



Е.В. Борисова

ИЗУЧЕНИЕ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ РАЗЛИЧНЫХ ЭЛЕМЕНТОВ ДЛЯ ЗАЩИТЫ СИСТЕМ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА

(Рязанский государственный радиотехнический университет им. В.Ф. Уткина)

Квантовое распределение ключей (КРК) позволяет надежно установить секретный ключ между двумя удаленными сторонами, обычно называемыми Алисой и Бобом [1, 2].

Это делает КРК, в принципе, не поддающимся взлому даже сверхмощным квантовым компьютером. Таким образом, КРК является многообещающим кандидатом на квантово-безопасную криптографию в эпоху квантовых вычислений, которая приближается с реально достижимым в настоящее время квантовым превосходством [3]. Однако на практике достижение невзламываемой системы КРК - это долгий путь из-за несовершенства устройств в реальной жизни. Несовершенства реальных систем КРК могут быть использованы противником, оснащенным современной технологией, для получения секретной информации.

Хорошо защищенный и охарактеризованный источник в системе квантового распределения ключей необходим для обеспечения ее безопасности. Одной из проблем реальной работы квантовых систем распределения ключа является возможность стороннего воздействия на работу приёмо-передающей аппаратуры. В данной статье рассматривается возможность воздействия с помощью лазерного повреждения и возможные пути предотвращения.

Есть достаточно обстоятельные исследования, относительно использования в качестве контрмеры оптоволоконных изоляторов или циркуляторов, которые часто размещаются в качестве последнего компонента в блоке источника. В подобных работах предлагается контрмера против атаки лазерного повреждения, состоящая из дополнительного компонента, размещенного на выходе из источника. Этот компонент должен либо выдерживать мощный входящий свет, ослабляя его до безопасного уровня, который не может модифицировать остальную часть источника, либо разрушаться до постоянного состояния высокого ослабления, которое разрушает линию.

Экспериментально продемонстрировано, что имеющиеся в продаже оптоволоконные изоляторы и циркуляторы обладают этими желаемыми свойствами, по крайней мере, при атаке непрерывным мощным лазером.

Также есть небольшое количество работ, посвящённых исследованию редкоземельных элементов для создания спектрально-селективного поглощения в мощных волоконных лазерах. [4, 5]

В существующих работах проведено исследование наиболее перспективных РЗЭ для создания полностью волоконной защиты диодов накачки. Исследованы спектры поглощения волоконных световодов, активированных ионами Sm^{3+} , Tm^{3+} , Tb^{3+} , Pr^{3+} и Ho^{3+} , имеющими интенсивные полосы поглощения



в ближней ИК области. Показана перспективность ряда РЗЭ для создания защиты источников накачки в конструкциях волоконных лазеров.

Способность реализованного световода эффективно подавлять излучение эрбиевого лазера со средней мощностью вплоть до 10 Вт при одновременно низких оптических потерях на длине волны накачки (981 нм) продемонстрирована экспериментально.

Для обеспечения эффективного спектрально-селективного поглощения необходимо, чтобы оптические потери в световоде на длинах волн сигнала и накачки различались на несколько порядков. Так, для эффективного подавления сигнала необходимо, чтобы уровень его оптических потерь превышал 15 – 20 дБ, в то время как потери для излучения накачки желательно иметь на уровне 0.1 – 0.2 дБ. Для определения наиболее перспективных легирующих добавок были исследованы спектры поглощения световодов, легированных РЗЭ, в широком диапазоне длин волн. [6]

Несмотря на простоту предложенной методики, к настоящему моменту использование легированных РЗЭ волоконных световодов в качестве защиты источников накачки было апробировано лишь в крайне ограниченном количестве работ, что очевидно связано с недостаточным исследованием характеристик РЗЭ в сетке кварцевого стекла. [6]

На мой взгляд, помимо описанного в статье применения оптоволокна, легированного редкоземельными элементами, возможно их применение и для защиты систем квантового распределения ключей. Причём, анализируя полученные результаты в данной статье, можно сделать вывод, что даже небольшая вставка легированного оптоволокна способна предотвратить возможное разрушение основной аппаратуры, при стороннем воздействии мощным лазером.

Литература

1. Bennett C. H. and Brassard G., “Quantum cryptography: Public key distribution and coin tossing,” in Proc. International Conference on Computers, Systems, and Signal Processing (Bangalore, India) (IEEE Press, New York, 1984) pp. 175–179.
2. Gisin N., Ribordy G., Tittel W., and Zbinden H., “Quantum cryptography,” Rev. Mod. Phys. 74, 145–195 (2002)
3. Lo H.-K., Curty M., and Tamaki K., “Secure quantum key distribution,” Nat. Photonics 8, 595–604 (2014).
4. Грух Д.А., Курков А.С., Раздобреев И.М., Фотиади А.А. Квантовая электроника, 32, 1017 (2002) [Quantum Electron., 32, 1017 (2002)].
5. Kotov L.V., Aleshkina S.S., Khudyakov M.M., Bubnov M.M., Medvedkov O.I., Lipatov D.S., Guryanov A.N., Likhachev M.M. J. Lightwave Technol., 35, 4540 (2017)
6. Т. А. Кочергина, С. С. Алешкина, М. М. Худяков, М. В. Яшков, Д. С. Липатов, А. Н. Абрамов, Л. Д. Исхакова, М. М. Бубнов, А. Н. Гурьянов, М. Е. Лихачев, “Использование редкоземельных элементов для создания спектраль-



но-селективного поглощения в мощных волоконных лазерах», Квантовая электроника, 48:8 (2018), 733–737 [Quantum Electron., 48:8 (2018), 733–737]

Т.И. Михеева, К.А. Молодыко

ОСНОВНЫЕ ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ РОЕВОЙ РОБОТИЗИРОВАННОЙ СИСТЕМЫ

(Самарский университет, ИнтелТранС)

В функционал роевого роботизированного устройства входит прием данных от других устройств, а также их передача на соседние устройства, локальное взаимодействие между собой. Каждый агент системы имеет набор простых правил и не имея центральной системы управления, имеет самоорганизующиеся поведение. Базовый функционал роевой системы основан на распределенной сети приема-передачи данных.

В реализуемой системе необходимо обеспечить взаимодействие множества роботизированных устройств между собой, получить, обработать и ретранслировать информацию (рисунок 1).



Рис. 1. UML диаграмма действия агента с информацией

В случае роевой системы, возникают проблемы оптимизации задач и поиска решений, для решения данных проблем используются алгоритмы поисковой оптимизации. Также для самоконтроля и самоорганизации роя необходимо применять методы имитации социального поведения или поведения роя [1] в зависимости от целей и задач поставленных для роевой системы. Методика выбора алгоритма поведения, основана на вариантах решений каждого алгоритма в плане оптимизации, а также в точности расчета поиска решения.