеристик модулятора от направления распространения света в установках КРКПЧ

Схема согласованной установки квантовой рассылки криптографического ключа на поднесущей частоте модулированного света

Была разработана принципиальная схема самосогласованного устройства КРКПЧ с учетом описанных выше модификаций приемного узла. Эта схема изображена на рис. 3. Устройство КРКПЧ содержит терминалы Алисы и Боба, соединенные волоконно-оптической линией связи. Терминал Алисы содержит источник монохроматического излучения – лазерный диод ЛД и электрооптический модулятор Алисы МА. В результате периодической фазовой модуляции монохроматического излучения лазерного диода дополнительно к основной частоте формируются две боковые частоты, оптические фазы которых совпадают с фазой электрического сигнала, управляющего модулятором. Алиса вводит в боковые частоты оптическую фазу, в точности равную фазе модулирующего радиочастотного (РЧ) сигнала. Сигнал, сформированный Алисой, передается по волоконно-оптической линии связи в терминал Боба. В терминале Боба этот сигнал направляется прежде всего в 4-портовый волоконно-оптический циркулятор, который его направляет в группу двух модуляторов Боба МБ1 и МБ2. Необходимость применения двух одинаковых модуляторов с противоположным направлением электрической волны была объяснена выше. Излучение, прошедшее модуляторы МБ1 и МБ2, падает на фарадеевское зеркало ФЗ, отражается от него и вновь проходит через ту же пару модуляторов. При этом динамически компенсируется двулучепреломление оптического волокна, соединяющего терминалы Алисы и Боба, а также поляризационная зависимость модуляторов МБ1 и МБ2. Таким образом, предлагаемый комплекс двух зеркально расположенных модуляторов совместно с фарадеевским зеркалом фактически является модулятором, нечувствительным к поляризации излучения. Пользуясь одновременно модуляторами МБ1 и МБ2, Боб вводит в боковые частоты собственный сигнал, характеризуемый фазой Боба. Сигнал, содержащий фазы Алисы и Боба, направляется циркулятором в узел спектральной маршрутизации центральной частоты и боковых

частот передаваемого излучения. Этот узел состоит из двух волоконно-оптических коллиматоров и интерферометра Фабри–Перо. Коллиматоры необходимы для формирования широкого светового пучка на пластинах интерферометра. Следует отметить, что вместо традиционного интерферометра Фабри–Перо, состоящего из плоских зеркал, может быть использован конфокальный интерферометр. Конфокальный интерферометр может быть просто интегрирован в волоконно-оптическую систему. Центральная частота оптического излучения настраивается на резонанс пропускания интерферометра Фабри–Перо и поэтому распространяется в направлении фотодиода ФД. Фотодиод ФД обеспечивает детектирование центральной частоты, содержащей классический сигнал. Боковые частоты отражаются с хорошей эффективностью от интерферометра Фабри–Перо и вводятся в циркулятор, который их направляет на детектор одиночных фотонов ДФ. Для работы описываемого устройства необходима также синхронизация фазы РЧ сигналов, управляющих соответствующими модуляторами на терминалах Алисы и Боба. Синхронизация может быть реализована при передаче оптического синхронизирующего сигнала (в виде сигнала биений двух оптических частот) в том же волокне, но на частоте DWDM, соседней с частотой передачи квантовой информации [9].

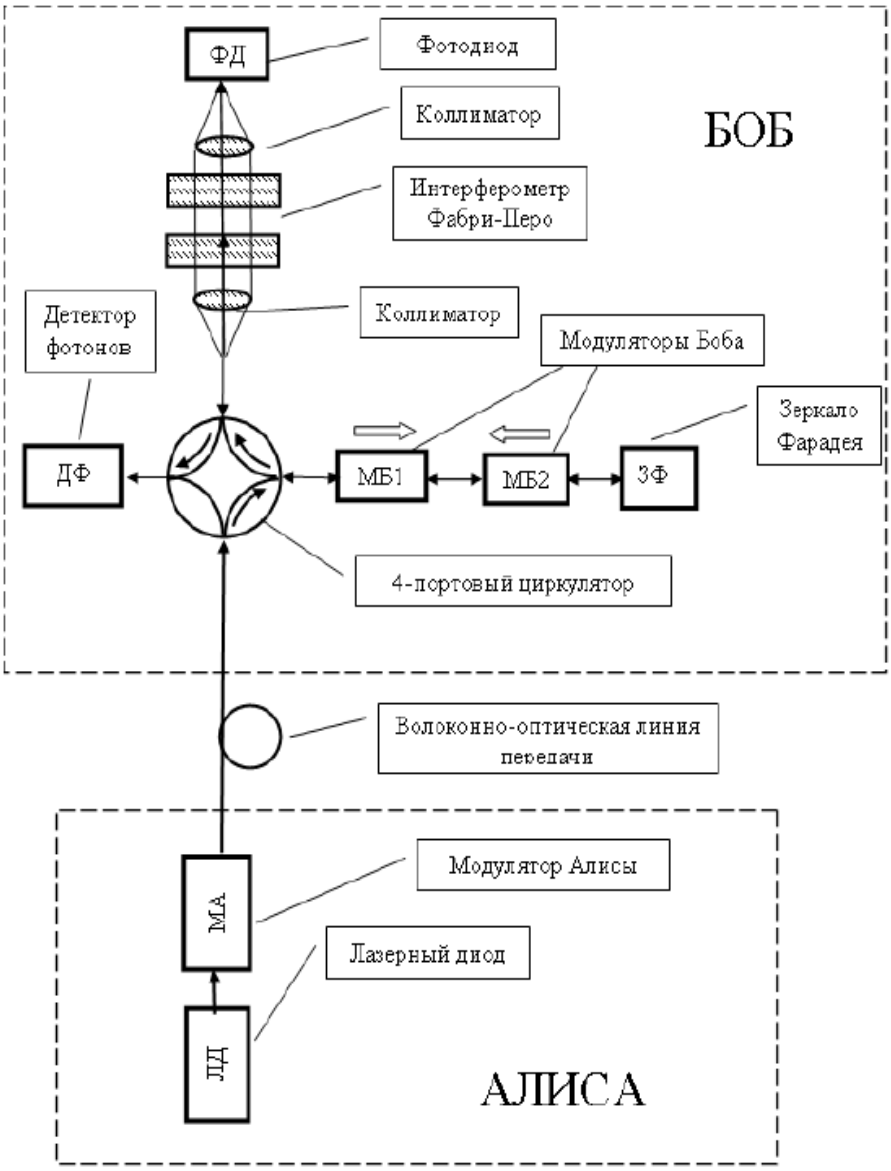
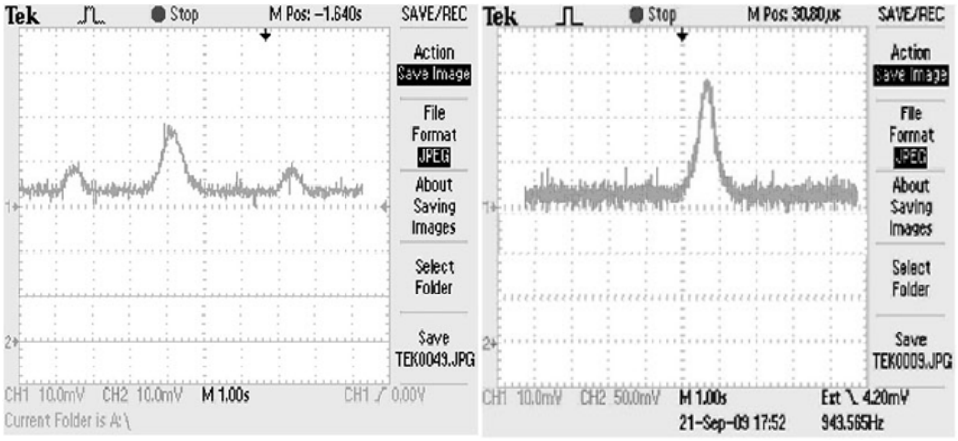


Рис. 3. Принципиальная схема согласованного устройства КРКПЧ

Экспериментальные результаты

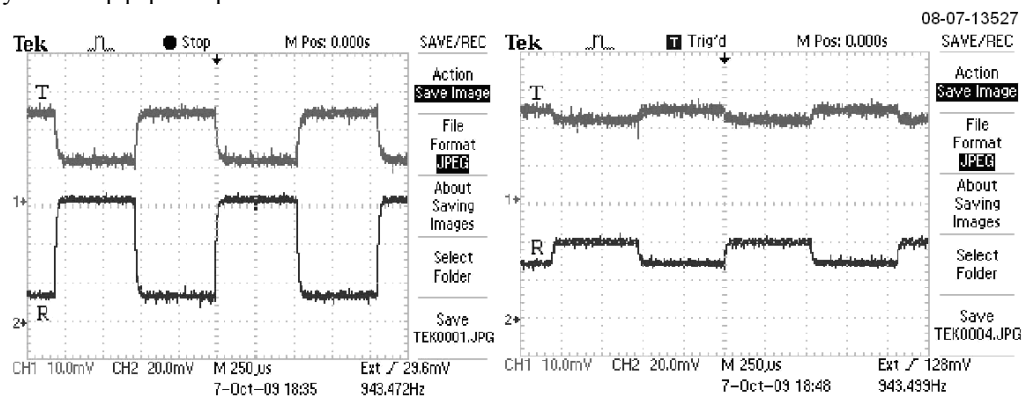
Используемые в технологии безопасного распространения ключа явления конструктивной и деструктивной интерференции на поднесущих частотах были продемонстрированы (для классического режима) в экспериментах со сканированием частоты лазера при одновременной записи на осциллографе спектров излучения, прошедших через спектральный фильтр. Соответствующие осциллограммы приведены на рис. 4.



а б

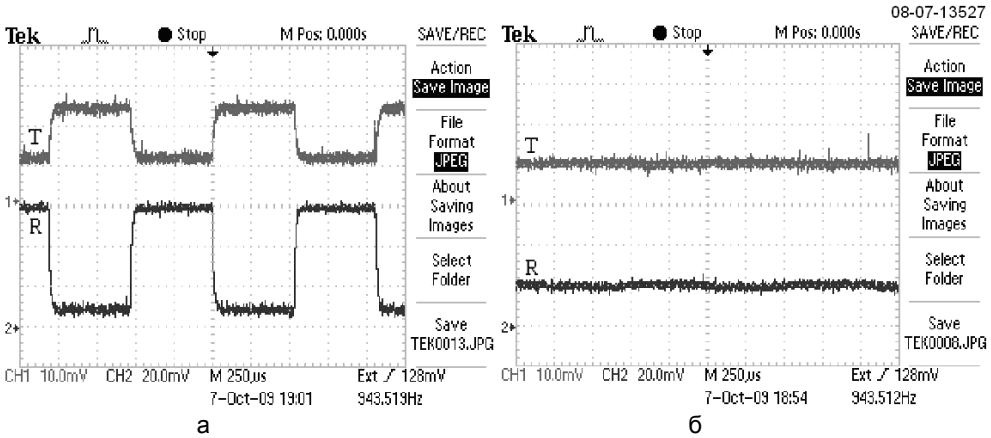
Рис. 4. Спектры сигнала при конструктивной (а) и деструктивной (б) интерференциях на поднесущих частотах

Для проверки эффективности компенсации поляризационной зависимости модуляторов был произведен следующий опыт. Оптическое волокно в области между Алисой и Бобом подвергалось механическому воздействию, в результате чего состояние поляризации передаваемого сигнала произвольно менялось, и в схеме без компенсации интерференционная картина должна была заметно исказиться. На рис. 5–6 приведены результаты этого опыта. Кривая T соответствует прошедшему сквозь интерферометр Фабри–Перо сигналу, т.е. сигналу на основной частоте, а кривая R – сигналу на боковой частоте, отраженному от интерферометра.



а б

Рис. 5. Сравнение интерференционных картин при осцилляции разности фаз поднесущих частот в схеме с реализованным механизмом компенсации (а) и без компенсации (б). Исходное состояние



а б

Рис. 6. Сравнение интерференционных картин при осцилляции разности фаз поднесущих частот в схеме с реализованным механизмом компенсации (а) и без компенсации (б). Результат механического воздействия

Из приведенных рисунков видно, что интерференционная картина при наличии компенсации не искажается, что позволяет утверждать, что эксперимент подтвердил практическую применимость описанного механизма компенсации.

Заключение

Предлагаемая модифицированная схема является согласованной (plug-and-play), поскольку в ней 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 привлекательным для практического применения, чем более традиционные схемы, использующие классический импульс только в целях синхронизации сигналов.

Литература

1. Bennett C.H. and G. Brassard. 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. and H. Zbinden. Quantum cryptography // Rev. Mod. Phys. – 2002. – V. 74. – P. 145.
3. Bennett C.H. Quantum cryptography using any two nonorthogonal states // Phys. Rev. Lett. – 1992. – V. 68. – P. 3121.
4. Мазуренко Ю.Т., Мерола Ж.-М., Годжебюр Ж.-П. Квантовая передача информации с помощью поднесущей частоты. Применение к квантовой криптографии // Оптика и спектроскопия. – 1999. – Т. 86 – С. 181.
5. Merolla J.-M., Mazurenko Y., Goedgebuer J.-P., Porte H. and W.T. Rhodes. Phasemodulation transmission system for quantum cryptography // Optics Lett. – 1999. – V. 24. – P. 104.
6. Merolla J.-M., Mazurenko Y., Goedgebuer J.-P. and W.T. Rhodes Single photon interference in sidebands of phase-modulated light for quantum cryptography // Phys. Rev. Lett. – 1999. – V. 82 – P. 1656.
7. Merolla J.-M., Mazurenko Y., Goedgebuer J.-P., Duraffourg L., Porte L. and W.T. Rhodes. Quantum cryptographic device using single photon phase modulation // Physical Review A. – 1999. – V. 60. – P. 1899.
8. Duraffourg L., Merolla J.-M., Goedgebuer J.-P., Mazurenko Y. and W.T. Rhodes. Compact transmission system using single-sideband modulation of light for quantum cryptography // Optics Letters. – 2001. – V. 26 – P. 1427.
9. Guerreau O.L., Merolla J.-M., Soujaeff A., Patois F., Goedgebuer J.-P., Malassenet F.J. Long-distance QKD transmission using single-sideband detection scheme with WDM synchronization // Selected Topics in Quantum Electronics. – 2003. – V. 9 – P. 1533.
10. 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.

Рупасов Андрей Викторович – Санкт-Петербургский государственный университет информационных технологий, механики и оптики, студент, sadbender@yandex.ru

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

Егоров Владимир Ильич – Санкт-Петербургский государственный университет информационных технологий, механики и оптики, студент, egorovvl@gmail.com

Мазуренко Юрий Тарасович – Санкт-Петербургский государственный университет информационных технологий, механики и оптики, доктор физ.-мат. наук, старший научный сотрудник, yurimaz@gmail.com