

A MACHINE-LEARNING APPROACH TO QUANTUM STATE ESTIMATION

R. Nigmatullin^{1,*}, *N. Borisov*^{2,3}, *B. Meretukova*^{2,3},
*D. Kagramanyan*¹, *A. Tayduganov*^{2,3}, *A. Ryzhikov*¹,
*D. Derkach*¹

¹Laboratory of Methods for Big Data Analysis, HSE University, Moscow, Russia

²Laboratory of Quantum Information Technologies, National University of Science
and Technology MISIS, Moscow, Russia

³QRate, Skolkovo, Moscow, Russia

Quantum Key Distribution (QKD) systems represent a cornerstone of secure quantum communication, relying on post-processing procedures to generate shared keys. Among these, error correction (EC) is a critical and computationally demanding step, where the estimation of the Quantum Bit Error Rate (QBER) plays a pivotal role in optimizing code rates for LDPC-based protocols. Traditional QBER estimation methods, grounded in physical models and statistics, often struggle with real-world variability and outliers, leading to suboptimal performance.

In this study, we propose a novel machine learning framework for QBER forecasting, reframing the problem as a time-series prediction task. Leveraging real-world data from quantum transmitters, we evaluated a suite of models, including gradient boosting with autoregressive components, exponential smoothing hybrids, and deep neural networks, to predict QBER with greater precision. Through extensive experiments, our approach demonstrates significant improvements in error correction efficiency compared to traditional methods, particularly under challenging conditions like system calibration drifts and non-stationary signal behavior.

The results highlight the potential of lightweight and interpretable machine learning models, such as gradient-boosted exponential smoothing, to outperform complex neural architectures in real-world scenarios. This research contributes to the advancement of quantum cryptography by enabling faster and more robust key generation, with reduced information disclosure during reconciliation. Our findings open new avenues for integrating machine learning into QKD systems for adaptive and scalable quantum communication.

Системы квантового распределения ключей (QKD) представляют собой краеугольный камень безопасной квантовой коммуникации, они во многом полагаются на процедуры постобработки для генерации ключей. В этих процедурах исправление ошибок (ЕС) является критично важным и вычислительно затратным этапом, где оценка квантового уровня ошибки (QBER) играет ключевую роль в оптимизации скорости передачи кода для протоколов на базе LDPC. Традиционные методы оценки QBER, основанные на физических моделях и статистике,

* E-mail: roman.nigmatullinm@gmail.com

часто сталкиваются с изменчивостью экспериментальных условий и выбросами в данных, что приводит к неоптимальной производительности.

В этом исследовании предлагается новый метод на основе машинного обучения для прогнозирования QBER и переформулируется проблема как задача прогнозирования временных рядов. С использованием реальных данных от квантовых передатчиков рассмотрены и оценены качество множества алгоритмов, включая градиентный бустинг с авторегрессионными компонентами, экспоненциальное сглаживание и глубокие нейронные сети, для прогнозирования QBER с большей точностью. Благодаря обширным экспериментам авторский подход демонстрирует значительное повышение эффективности коррекции ошибок по сравнению с традиционными методами, особенно в сложных условиях, таких как раскалировка системы и нестационарный характер уровня ошибки.

Полученные результаты подчеркивают потенциал вычислительно легких классических алгоритмов машинного обучения, таких как экспоненциальное сглаживание с градиентным бустингом, которые превосходят сложные нейросети в реальных экспериментах. Это исследование способствует развитию квантовой криптографии, обеспечивая более быструю и надежную генерацию ключей при меньшем раскрытии информации во время сверки. Открываются новые возможности для интеграции машинного обучения в системы QKD для адаптивной и масштабируемой квантовой коммуникации.

PACS: 44.25.+f; 44.90.+c