

ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ ДЛЯ ОПТИМІЗАЦІЇ КВАНТОВИХ КАНАЛІВ ЗВ'ЯЗКУ У КВАНТОВІЙ КРИПТОГРАФІЇ

Зінченко В. Л.;¹ Лифар В. О., д.т.н, доц.²

¹ Інститут телекомунікацій і глобального інформаційного простору НАН України;

² Східноукраїнський національний університет ім. В. Даля

^{1,2} Україна, Київ

¹ v.l.zinchenko@hotmail.com; ² lyfarva61@gmail.com

Анотація. У роботі досліджено можливості використання нейронних мереж для корекції помилок у квантових каналах зв'язку в системах квантової криптографії. Отримані результати демонструють зниження кількості помилок на 25% порівняно з традиційними методами, що підвищує надійність передачі даних. Запропонований підхід має перспективи практичного застосування в реальних квантових системах.

Ключові слова: квантовий канал зв'язку; згорткова мережа; протокол BB84.

Вступна частина. Сучасні виклики інформаційної безпеки вимагають нових технологій захисту даних, і однією з найбільш перспективних є квантова криптографія. Вона базується на законах квантової фізики, забезпечуючи високий рівень безпеки шляхом використання фотонів для передачі інформації через квантовий канал зв'язку. Однак, квантовий канал схильний до шуму, фазових спотворень та втрат інформації, що може знижувати ефективність передачі даних.

На сьогоднішній день існують численні методи корекції помилок у квантових каналах, проте вони мають певні обмеження. Наприклад, традиційні методи квантової корекції помилок (Error Correction Codes) можуть вимагати значних обчислювальних ресурсів і не завжди забезпечують достатньо швидку реакцію на зміни умов у каналі зв'язку. Це створює необхідність у пошуку нових підходів для покращення роботи квантових каналів зв'язку, зокрема з використанням методів штучного інтелекту [1].

Актуальність теми зумовлена тим, що нейронні мережі здатні автоматично адаптуватися до мінливих умов у квантових системах, що може значно підвищити надійність і швидкість передачі даних. Останні дослідження показують, що застосування методів глибокого навчання у квантових системах дає змогу зменшити вплив завад і спотворень на сигнал. Однак, питання оптимізації структури нейронних мереж для роботи з квантовими каналами залишається недостатньо дослідженим [2-3].

Мета роботи. Дослідження можливостей нейронних мереж для підвищення якості квантових каналів зв'язку у системах квантової криптографії шляхом оптимізації структури нейронної мережі та її навчання на основі даних з квантових каналів.

Основна частина. У ході дослідження було проведено моделювання квантового каналу зв'язку з використанням методів квантової криптографії на основі протоколу BB84. Було створено модель шумового каналу, де випадкові фазові спотворення та втрати сигналу викликали зниження ефективності передачі інформації. Для вирішення цієї проблеми було розроблено та навчено нейронну мережу на основі архітектури згорткової нейронної мережі (CNN), яка дозволяє швидко обробляти великі обсяги даних та ефективно коригувати помилки.

Модель нейронної мережі була навчена на симуляційних даних, отриманих з квантового каналу зв'язку, де змінювались умови передачі. Нейронна мережа отримувала на вхід дані про

стан каналу та передбачала найбільш ймовірні корекції помилок. Після навчання модель показала здатність адаптуватися до нових умов і суттєво знижувати рівень помилок. Основною перевагою запропонованої моделі є її швидкість адаптації та висока точність корекції, що дозволяє використовувати її у реальних квантових системах.

Результати дослідження показали, що використання нейронних мереж дозволяє зменшити кількість помилок при передачі даних через квантовий канал на 25% порівняно з традиційними методами корекції помилок. Крім того, час обробки даних був значно зменшений, що робить цей підхід перспективним для використання у реальних системах квантової криптографії.

Висновки. Застосування нейронних мереж для корекції помилок у квантових каналах зв'язку дозволяє значно підвищити надійність квантової криптографії. Розроблена модель нейронної мережі продемонструвала високу ефективність у боротьбі з фазовими спотвореннями та завадами, що робить її перспективним рішенням для практичного використання. У подальших дослідженнях планується адаптувати нейронну мережу до реальних умов експлуатації квантових систем та удосконалити її архітектуру для ще кращої роботи в умовах високих шумів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- [1] Ahn, C., Wiseman, H. M., & Milburn, G. J. (2003). Quantum error correction for continuously detected errors. *Physical Review A*, 67(5). <https://doi.org/10.1103/physreva.67.052310>.
- [2] Sivak, V. V., Eickbusch, A., Royer, B., Singh, S., Tsioutsios, I., Ganjam, S., Miano, A., Brock, B. L., Ding, A. Z., Frunzio, L., Girvin, S. M., Schoelkopf, R. J., & Devoret, M. H. (2023). Real-time quantum error correction beyond break-even. *Nature*. <https://doi.org/10.1038/s41586-023-05782-6>.
- [3] Coutts, B., Girard, M., & Watrous, J. (2021). Certifying optimality for convex quantum channel optimization problems. *Quantum*, 5, 448. <https://doi.org/10.22331/q-2021-05-01-448>.

Volodymyr Zinchenko, Volodymyr Lifar

Using Neural Networks for Optimizing Quantum Communication Channels in Quantum Cryptography

Abstract. *This study explores the use of neural networks for error correction in quantum communication channels within quantum cryptography systems. The results demonstrate a 25% reduction in errors compared to traditional methods, enhancing the reliability of data transmission. The proposed approach has practical application potential in real quantum systems.*

Keywords: *Quantum communication channel; convolutional network; BB84 protocol.*