Элементы сложносоставных модуляторов для систем квантовой связи на боковых частотах

Н. Д. Герасименко[2], В. С. Герасименко[1, 2]

[1] Национальный исследовательский университет ИТМО, Санкт-Петербург, Россия
[2] ООО "СМАРТС-Кванттелесом", Санкт-Петербург, Россия

В системах квантовой связи на боковых частотах основными элементами являются фазовые модуляторы, однако с ними соседствуют и другие, зачастую не менее важные компоненты. Главные из них — это перестраиваемый аттенюатор в блоке отправителя (в Алисе) и связка двух фазовых модуляторов с поляризационными светоделителями в блоке получателя (в Бобе). Подсистема модулятор-аттенюатор в Алисе необходима для того, чтобы гарантировать отправку в канал однофотонного состояния в правильное время. Использование же поляризационных делителей и двух модуляторов в Бобе связано с тем, что модуляторы — поляризационно-зависимые устройства, а канал связи — обычный одномодовый. В данной работе рассматривается моделирование интегрально-оптических элементов, позволяющих объединить названные подсистемы на одном чипе.

Ключевые слова: Фазовая модуляция света, Амплитудная модуляция света, Управление светом, Интегральная оптика, Ниобат лития.

Цитирование: **Герасименко, Н. Д.** Элементы сложносоставных модуляторов для систем квантовой связи на боковых частотах / Н. Д. Герасименко, В. С. Герасименко // HOLOEXPO 2023: 20-я Международная конференция по голографии и прикладным оптическим технологиям : Тезисы докладов. — СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2023. — С. 236–239.

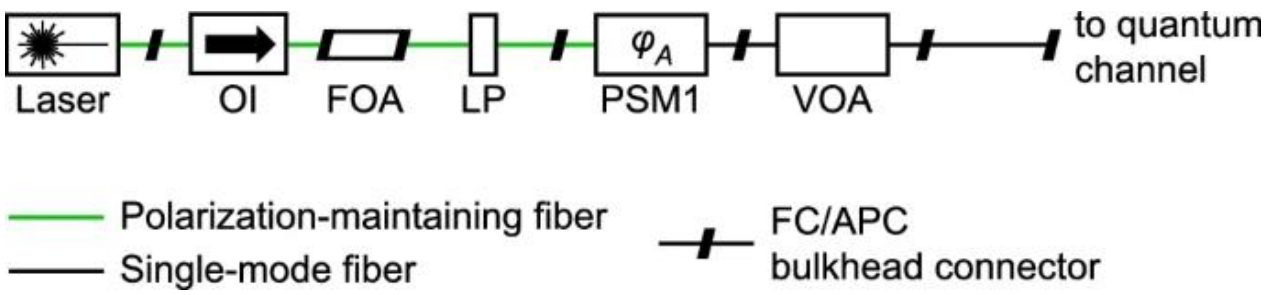
Введение

Системы квантовой рассылки ключа (КРК) на боковых частотах (БЧ) активно разрабатываются уже больше 10 лет [1]. Именно такие системы использовались при первой в России передаче квантового ключа по городской оптоволоконной сети [2]. Они же применяются в создаваемых сейчас междугородних линиях квантовой связи.

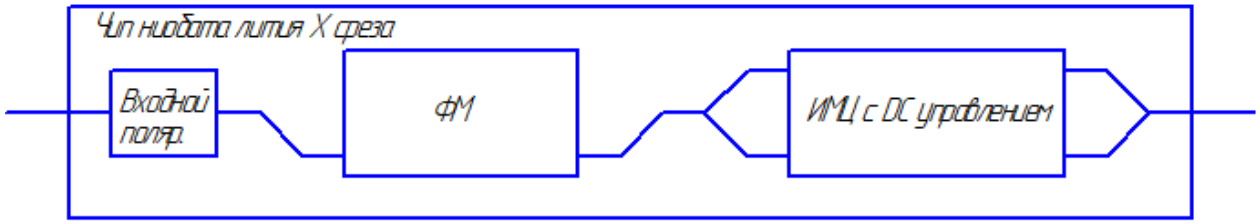
За это время было сделано многое для повышения скорости генерации квантового ключа и защиты системы от различных атак [2, 3]. Главными из них являются троянский конь и лазерное повреждение. В первом случае злоумышленник (Ева) отправляет в квантовый канал импульс большой мощности, чтобы по результатам анализа отраженного света судить о состоянии устройства, кодирующего информацию (в случае КРК БЧ — электрооптического фазового модулятора) [4]. Обычно такую атаку предпринимают против блока получателя (Боба), но возможность подобного воздействия на блок отправителя (Алису) нужно учитывать. Во втором варианте атаки злоумышленник использует обстоятельство, что в любые системы КРК ослабляют до одиночных фотонов излучение лазерного источника и используют для этого обычно оптомеханические устройства. Это позволяет Еве попытаться своим мощным лазером повредить аттенюатор в Алисе, чтобы увеличить число фотонов в канале [5].

1. Составное устройство в блоке отправителя

Оптическая схема Алисы состоит из лазерного источника (Laser), изолятора (IO), статичного оптического аттенюатора (FOA), линейного поляризатора (LP), электрооптического фазового модулятора (PSM1), соединенных последовательно волокнами с сохранением поляризации, и перестраиваемого аттенюатора (VOA), как изображено на рис. 1а [3]. Из перечисленных компонентов три можно объединить в одном устройстве: линейный поляризатор, фазовый модулятор и перестраиваемый аттенюатор. В принципе для этого достаточно модифицировать волноводную схему типичного амплитудного модулятора на подложке ниобата лития как показано на рис. 1б: сместить волноводный интерферометр Маха-Цендера (ИМЦ) под область электрода постоянного тока (DC), а линейный волновод со стороны входа схемы расположить с помощью S-образных изгибов в зазор между СВЧ электродами. При этом все остальные элементы модулятора остаются без изменений [6]. Также можно отметить, что при использовании предложенной схемы попытка лазерного повреждения не приведет к увеличению числа фотонов в канале, а даже если повреждение случится — потери только возрастут. С точки же зрения опасности применения троянского коня ИМЦ в состоянии с низким пропусканием не зависит от направления прохода, так что потенциальный «сканирующий» импульс все равно испытает двойное ослабление; кроме того, количество отражающих поверхностей в схеме сократится.



а) схема блока отправителя [3]



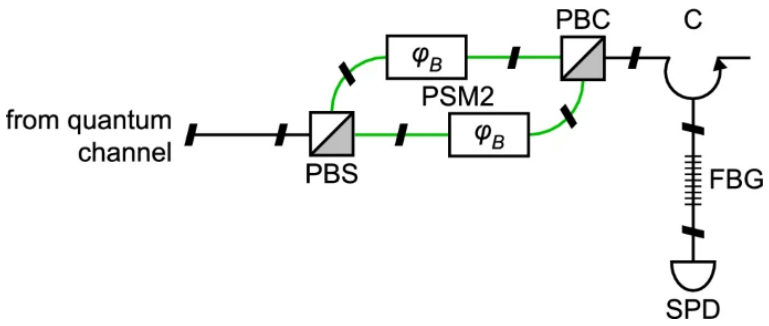
б) схема комбинированного устройства, объединяющего LP (Входной поляр.), PSM1 (ФМ) и VOA (ИМЦ с DC управлением)

Рис. 1. Оптические компоненты Алисы

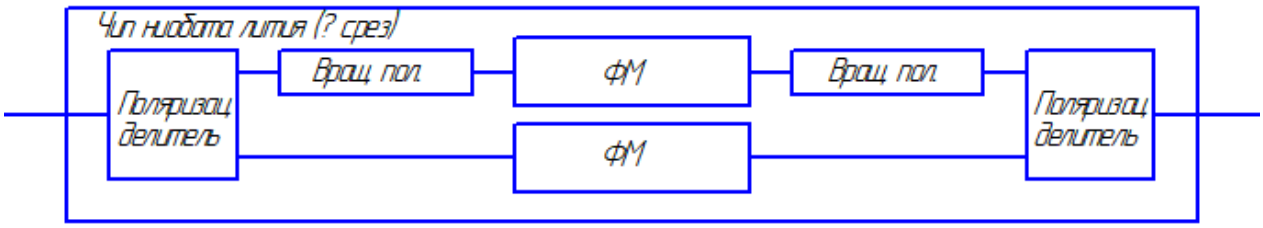
2. Составное устройство в блоке получателя

В схеме же Боба используются поляризационный делитель (PBS), два соединенных параллельно электрооптических фазовых модулятора (PSM2), поляризационный объединитель (PBC), оптический циркулятор (C), светофильтр на основе Брегговской решетки

(FBG) и однофотонный детектор (SPD), изображеные на рис. 2а, при этом волокна от выхода PBS до входа PBC (в обоих случаях включительно) сохраняют поляризацию[3]. В данном случае можно попытаться объединить часть, собранную на волокнах с сохранением поляризации: волноводные поляризационные делители отличаются от неполяризационных только протяженностью области перекачки энергии, при этом делители и объединители устроены одинаково; с фазовыми модуляторами сложнее — в силу линейности электрооптического эффекта в ниобате лития при симметричном расположении волноводов относительно СВЧ электрода возникающая фазовая задержка будет иметь противоположные знаки, — скорее всего, придется делать два независимых СВЧ электрода с одинаковым относительно них расположением волноводов; также отдельной задачей оказывается получение вращателей поляризации, при этом решать ее можно несколькими способами. Тем не менее получение этого усложненного на этапе производства составного модулятора позволит упростить настройку и эксплуатацию Боба и может ограниченно повысить его защищенность от атак типа троянский конь.



а) схема блока получателя [3]



б) схема комбинированного устройства, объединяющего PBS (Поляризац. делитель), PSM2 (ФМ) и PBC (Поляризац. делитель), требует добавления вращателей поляризации

Рис. 2. Оптические компоненты Боба

Заключение

В данной работе были предложены схемы сложносоставных модуляторов на подложках ниобата лития, объединяющие несколько узлов, используемых в системах КРК БЧ, на одном чипе. Предложенные комбинированные устройства в той или иной степени улучшают защищенность Алисы и Боба от наиболее распространенных атак и потенциально улучшают их эксплуатационные характеристики.

Список источников

[1] **Egorov, V. I.** Analysis of a sidebands-based quantum cryptography system with different detector types / V. I. Egorov, D. N. Vavulin, I. Z. Latypov, A. V. Gleim, A. V. Rupasov // Nanosystems: Physics, Chemistry, Mathematics. – 2013. – Vol. 4. – №. 2. – P. 190-195.

[2] **Gleĭm, A. V**. Sideband quantum communication at 1 Mbit/s on a metropolitan area network / A. V. Gleĭm, V. V. Chistyakov, O. I. Bannik, V. I. Egorov, N. V. Buldakov, A. B. Vasilev, A. A. Gaĭdash, A. V. Kozubov, S. V. Smirnov, S. M. Kynev, S. É. Khoruzhnikov, S. A. Kozlov, V. N. Vasil'ev // Journal of Optical Technology. – 2017. – Vol. 84. – №. 6. – P. 362-367.

[3] **Sajeed S.** An approach for security evaluation and certification of a complete quantum communication system / S. Sajeed, P. Chaiwongkhot, A. Huang, H. Qin, V. Egorov, A. Kozubov, A. Gaidash, V. Chistiakov, A. Vasiliev, A. Gleim, V. Makarov // Scientific Reports. – 2021. – Vol. 11. – №. 1. – P. 5110.

[4] **Jain N.** Trojan-horse attacks threaten the security of practical quantum cryptography / N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, G. Leuchs // New Journal of Physics. – 2014. – Vol. 16. – №. 12. – P. 123030.

[5] **Huang A.** Laser-damage attack against optical attenuators in quantum key distribution / A. Huang, R. Li, V. Egorov, S. Tchouragoulov, K. Kumar, V. Makarov // Physical Review Applied. – 2020. – Vol. 13. – №. 3. – P. 034017.

[6] **Петров В.М.** Отечественные СВЧ интегрально-оптические модуляторы для квантовых коммуникаций / В. М. Петров, А. В. Шамрай, И. В. Ильичев, П. М. Агрузов, В. В. Лебедев, Н. Д. Герасименко, В. С. Герасименко // Фотоника [Photonics Russia] – 2020. – Т. 14. – № 5. – С. 414-423

[7] Голография. Наука и практика / URL: http://www.holoexpo.ru

[8] **Zherdev, A. Y.** Modeling of spatial-frequency spectrum of security holograms and optoelectronic spectrum analyzer for their identification in real time / A. Y. Zherdev, S. B. Odinokov, D. S. Lushnikov // SPIE Conference Proceeding. — 2011. — Vol. 8074. — P. 80740R. — DOI:10.1117/12.886456.

Elements of complex modulators for quantum communication systems at side bands

N. D. Gerasimenko[2], V. S. Gerasimenko[1, 2]

[1] ITMO University, Saint Petersburg, Russia

2 Quanttelecom LLC, Saint Petersburg, Russia

In systems of quantum communication at side bands, phase modulators are the main elements, but there are other important components too. The main ones are a variable optical attenuator in the sender unit (in Alice) and a bundle of two phase modulators with polarization beam splitters in the receiver unit (in Bob). The modulator-attenuator subsystem in Alice is needed to ensure that the proper single-photon state is sent to the channel at the correct time. The use of polarization splitters and two modulators in Bob is due to the fact that modulators are polarization-dependent devices, and the communication channel is an ordinary single-mode one. In this paper, we consider the modeling of integrated optical elements that make it possible to combine these subsystems on a single chip.

Keywords: Phase modulation of light, Amplitude modulation of light, Light control, Integrated optics, Lithium niobate.