УДК 681.3.067:621.396.2

Д.М. Голубчиков

МЕТОДИКА ИССЛЕДОВАНИЯ И ОЦЕНИВАНИЯ СИСТЕМ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

Показана необходимость разработки методики исследования и оценивания систем квантовой криптографии. Выделены компоненты для детального изучения, проведены эксперименты и продемонстрировано влияние параметров излучающего модуля и дисперсионных показателей линии на характеристики эффективности и защищенности систем квантового распределения ключей.

Системы квантового распределения ключей; методики исследования; эффективность, защищенность.

D.M. Golubchikov

TECHNIQUE OF RESEARCH AND EVALUATION OF QUANTUM KEY DISTRIBUTION SYSTEMS

The relevance of development of technique of research and evaluation of quantum key distribution system was demonstrated. Components which requires detailed analysis were choosen. Experiments were made and influence of parameters of emitting module and dispersing factor of communication line on characteristics of efficiency and security of quantum key distribution system was proved.

Quantum key distribution systems; technique of research; efficiency; proofness.

Квантовая криптография – динамично развивающаяся ветвь науки о квантовых вычислениях, первой реализованная в экспериментальных моделях и системах. На рынке уже представлены первые коммерческие системы квантовой криптографии. Однако фирмы, производящие оборудование данного класса, предпочитают держать в секрете технологические новинки, применяемые ими при построении систем. Такая политика не дает заказчикам уверенности в эффективности и реальной защищенности систем кантового распределения ключей. В связи с этим общественность заинтересована в комплексном экспериментальном исследовании производимых систем и опубликовании результатов тестирования. Компании предлагают результаты собственных тестирований, критерии оценки которых различны у всех производителей и не могут дать объективного результата.

Вследствие чего необходимо разработать методику исследования и оценивания систем квантового распределения ключей, которая бы учитывала индивидуальные особенности систем от разных производителей.

Как указывается в [1-3] все предлагаемые коммерческие системы основываются на так называемой технологии «Plug&Play» и построены по схеме интерферометра с автоматической компенсацией поляризационных искажений, предложенной Мартинелли в работе [4]. При более детальном рассмотрении оптической части систем были выявлены функциональные особенно-

сти, такие как наличие дополнительной линии задержки и классического детектора в Id 5000 Vectis. В части отвечающей за шифрование трафика основным отличием является уровень модели OSI, на котором происходит шифрование данных. В MagiQ QPN7505 и SQBox Defender данные шифруются с помощью алгоритма AES 256-ти битным и 192-х битным ключами соответственно. Причем в SQBox данные шифруются на физическом уровне модели OSI, в QPN7505 на канальном уровне. Id 5000 Vectis позволяет выбирать длину ключа из набора 128, 192, 256 бит для шифра AES и шифрует данные на канальном уровне, как и QPN5505.

При исследовании квантовых криптографических систем основное внимание уделяется их оптической части, отвечающей за процесс формирования и пересылки квантовых состояний. Основой этой части являются источник и приемники излучения. Для дальнейшей оценки характеристик необходимо получить энергетические и частотные характеристики лазерного импульса, а так же его форму при разных длительностях. К энергетическим характеристикам отнесем уровень мощности на выходе устройства. Для его измерения выход передающего блока необходимо соединить с высокочувствительным измерителем мощности оптического излучения. В нашем эксперименте роль такового выполнял оптический анализатор спектра Yokogawa ANDO AQ-6370. По результатам измерений была построена таблица допустимых значений зависимости мощности передающего модуля от длительности импульса. Максимальная мощность регистрировалась при длительности импульса 10000 пс и составляла 40,3 мкВт, а минимальная (регистрируемая) – 0,163 мкВт при длительности импульсов излучения 400 пс. При дальнейшем уменьшении длительности импульсов значение мощности невозможно зарегистрировать с помощью данного прибора. По результатам анализа полученных данных построены графики, которые позволяют рассчитать ожидаемую мощность на выходе устройства при дальнейшем снижении длительности импульса. Полученная зависимость является линейной. Мощность излучения приблизится к 0 при длительности порядка 20 пс. Все расчеты проводились с учетом влияния на уровень мощности выходного аттенюатора, так как минимальное значение затухания 1,35 дБ, устанавливаемое на нем, исключить невозможно (для системы QPN 5505). Исследование частотных характеристик передающего модуля показало наименьшую ширину спектра излучения 0,014 нм при значениях длительности импульса от 1500 до 6500 нс, при выходе за эти пределы значение ширины спектра растет. Так на минимальных длительностях импульса оно возрастает до 0,11 нм. Оценивая полученные значения ширины спектра оптического излучения можно сделать вывод о применении лазерного модуля с распределенной обратной связью. Уширение спектра излучения отрицательно сказывается на форме оптического импульса при распространении через оптический канал. Для анализа формы импульса к выходу передающего модуля необходимо подключить высокочастотный осциллограф через аналоговый приемный оптический модуль. Для получения формы использован цифровой осциллограф LeCroy WS104XS и аналоговый приемный оптический модуль ПРОМ-0112. На рис. 1 приведены формы максимального и минимального по

длительности оптических импульсов, как результат кусочно-линейной аппроксимации кривых, полученных на осциллографе.

Полученных данных достаточно для анализа процесса распространения оптического импульса в волоконно-оптической линии связи большой протяженности и изменения его параметров на выходе.

Все производители гарантируют работу своего оборудования на линиях до 100 км. Не указывая при этом действительную скорость генерации секретных ключей. На протяженных дистанциях значительное влияние на оптический импульс оказывают дисперсионные характеристики волокна.

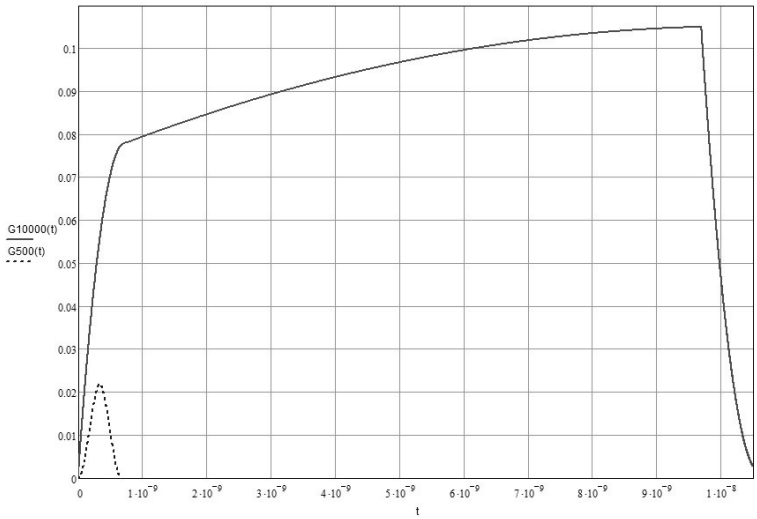

Рис. 1. Формы оптических импульсов максимальной и минимальной длительности

Вторым этапом исследования характеристик квантовых систем распределения ключей является анализ процесса прохождения оптического импульса волоконно-оптической линии, которая является средой распространения оптического излучения и, в зависимости от примененного типа волокна, оказывает существенное влияние на скоростные характеристики систем квантовой криптографии [5]. При анализе было показано, что влияние межмодовой и поляризационной дисперсий отсутствует вследствие использования одномодового волокна и схемы автокомпенсации поляризационных искажений. Но влияние хроматической дисперсии сильно искажает форму, и, следовательно, ведет к перераспределению вероятности появления фотона в интервале времени регистрации. Рисунок 2 иллюстрирует изменение формы импульса при распространении через волоконно-оптическую линию связи протяженностью 100 км, первый график показывает искажение формы импульса длительностью 10000 пс при ширине спектра излучения лазера 0,02 нм, второй график показывает изменение формы при длительности импульса 500 пс и ширине спектра излучения 0,05нм. Учитывая рекомендации производителей работать с длительностями импульсов 400-600 пс, такое существенное перераспределение вероятности момента появления фотона на входе детектора ведет к необходимости

уширения интервала детектирования, что в свою очередь приводит к росту двойных срабатываний и снижению общей скорости формирования секретных ключей.

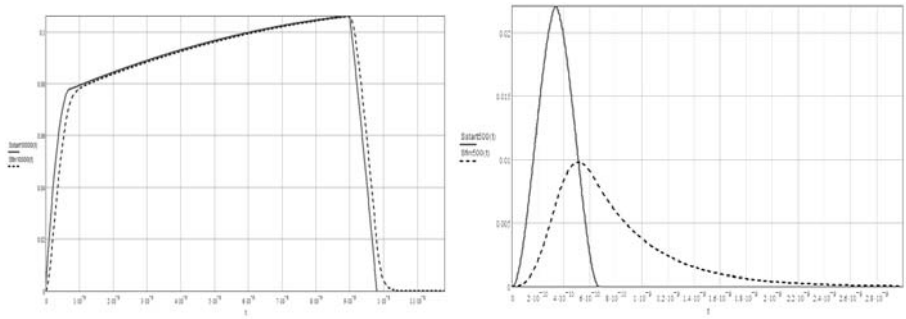

Рис. 2. Искажение формы оптического импульса

Как видно из графиков при работе с импульсами большой длительности расширение интервала ожидания регистрации фотона практически не требуется. А при работе с малыми длительностями интервал ожидания регистрации увеличивается более чем в 3 раза по отношению к длительности исходного импульса. Это обстоятельство необходимо учитывать при настройке систем квантового распределения ключей.

При исследовании систем квантовой криптографии и анализе распространения излучения в квантовом канале при прямом прохождении сигнала достаточно использовать математический аппарат волновой оптики, но при обратном распространении сигнала необходимо переходить к описанию посредствам аппарата квантовой оптики, так как при обратном распространении сигнал ослабляется до уровня однофотонного. Как уже было отмечено, изменение формы оптического импульса приводит к перераспределению вероятности момента появления фотона на входе детектора. Форма импульса отображает функцию плотности вероятности обнаружения фотона на интервале времени. Вероятность регистрации фотона на интервале $[t_1;t_2]$ представляется интегралом функции распределения плотности вероятности на этом интервале с учетом коэффициента затухания волоконно-оптического тракта. Для достижения максимальной эффективности можно изменять интервал регистрации фотона с целью снижения количества импульсов темнового тока попадающих в этот интервал.

Эффективность систем квантовой криптографии определяется скоростью формирования ключей и характеристиками защищенности канала. Скорость формирования ключей зависит от таких параметров как частота следования оптических импульсов, задается тактовым генератором системы, среднее колво фотонов на импульс, устанавливается с помощью коэффициента затухания аттенюаторов, и коэффициента эффективности однофотонного детектора, зависит от материала детектора и напряжения смещения. Оптические импульсы на выходе появляются с частотами 607,5 кГц для MagiQ QPN 5505 и 5 МГц для Id 3000 Clavis. Однако в Id 3000 Clavis использована покадровая стратегия передачи квантовых состояний, что существенно снижает эффективную частоту генерации, на которую оказывает влияние длина канала связи, чем длин-

нее канал, там больше задержка между кадрами. Среднее количество фотонов на импульс является как показателем, влияющим на скорость формирования ключей, так и показателем изменяющим уровень защищенности квантового канала от атак разделения оптического потока[6,7]. В системах квантовой криптографии применен лазерный источник излучения на выходе которого число фотонов распределено по закону Пуассона и для получения однофотонного импульса необходимо обеспечить ослабление сигнала до уровня мощности -101,09 дБм при частоте следования 607,5 кГц – это будет соответствовать среднему числу фотонов на импульс $\mu = 1$, и, доля двух- и более фотонных импульсов составят свыше 29% от общего числа, что снижает характеристики защищенности квантового канала, а доля бесфотонных составит 36,7%. Производители рекомендуют выбирать $\mu = 0{,}1..0{,}5$, тогда доля многофотонных импульсов составит от 0,4% до 9%, однако и доля бесфотонных возрастет до 90,5% и 60,6% соответственно.

Самым сложным этапом исследования систем квантовой криптографии является исследование характеристик однофотонных детекторов, так как оно требует вскрытия аппаратуры квантовой криптографии и внедрения в схему измерительных устройств. Важными характеристиками эффективности работы однофотонных детекторов являются напряжение смещения, длительность и амплитуда вольтодобавки, температура фотодиода.

С появлением на рынке новых устройств и решений в области квантовой криптографии необходимо проводить корректировку методики оценивания, учитывая особенности и ноухау появляющихся систем.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Stucki D, Gisin N, Guinnard O, Ribordy G and Zbinden H.* Quantum key distribution over 67 km with a plug&play system // New Journal of Physics. - 2002. Vol. 4. – № 1. - P. 41.
2. *Muller A, Herzog T, Huttner B, Tittel W, Zbinden H and Gisin N.* Plug&play systems for quantum cryptography // Appl. Phys. Lett. – 1997. Vol. 7. P.793–795.
3. *Ribordy G, Gautier J-D, Gisin N, Guinnard O and Zbinden H.* Fast and user-friendly quantum key distribution // J. Mod. Opt. – 2000. Vol. 47. – P.517–531.
4. *Martinelli M.* A universal compensator for polarization changes induced by birefringence on a retracting beam // Opt. Commun. – 1989. Vol. 72. - P. 341-344.
5. *Голубчиков Д.М.* Моделирование квантового канала распределения ключа // Известия ТРТУ. Специальный выпуск. Технические науки. Материалы LII научно-технической конференции профессорско-преподавательского состава, аспирантов и сотрудников ТРТУ. - Таганрог: Изд-во ТРТУ. 2006. – №9(64) - С.162-163.
6. *Nielsen P M, Schori C, Sorensen J L, Savail L, Damgard I and Polzik E.* Experimental quantum key distribution with proven security against realistic attacks // J. Mod. Opt. – 2001. Vol. 48. - P.1921–1942.
7. *Голубчиков Д.М.* Анализ возможности использования квантового усилителя для съема информации с квантового канала распределения ключа и методы его обнаружения. // Информационные системы и технологии 2007. Научно-техническая конференция студентов, аспирантов и молодых преподавателей. Тезисы докладов. - Обнинск, отдел множительной техники ИАТЭ, 2007. - С. 52-53.

Голубчиков Дмитрий Михайлович
Технологический институт федерального государственного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: golubchikov.dmitry@gmail.com.
347928, г. Таганрог, пер. Гарибальди, 2, кв. 6.
Тел.: 8-906-421-85-97.
Кафедра радиоэлектронных средств защиты и сервиса.
Аспирант.

Golubchikov Dmitry Mikhailovich
Taganrog Institute of Technology – Federal State-Owned Educational Establishment of Higher Vocational Education “Southern Federal University”.
E-mail: golubchikov.dmitry@gmail.com.
2, Garibaldi, Taganrog, 347928, Russia.
Phone: 8-906-421-85-97.
Department of Electronic Means of Protection, Security and Services.
Post-graduate student.