17

Применение алгоритмов машинного обучения для демодуляции состояний в системах квантового распределения ключа с квадратурной модуляцией

© Б.Е. Первушин[1], А.В. Зиновьев[2], Д.Н. Кириченко[2], И.М. Филипов[2], Р.К. Гончаров[2], Э.О. Самсонов[2]

[1] ООО „Яндекс“,
Москва, Россия
[2] Университет ИТМО,
Санкт-Петербург, Россия

e-mail: avzinovev15@yandex.ru

Поступила в редакцию 28.04.2025 г.
В окончательной редакции 27.06.2025 г.
Принята к публикации 28.06.2025 г.

Применение алгоритмов машинного обучения для демодуляции состояний в системе квантового распределения ключей на непрерывных переменных (CV-QKD) с использованием квадратурной амплитудной модуляции (QAM) с 16 состояниями. При использовании алгоритмов классификации средний коэффициент ошибок по битам (BER) составил 0.019, а для алгоритмов кластеризации — 0.022, что в 1.75 и 1.5 раза меньше, чем при применении классического метода демодуляции с использованием логарифмического отношения правдоподобия (LLR).

Ключевые слова: квантовое распределение ключа, машинное обучение.

DOI: 10.61011/OS.2025.07.61109.7725-25

1. Введение

Квантовое распределение ключей (QKD) используется для распределения ключа между двумя удаленными пользователями с целью его применения в симметричном шифровании данных. Оно основано на трех принципах квантовой механики: принципе неопределенности Гейзенберга, теореме о запрете клонирования и квантовой запутанности. Все эти три принципа обеспечивают теоретически устойчивое шифрование даже при появлении достаточно мощного квантового компьютера.

В то же время алгоритмы машинного обучения (ML) все активнее разрабатываются и уже находят применение в неограниченном количестве областей науки и техники, включая область QKD.

Квантовые коммуникации делятся на две крупные парадигмы: с дискретными переменными (DV) и с непрерывными переменными (CV). CV-протоколы подразделяются на протоколы с дискретной модуляцией [1] и гауссовской модуляцией [2] по методу модуляции оптического сигнала. DV-протоколы — это протоколы, удовлетворяющие одному или нескольким из следующих условий: используются детекторы одиночных фотонов, применяется парадигма одиночных фотонов, квантовая вероятность ошибки по битам (QBER) оценивается как основной параметр.

DV-QKD-протоколы принципиально отличаются от протоколов на CV с дискретной модуляцией. В первых измеряемая физическая величина сама по себе может принимать только дискретный набор значений из-за того, что регистрируются одиночные фотоны. С другой стороны, для протоколов на CV с дискретной модуляцией типично, что дискретный набор значений используется для кодирования квадратур поля, которые в принципе могут принимать непрерывный набор значений.

Базовые протоколы CV-QKD с дискретной модуляцией используют методы фазовой манипуляции (PSK) и квадратурно-амплитудной манипуляции (QAM). В то же время CV-QKD-протоколы с гауссовской модуляцией реализуют такую модуляцию оптического сигнала, при которой обе квадратуры статистически распределены по оптическим посылкам в соответствии с гауссовым распределением с нулевым средним значением.

В данной работе для тестирования был выбран CV-протокол с дискретной модуляцией, поскольку для него, как и для гауссовской модуляции, доказана безопасность [3], а также показано, что для протокола с дискретной модуляцией может быть достигнута более высокая скорость генерации секретного ключа [4].

В настоящее время ведутся исследования и разработки алгоритмов машинного обучения и нейронных сетей для применения в области квантового распределения ключей. Существует несколько сценариев их использования в области QKD.

1. Оптимизация параметров и калибровка системы. В любой QKD-системе существуют два набора параметров: неизменяемые и задаваемые пользователем. Неизменяемые параметры — это такие параметры, как потери в оптическом канале, эффективность детектирования и другие параметры, определяемые характеристиками оборудования или особенностями канала. Пользовательские параметры являются изменяемыми и

оптимизируются для достижения максимальной скорости безопасной генерации ключа [5–12].

2. Классификация и кластеризация состояний. В 2019 г. группа из Центрального Южного университета Чанша опубликовала работу [13] по использованию классического метода машинного обучения — DBSCAN — для быстрого определения формата модуляции в CV-QKD-протоколе. В следующем году их коллеги из того же университета реализовали многометрический алгоритм классификации с использованием классического алгоритма K-ближайших соседей для CV-QKD-протокола с дискретной модуляцией [14].

3. Расчет скорости генерации секретного ключа. Научная группа из Нанкинского университета (Китай) опубликовала в 2021 и 2022 гг. результаты своих работ [15–17] по использованию нейронной сети для быстрого расчета скорости безопасной генерации ключа в CV-QKD-протоколе.

4. Распознавание фазы состояний и калибровка. Использование небольшой модели машинного обучения для определения фазового состояния было продемонстрировано в работе [18] испанских ученых в 2021 г. Разработанный алгоритм на основе модели глубокой нейронной сети осуществлял фазовую компенсацию в фазово-кодирующем протоколе. В 2020 г. научная группа из города Нанкин исследовала стабилизацию фазовой модуляции с использованием алгоритма LSTM на основе фазово-кодирующего протокола BB84 [19].

В настоящей статье описан эксперимент по реализации системы квантового распределения ключей с квадратурно-амплитудной модуляцией. Для демодуляции полученных данных использовались алгоритмы машинного обучения: классификации и кластеризации. Результаты демодуляции сравнивались с классическим методом с использованием логарифма отношения правдоподобия.

2. Сбор экспериментальных данных

В связи с необходимостью апробации алгоритмов на экспериментальных данных была собрана оптическая схема. Она представляет собой интерферометр Маха-Цендера с сигнальными импульсами в одном плече и локальным осциллятором в другом. Отличие реализованной схемы от классической схемы системы квантового распределения ключей состоит в отсутствии мультиплексирования сигналов во времени и по поляризации, а также в отсутствии передачи состояний по каналу, так как это излишне усложнило бы экспериментальную реализацию.

В схеме, изображенной на рис. 1, излучение генерируется одномодовым лазером. Для защиты лазера от обратного излучения используется оптический изолятор. После оптического изолятора сигнал попадает на первый амплитудный модулятор, который создает

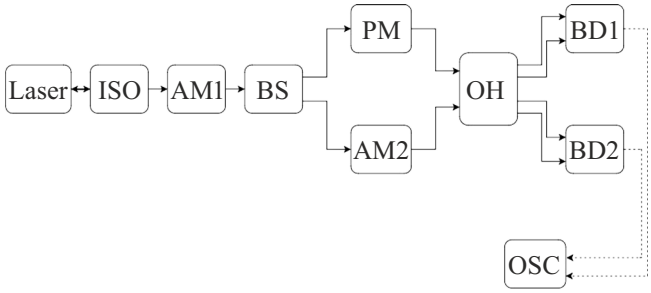

Рис. 1. Экспериментальная схема реализации CV-QKD-протокола с дискретной квадратурной модуляцией. ISO — изолятор; AM1, AM2 — амплитудные модуляторы; BS — светоделитель; PM — фазовый модулятор; OH — оптический гибрид; BD1, BD2 — балансные детекторы; OSC — осциллограф.

импульсный режим. Далее излучение разделяется на светоделителе. Половина излучения идет в плечо интерферометра с амплитудным модулятором и используется как сигнальное излучение. Излучение в другом плече является фазово-модулированным и используется в качестве локального осциллятора. Стоит отметить, почему фазовый модулятор и амплитудный модулятор расположены в разных плечах интерферометра. В подавляющем большинстве работ фаза и амплитуда модулируются именно для сигнального состояния, а в плече локального осциллятора используется дополнительный оптический путь для компенсации времени задержки, возникающего из-за наличия дополнительных амплитудного и фазового модуляторов в сигнальном плече. В данной работе для упрощения схемы фазовый и амплитудный модуляторы были разнесены по двум плечам, благодаря чему отпала необходимость в балансировке плеч интерферометра. При этом фаза локального осциллятора модулируется относительно фаэы сигнала, что можно учесть заменой фазы на равную, но обратную по знаку.

Оптический гибрид используется для выполнения двойного гомодинного детектирования. С помощью двух балансных детекторов реализуется одновременное детектирование двух квадратур сигнала. Выходные сигналы с балансных детекторов пропорциональны двум квадратурам сигнального состояния. Оптический гибрид разделяет сигнал и локальный осциллятор, причем локальный осциллятор в двух плечах сдвинут по фазе на 90 градусов, что позволяет измерять две квадратуры сигнала. Использование двойного гомодинного детектирования дает возможность определить положение каждого импульса на фазовой плоскости. Сигналы с балансных детекторов поступают на осциллограф, где сохраняются. Дальнейшая обработка происходит на компьютере. Мощность лазерного источника составляла 0 dBm на длине волны 1550 nm. На радиочастотный вход первого амплитудного модулятора подается импульсный сигнал с периодом 0.5 μs и скважностью 0.5. Период был выбран исходя из того, что даже незначительный дисбаланс плеч

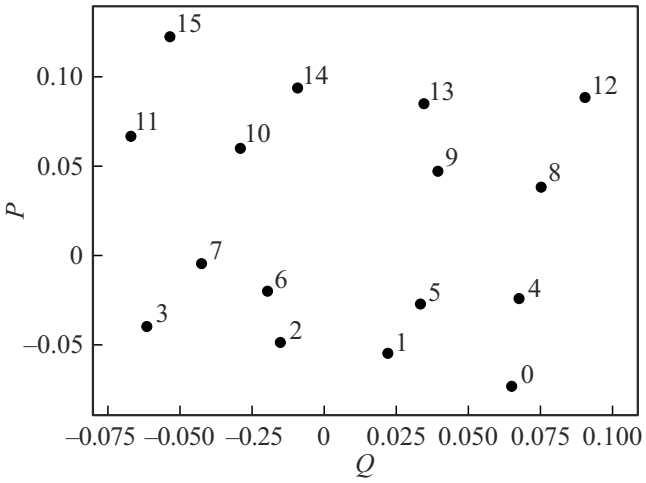

Рис. 2. Центры созвездия экспериментальных сигналов. Каждая точка соответствует центру распределения соответствующего состояния в квадратурной модуляции с 16 состояниями.

может сильно влиять на интерференцию на оптическом гибриде, а также для получения достаточной статистики при сохранении на осциллографе. На фазовый модулятор и второй амплитудный модулятор подавались периодические сигналы, определяемые 16 состояниями квадратурной модуляции и одним опорным импульсом. Опорный импульс характеризовался нулевой фазой и максимальным пропусканием на втором амплитудном модуляторе. Такие сигналы подаются на второй амплитудный и фазовый модуляторы таким образом, чтобы на выходе двух балансных детекторов распределения состояний были максимально близкими к идеальному созвездию.

Как упоминалось ранее, нестабильность плеч характерна для волоконно-оптических интерферометров, что приводит к нестабильности относительной фазы локального осциллятора и сигнальных импульсов. Реализованная схема не является исключением, поэтому для компенсации фазового дрейфа использовался метод компенсации фазы с использованием двух опорных импульсов, описанный в статье [20].

В результате эксперимента были собраны данные, представленные на рис. 2 и 3. Для каждого класса зарегистрировано по $1.5 \cdot 10^4$ состояний. На первом рисунке показаны центры всех состояний на одном графике для сравнения их взаимного расположения, на втором — распределения для каждого состояния на отдельных графиках для более наглядного рассмотрения.

Можно увидеть, что экспериментально полученные центры распределения повторяют картину идеального созвездия [13]. Однако в этом исходном виде облака состояний пересекаются. Для уменьшения пересечения была проведена постобработка, в которой вычислялся корень из значений квадратур сигналов. Для полученных данных были использованы методы машинного обучения для демодуляции состояний.

3. Реализация алгоритмов

Для сравнения с классическим алгоритмом демодуляции LLR (а также в силу того, что рассматривается система QKD) в качестве метрики качества алгоритмов предпочтительно рассматривать коэффициент битовых ошибок. Для этого каждому состоянию была сопоставлена 4-битовая строка. Использовалось кодирование, при котором два соседних состояния отличаются на единицу в расстоянии Хэмминга, т.е. соответствующие битовые строки различаются только в одной позиции. Такое кодирование используется для уменьшения битовых ошибок при демодуляции.

Метод LLR основан на использовании условных вероятностей того, что при детектировании сигнала с определенными значениями квадратур k-й бит в его битовом представлении будет равен 0 или 1:

$$\mathrm{LLR}(k) \simeq \ln\left[\frac{\exp\left(-\left(|r - c^*(k,0)|^2/2\delta^2\right)\right)}{\exp\left(-\left(|r - c^*(k,1)|^2/2\delta^2\right)\right)}\right]$$

$$= \frac{1}{2\delta^2}\left(|r - c^*(k,1)|^2 - |r - c^*(k,0)|^2\right), \quad (1)$$

где r — измеренный вектор; $c^*(k,1), c^*(k,0)$ — ближайшее состояние, в битовом представлении которого бит на k-м месте равен 1 или 0 соответственно; δ^2 - дисперсия шума в канале. Знак LLR для каждого бита определяет его значение. Описанный алгоритм использования логарифмического отношения правдоподобия на экспериментальных данных дает коэффициент битовых ошибок 0.033.

Для исследования применимости алгоритмов машинного обучения для демодуляции состояний в системе с квадратурной модуляцией были выбраны алгоритмы классификации: метод ближайшего соседа, метод опорных векторов и дерево решений. В качестве метода кластеризации был выбран алгоритм k-средних. Также рассматривались алгоритмы DBSCAN и Agglomerative Clustering. DBSCAN не требует задания начального количества кластеров, что может быть использовано при разработке протокола и повышении его безопасности, но может оказаться неприменим в случае низкого отношения сигнал-шум. В этом случае все кластеры расположены слишком плотно, поэтому выделить отдельные кластеры этим алгоритмом становится невозможно. Agglomerative Clustering, в свою очередь, слишком медлителен и не может быть применен для больших объемов данных и при работе в реальном времени.

Для применения методов классификации в соответствии с методологией машинного обучения общий набор данных был разделен на обучающую и тестовую выборки в соотношении 60 к 40%. Алгоритмы классификации обучались на обучающей выборке, а на тестовой выборке производилось разделение состояний и определение итоговой точности алгоритмов. В качестве метрики оценки использовалась точность классификации, т.е.

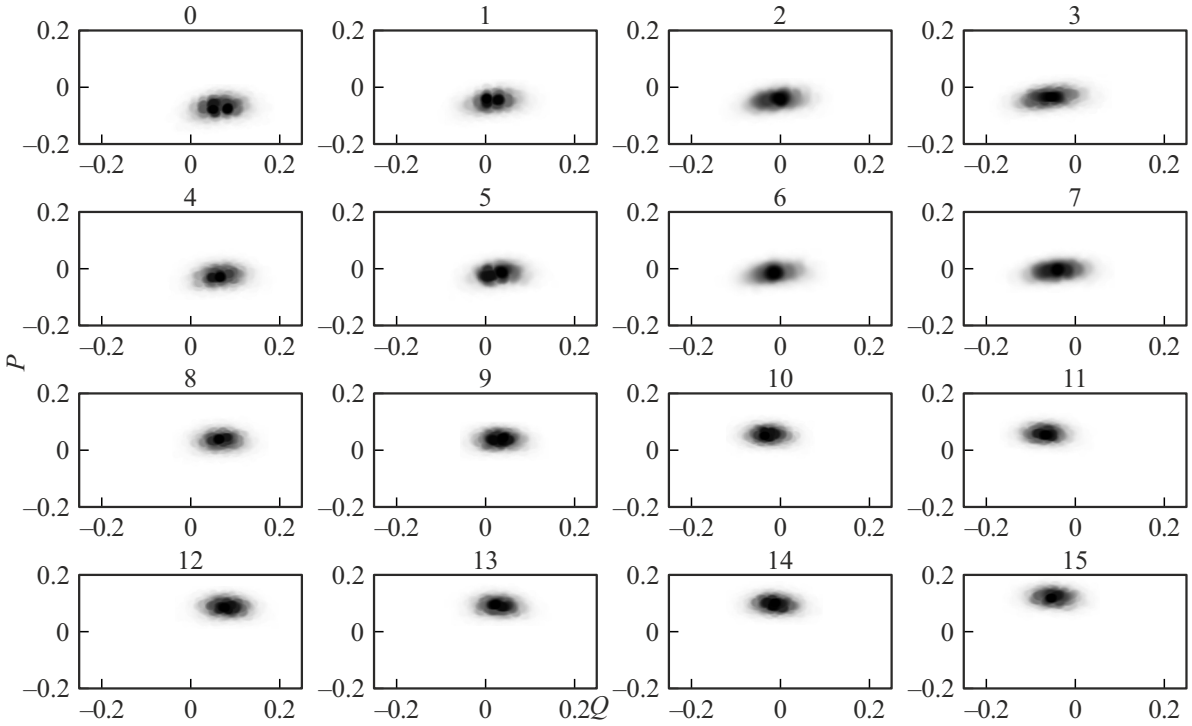

Рис. 3. Экспериментально полученные состояния на фазовой плоскости. По осям показаны электрические сигналы с балансных детекторов, пропорциональные соответствующим квадратурам сигнала.

отношение правильно классифицированных объектов к их общему количеству.

При обучении алгоритмов производилась оптимизация соответствующих гиперпараметров. Для оптимизации гиперпараметров использовался принцип кроссвалидации с 5 блоками. График применения алгоритмов классификации представлен на рис. 4.

Для алгоритма k-means использовались центры идеального созвездия в масштабе, аналогичном экспериментальным данным.

Результаты применения алгоритмов для демодуляции состояний

Алгоритм	Точность	BER	Время предсказания, s
LLR	–	0.033	0.393
Метод k-ближайших соседей	0.965	0.019	0.942
Нелинейный SVM	0.965	0.019	42.11
SVM с гауссовым ядром	0.966	0.019	71.74
Дерево решений	0.951	0.02	0.013
k-means	0.933	0.022	0.161

4. Сравнение и анализ коэффициента ошибок по битам

Для сравнения алгоритмов измерялось время прогнозирования тестовой выборки. Результаты по точности алгоритмов, коэффициенту ошибок по битам (BER) и времени тестирования приведены в таблице.

Из полученных результатов видно, что при использовании алгоритмов машинного обучения коэффициент ошибок по битам уменьшается в 1.74 раза для классификационных алгоритмов и в 1.5 раза для алгоритма k-средних, что указывает на хороший потенциал алгоритмов машинного обучения в качестве алгоритмов демодуляции сигналов. Метод опорных векторов (SVM) характеризуется большим временем предсказания, однако в некоторых конфигурациях систем даже небольшой выигрыш в коэффициенте ошибок по битам может быть приоритетным по сравнению с временем работы алгоритма.

Результаты показывают, что с помощью различных алгоритмов машинного обучения можно выбрать наиболее подходящий алгоритм для конкретного протокола и системы QKD. Более того, некоторые алгоритмы также позволяют улучшить постобработку последовательности. Например, используя метод опорных векторов, можно перейти к каналам со стиранием, т. е. отбрасывать объекты, в которых алгоритм не уверен в правильности классификации.

5. Заключение

В работе показано применение алгоритмов машинного обучения для демодуляции состояний в CV-QKD-

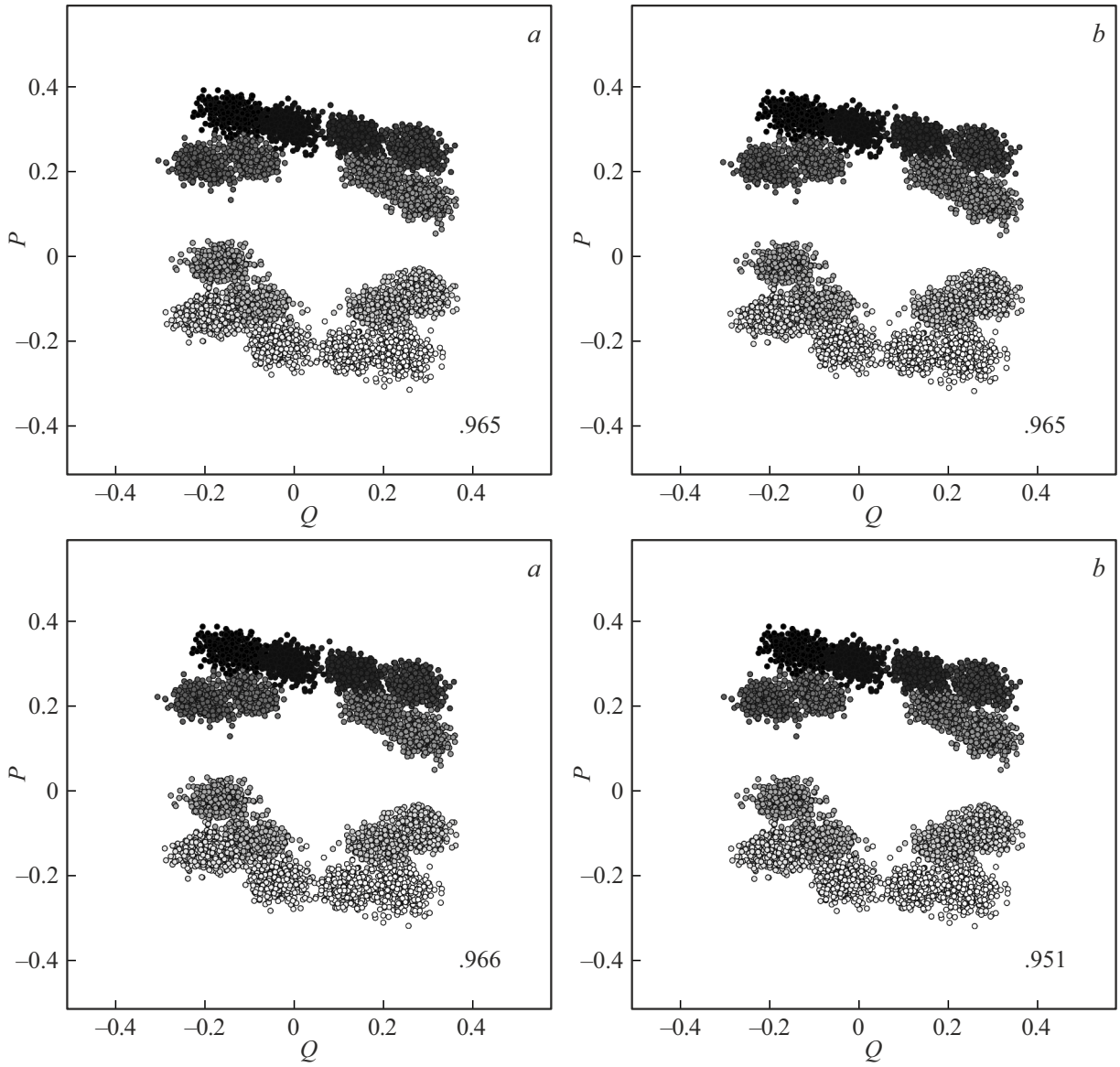

Рис. 4. Графическое представление результатов использования алгоритмов классификации для демодуляции состояний: *a* — метод *k*-ближайших оседей, *b* — нелинейный метод опорных векторов (нелинейный SVM), *c* — метод опорных векторов (SVM) с гауссовым ядром, *d* — дерево решений. На графиках указана точность работы алгоритмов.

системе с квадратурной модуляцией с 16 состояниями. При использовании классификационных алгоритмов BER в среднем составил 0.019, а при кластеризации — 0.022, что в 1.75 и 1.5 раза меньше, чем при использовании классического метода демодуляции с использованием LLR. Дальнейшая работа будет направлена на реализацию полной системы квантового распределения ключей с квадратурно-амплитудной модуляцией, а также на исследование и применение ансамблевых методов и нейронных сетей для демодуляции состояний.

Финансирование работы

Исследование выполнено при поддержке Российского научного фонда (проект № 24-11-00398).

Конфликт интересов

Авторы заявляют, что у них нет конфликта интересов.

Список литературы

[1] T. Hirano, T. Ichikawa, T. Matsubara, M. Ono, Y. Oguri, R. Namiki, K. Kasai, R. Matsumoto, T. Tsurumaru. Quantum Science and Technology, **2** (2), 024010 (2017).
[2] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, H. Hübel. Advanced Quantum Technologies, **1** (1), 1800011 (2018).
[3] C. Lupo Y. Ouyang. PRX Quantum, **3** (1), 010341 (2022).
[4] I.B. Djordjevic. IEEE Photonics Journal, **11** (4), 1–10 (2019).

[5] W. Wang H.-K. Lo. Physical Review A, **100** (6), 062334 (2019).
[6] F.-Y. Lu, Z.-Q. Yin, C. Wang, C.-H. Cui, J. Teng, S. Wang, W. Chen, W. Huang, B.-J. Xu, G.-C. Guo. JOSA B, **36** (3), B92–B98 (2019).
[7] H.-J. Ding, J.-Y. Liu, C.-M. Zhang, Q. Wang. Quantum Information Processing, **19**, 1–8 (2020).
[8] Y. Yi, Y. Rao, C. Huang, S. Zeng, Y. Yang, Q. He, X. Chen. IEEE 2021 4th International Conference on Pattern Recognition and Artificial Intelligence (PRAI), 164–168 (2021).
[9] Y. Ou, E. Hugues-Salas, F. Ntavou, R. Wang, Y. Bi, S. Yan, G. Kanellos, R. Nejabati, D. Simeonidou. IEEE 2018 European Conference on Optical Communication (ECOC), 1–3 (2018).
[10] Z.-A. Ren, Y.-P. Chen, J.-Y. Liu, H.-J. Ding, Q. Wang. IEEE Communications Letters, **25** (3), 940–944 (2020).
[11] W. Liu, P. Huang, J. Peng, J. Fan, G. Zeng. Physical Review A, **97** (2), 022316 (2018).
[12] D. Jin, Y. Guo, Y. Wang, Y. Li, D. Huang. Physical Review A, **104** (1), 012616 (2021).
[13] H. Zhang, P. Liu, Y. Guo, L. Zhang, D. Huang. JOSA B, **36** (3), B51–B58 (2019).
[14] Q. Liao, G. Xiao, H. Zhong, Y. Guo. New Journal of Physics, **22** (8), 083086 (2020).
[15] M.-G. Zhou, Z.-P. Liu, W.-B. Liu, C.-L. Li, J.-L. Bai, Y.-R. Xue, Y. Fu, H.-L. Yin, Z.-B. Chen. (2021). arXiv:2108.02578.2108.02578.
[16] Z.-P. Liu, M.-G. Zhou, W.-B. Liu, C.-L. Li, J. Gu, H.-L. Yin, Z.-B. Chen. Optics Express, **30** (9), 15024–15036 (2022).
[17] M.-G. Zhou, Z.-P. Liu, W.-B. Liu, C.-L. Li, J.-L. Bai, Y.-R. Xue, Y. Fu, H.-L. Yin, Z.-B. Chen. Scientific Reports, **12** (1), 8879 (2022).
[18] M. Ahmadian, M. Ruiz, J. Comellas, L. Velasco. Journal of Lightwave Technology, **40** (13), 4119–4128 (2022).
[19] J.-Y. Liu, H.-J. Ding, C.-M. Zhang, S.-P. Xie, Q. Wang. Phys. Rev. Appl., **12** (1), 014059 (2019).
[20] F.M. Goncharov, B.E. Pervushin, B.A. Nasedkin, R.K. Goncharov, D.A. Yashin, M.E. Gellert, D.V. Sulimov, P.A. Morozova, I.M. Filipov, I.A. Adam. Nanosystems: Physics, Chemistry, Mathematics, **14** (1), 59–68 (2023).