

УДК 681.7.0686

ГЕНЕРАЦИЯ ВТОРОЙ ГАРМОНИКИ В КРИСТАЛЛЕ ФАЗОВОГО МОДУЛЯТОРА ДЛЯ АТАКИ НА СИСТЕМУ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

Сурин Д.А. (ИТМО)

Научный руководитель – кандидат физико-математических наук Наседкин Б.А.
(ИТМО)

Введение. Квантовое распределение ключей является современным методом защищенной коммуникации, который теоретически гарантирует безусловную безопасность, однако практические реализации таких систем выполнены с помощью неидеальных компонентов, из-за чего содержат уязвимости [1]. Одним из таких компонентов является электрооптический фазовый модулятор, в основе которого лежит кристалл ниобата лития. Ниобат лития является нелинейно-оптическим материалом, в котором возможен эффект генерации второй гармоники. Именно этот эффект может быть использован злоумышленником для осуществления атаки на техническую реализацию систем квантового распределения ключей, поэтому его изучение актуально с целью поиска контрмер и повышения безопасности.

Основная часть. В настоящей работе исследуется кристалл ниобата лития х-среза, подготовленный для использования в фазовом модуляторе. Рассчитаны длины волн излучения накачки, при которых выполняется условие фазового синхронизма, а следовательно, реализуется эффект генерации второй гармоники, то есть генерация излучения с частотой вдвое большей частоты излучения накачки [2]. Эффект был продемонстрирован в эксперименте при использовании импульсного лазера с длиной волны 1050 нм. Сгенерированное излучение может быть использовано для осуществления атаки с ослеплением детектора одиночных фотонов [3], при этом излучение накачки останется незамеченным, так как не попадает в диапазон чувствительности мониторингового фотодиода.

Выводы. Предложен способ незаметно ввести в систему длинноволновое излучение на длинах волн 1055 нм, 1679 нм и 2428 нм с последующим преобразованием частоты в кристалле фазового модулятора с целью ослепления детектора одиночных фотонов. Показано, что при использовании импульсной накачки на длине волны 1050 нм мощностью 47 мВт, в кристалле генерируется излучение с длиной волны 525 нм мощностью 181 мкВт.

Список использованных источников:

1. Diamanti E. et al. Practical challenges in quantum key distribution // npj Quantum Information. – 2016. – V. 2. – No. 1. – P. 1-12.
2. Helt L. G., Liscidini M., Sipe J. E. How does it scale? Comparing quantum and classical nonlinear optical processes in integrated devices // JOSA B. – 2012. – V. 29. – No. 8. – P. 2199-2212.
3. Huang A. et al. Testing random-detector-efficiency countermeasure in a commercial system reveals a breakable unrealistic assumption // IEEE Journal of Quantum Electronics. – 2016. – V. 52. – No. 11. – P. 1-11.