ИЗВЕСТИЯ РАН. СЕРИЯ ФИЗИЧЕСКАЯ, 2020, том 84, № 3, с. 447–450

УДК 530.145.1

ВИЗУАЛЬНЫЕ СРЕДСТВА ДЛЯ МОНИТОРИНГА МАГИСТРАЛЬНЫХ КВАНТОВЫХ СЕТЕЙ

© 2020 г. А. А. Литвинов[1, 2], Е. М. Кацевман[2], О. И. Банник[1, 2], Л. Р. Гилязов[1, 2], К. С. Мельник[1, 2], М. Р. Амирханов[2], Д. Ю. Таранкова[3], А. Р. Яфаров[1, 2], Н. С. Перминов[1, 2, 4, *]

[1]Федеральное государственное бюджетное образовательное учреждение высшего образования "Казанский национальный исследовательский технический университет имени А.Н. Туполева-КАИ", Казанский квантовый центр, Казань, Россия

[2]Общество с ограниченной ответственностью "Казанские квантовые коммуникации", Казань, Россия

[3]Федеральное государственное бюджетное образовательное учреждение высшего образования "Казанский национальный исследовательский технический университет имени А.Н. Туполева-КАИ", Кафедра радиоэлектроники и информационно-измерительной техники, Казань, Россия

[4]Казанский физико-технический институт имени Е.К. Завойского – обособленное структурное подразделение Федерального государственного бюджетного учреждения науки "Федеральный исследовательский центр "Казанский научный центр Российской академии наук", Казань, Россия

**E-mail: qm.kzn@ya.ru*

Поступила в редакцию 20.09.2019 г.
После доработки 15.11.2019 г.
Принята к публикации 27.11.2019 г.

Рассмотрена проблема визуального мониторинга магистральных квантовых сетей с линиями протяженностью более 100 км. Выполнен анализ локальных трендов параметров производительности для экспериментальной демонстрации междугородней квантовой связи и перспектив коммерциализации квантово-классических облачных сервисов защиты.

DOI: 10.31857/S0367676520030187

ВВЕДЕНИЕ

Комплексные решения [1] в области систем квантовой коммуникации (КК) имеют решающее значение для реализации квантовых сетей, способных работать как в городских, так и в магистральных стандартных волоконно-оптических линиях связи (ВОЛС). При этом, с точки зрения систем связи, особую сложность в реализации представляют магистральные квантовые сети (МКС) с линиями длиной более 100 км и потерями между узлами более 25 дБ, где соотношение "сигнал/шум" нельзя считать большим. С точки зрения фундаментальной статистики принципиальная сложность здесь заключается в том, что несмотря на относительной невысокий средний процент ошибок величина размаха ошибок и дисперсия ошибок могут быть крайне велики, что влечет малую достоверность диагностирования ошибок при выполнении непрерывных тестов МКС и особенно масштабных МКС с большим числом узлов.

Решением для подобной проблемы в теории связи является применение прогностических средств мониторинга и фильтрации ошибок, что позволит увеличить достоверность определения QBER (quantum bit error rate) для междугородних КК в режиме непрерывного использования. Отметим также, что ввиду больших ошибок для предельных паспортных режимов работы комплексов КК, безопасность комплекса связи должна определяться специальной диагностической системой, отличной от диагностической системы для рабочих паспортных режимов. Эта разница в диагностике обусловлена и тем, что достоверность определения ошибок в предельном режиме эффективно зависит от значительного большего числа физических факторов, которые не всегда легко отслеживать в рамках работы одного конструкционно законченного изделия. То есть более мощная специализированная система диагностики должна поставляться с комплексом КК в виде отдельного изделия и уметь работать в фоновом режиме МКС для отслеживания всей истории изменений в работоспособности линии даже при отключенном комплексе КК в узле.

В данной работе исследованы тренды и корреляции параметров производительности для первого в России экспериментальной междугородней квантовой связи на 143 км при 37 дБ потерь на стандартных ВОЛС [2], что превышает 100 км (размер малого стандартного плеча магистраль-

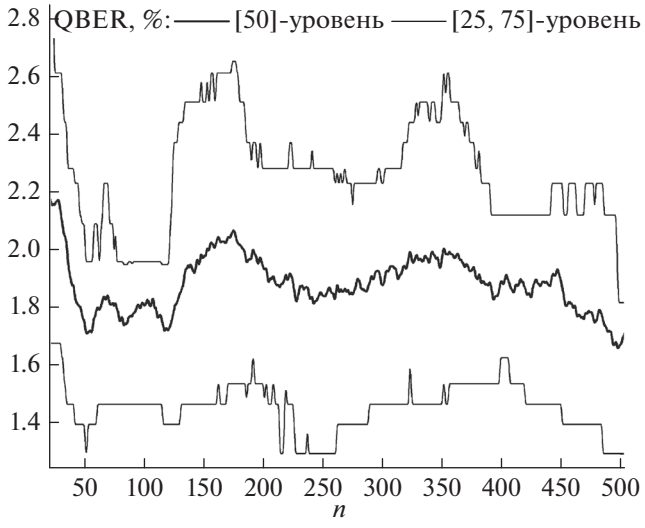

Рис. 1. Процентные фильтры уровней [25, 50, 75] при 50-точечном сглаживании для значений QBER, показывающие наличие трендов в ошибках на протяжении двухдневных тестов.

ных ВОЛС вдоль железных дорог) с затуханием более 25 дБ.

ШУМЫ В КВАНТОВОЙ СВЯЗИ И СОВРЕМЕННАЯ СТАТИСТИКА

В августе 2019 г. была экспериментально продемонстрирована магистральная квантовая связь [2] на расстоянии 143 км между городом Казань и поселком городского типа Апастово в Республике Татарстан с использованием прототипа квантового распределения ключей, обеспечивающего высокую помехоустойчивость линий и узлов сети за счет фазового кодирования в поднесущей волне [3]. Средняя скорость генерации секретного ключа составляла 12 бит в секунду с потерями в линии – 37 дБ на расстоянии 143 км в течение многодневного полевого испытания. Ранее в [6] сообщалось о попытке реализовать стабильные коммерческие дальнодействующие КК на регулярной волоконной линии, где для условий, аналогичных нашим [2] условиям (потери 37 дБ), было получено отношение скорости генерации ключей к тактовой частоте около 7 бит/с на 100 МГц, что примерно в 2 раза ниже значений для нашего теста 12 бит/с на 100 МГц в Казани [2]. Однако в работе [6] невозможно было получить достаточно стабильную работу системы КК в течение нескольких дней, чтобы быть уверенным в достоверности параметров безопасности. Мы предполагаем, что после решения вопросов стабилизации (как это было сделано, например, в [7]), комплекс КК, описанный в [6, 8], будет пригоден для дальнодействующих МКС.

Большинство новых идей [9] об аксиоматически достоверной сверхвысокой квантовой безопасности являются доказательными только в рамках стандартных статистических методов и оперируют по существу только одним понятием только одного из подвидов информационной энтропии [10, 11]. Однако хорошо известно, что для количественного доказательства случайности генератора случайных чисел, являющегося наиболее значимым примитивом любой истинно квантовой криптосистемы, используется не менее 20–30 базовых статистических тестов (NIST, U1) [12]. Проще говоря, уровень значимости наиболее традиционных доказательств квантовой безопасности составляет не более 1/20–1/30 (~5%) по отношению к передовым статистическим методам, которые в настоящее время применяются во всех высокотехнологичных областях. Поэтому разработку классификационных и сертификационных рангов для КК необходимо вести с учетом современных методов статистического анализа. На наш взгляд, среди них особое место занимает метод последовательности ранжированных амплитуд [13], позволяющий не только повысить точность и скорость [14] обработки данных для квантовых систем, но и увеличить достоверность анализа при небольших выборках (около 100–200 точек) [15]. Вышеизложенные идеи об истории теоретико-математической статики в квантовой информатике послужили отправной точкой для начала разработки новых прикладных методов для надежной классификации и диагностики сложных шумоподобных данных для базовых примитивов квантовых крипто-комплексов [16, 17].

ДИАГНОСТИКА МАГИСТРАЛЬНЫХ КВАНТОВЫХ СЕТЕЙ

Во время двухдневных полевых тестов магистральных КК в Казани [2] в августе 2019 г. был получен ряд значений QBER (взяты значения в пределах допустимого значения QBER меньше 4%), который даже при первом рассмотрении обладает трендовой структурой, отвечающей неслучайным факторам (температура, влажность и прочее). На рис. 1 показаны процентные фильтры уровней [25, 50, 75] при 50-точечном сглаживании для значений QBER, визуально показывающие наличие трендов в ошибках на протяжении двухдневных тестов. Детализацию неслучайности можно в дальнейшем выполнить в формате прогноза, опирающегося на простейшие линейные регрессии. Соответственно, для установления достоверности факта наличия регрессии можно использовать автокорреляционная функцию. На рис. 2 показана автокорреляционная функция для девиаций QBER относительно среднего значения в зависимости от дискретного индекса времени δm (привязан к единице из-

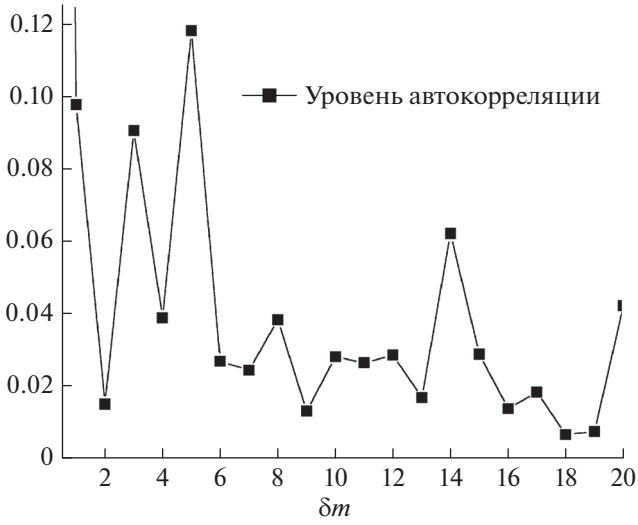

Рис. 2. Автокорреляционная функция для девиаций QBER относительно среднего значения в зависимости от дискретного индекса времени δm, показывает наличие избыточных корреляций во временном интервале [1, 5].

мерения: около 520 точек на 2 дня испытаний), что еще более явно показывает наличие избыточных локальных корреляций во временном интервале [1, 5]. Таким образом, показано, что в магистральных КК присутствуют шумовые факторы, которые можно предсказать. Это значит, что специализированная диагностическая система магистральных КК должна явно прогнозировать уровень шумов, что в свою очередь повысит достоверность определения уровня помех и уровня безопасности МКС.

НЕПАРАМЕТРИЧЕСКИЙ АНАЛИЗ ВРЕМЕННЫХ МЕТОК КЛЮЧЕЙ

Одним из малоизученных в контексте квантовой криптографии вопросов является вопрос о локальном мониторинге разницы временных меток битов внутри одного сырого ключа. Здесь мы предлагаем использовать альтернативную меру случайности для исходных данных для разницы временных меток $\{y_k\}$, основанную на ранговой статистике $\{x_{k,p} = \mathrm{sign}(y_k - p)\}$: аналог коэффициента автокорреляции $Qp = \log_{10}\left(\left\langle\left\{x_{k,p}x_{k+1,p}\right\}\right\rangle\right)$ с непрерывным индексом p, что дает p-параметрическое семейство по сравнению с обычными коэффициентами корреляции [18]. На рис. 3 показан коэффициент качества случайности Q_p для временных меток сырого ключа для альтернативного измерения уровня локальных корреляций. Отметим, что десятичный логарифм стандартного коэффициента автокорреляции Пирсона дает значение равное -1.06, существенно отличное по

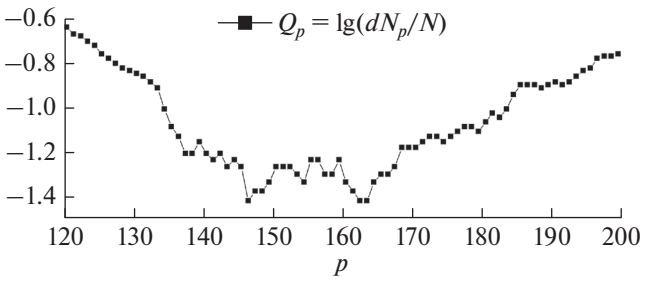

Рис. 3. Коэффициент качества случайности Q_p для временных меток сырого ключа для альтернативного измерения уровня локальных корреляций.

сравнению с $\min[p](Q_p) = -1.42$, что показывает дополнительные возможности новой методики.

Как на избыточности автокорреляции по Пирсону строится прогностическая регрессия, также и для альтернативной меры корреляций можно построить альтернативную прогностическую регрессию. При этом отличия в уровнях корреляции по Пирсону и по введенной корреляции Q_p фактически количественно показывают какая прогностическая модель будет лучше работать в данной конкретной ситуации. Таким образом, расширенные ранговые статистики при мониторинге квантовой случайности ключей в магистральных КК открывают новое возможности для прогнозирования шумов и сбоев в МКС.

ЗАКЛЮЧЕНИЕ

В работе рассмотрен вопрос о принципиальной применимости традиционных статистических доказательств для мониторинга дальнодействующих комплексов квантовой связи, работающих в предельных паспортных режимах в условиях высоких шумов. В полевых тестах показана неприменимость стандартных для квантовой информатики критериев для глубокой детальной прикладной оценки достоверности обнаружения шумов. Тем не менее для магистральных КК существует необходимость внедрения базовых классификационных и сертификационных критериев безопасности [9, 19]. Необходимо отметить значимость прогностических систем мониторинга в разрезе построения масштабной национальной квантовой сети, что основано на первом в России непрерывном тесте магистральных КК [2]. При этом диагностика ошибок в предельном паспортном режиме зависит от большого числа физических факторов, которые трудно отслеживать в рамках работы только одного конструкционно законченного изделия. Следовательно, нужна расширенная система визуальной диагностики, которая должна поставляться с комплексом КК и иметь возможность работать в фоновом режиме МКС для отслеживания всей истории изменений в работоспособности линии даже

при отключенном комплексе КК в узле. Такая квантово-классическая диагностическая подсеть в МКС, способная диагностировать даже малые шумы в сети в отсутствии априорной информации о типе помех, открывает перспективы коммерциализации квантово-классических облачных сервисов для робастной защиты информации. Отметим, что на данный момент поднятая в работе тема мониторинга КК является дискуссионной и более актуальна в таких приложениях как, например, эконометрический технический анализ временных рядов.

Коллектив авторов выражает особую благодарность профессору кафедры радиоэлектроники и информационно-измерительной техники КНИТУ-КАИ Р.Р. Нигматуллину за обсуждение темы непараметрических ранговых критериев в физике. Исследования шумов в области фотоники и квантовых технологий были поддержаны грантом Правительства Российской Федерации, проект № 14.Z50.31.0040 от 17.02.2017 (экспериментальная часть). Работа частично выполнена в рамках бюджетной темы лаборатории квантовой оптики и информатики КФТИ – ОСП ФИЦ КазНЦ РАН (численное моделирование).

СПИСОК ЛИТЕРАТУРЫ

1. *Втюрина А.Г., Елисеев В.Л., Жиляев А.Е. и др.* // Докл. ТУСУР. 2018. Т. 21. № 2. С. 15.
2. *Bannik O.I., Gilyazov L.R., Gleim A.V. et al.* // arXiv: 1910.10011. 2019.
3. *Merolla J.M., Mazurenko Y., Goedgebuer J.P., Rhodes W.T.* // Phys. Rev. Lett. 1999. V. 82. № 8. P. 1656.
4. *Минаев В.А., Королев И.Д., Кулиш О.А., Мазин А.В.* // Вопр. радиоэлектр. 2019. № 4. С. 90.
5. *Тимофеев А.М.* // Информатика. 2019. Т. 16. № 2. С. 90.
6. *Stucki D., Barreiro C., Fasel S. et al.* // Opt. Expr. 2009. V. 17. № 16. P. 13326.
7. *Kulik S.P., Molotkov S.N., Potapova T.A.* // JETP Lett. 2014. V. 98. № 10. P. 626.
8. *Grande I.H.L., Larotonda M.A.* // Quant. Inform. Process. 2018. V. 17. № 7. P. 176.
9. *Sajeed S., Chaiwongkhot P., Huang A. et al.* // arXiv: 1909.07898. 2019.
10. *Holevo A S.* // Probl. Pered. Inform. 1973. V. 9. № 3. P. 3.
11. *Колесниченко А.В.* // Препр. ИПМ РАН. 2018. № 104. С. 60.
12. *Rukhin A., Soto J., Nechvatal J. et al.* // NIST Spec. Publ. 2001. V. 800-22. P. 153.
13. *Nigmatullin R.R., Smith G.* // Phys. A. 2003. V. 320. P. 219.
14. *Smirnov M.A., Perminov N.S., Nigmatullin R.R. et al.* // Appl. Opt. 2018. V. 57. № 1. P. 57.
15. *Перминов Н.С., Смирнов М.А., Нигматуллин Р.Р. и др.* // Комп. опт. 2018. Т. 42. № 2. С. 338.
16. *Perminov N.S., Bannik O.I., Tarankova D.Y., Nigmatullin R.R.* // arXiv: 1810.04295. 2018.
17. *Nigmatullin R.R., Vorobev A.S.* // Fluct. Noise Lett. 2019. Art. № 1950023.
18. *Перминов Н.С., Банник О.И., Гилязов Л.Р. и др.* // Тр. VI Молод. Междун. науч.-техн. конф. “Прикладная электродинамика, фотоника и живые системы–2019” (Казань, 2019). С. 459.
19. *Drahi D., Walk N., Hoban M.J. et al.* // arXiv: 1905.09665. 2019.