

КРИПТОПЕРЕТВОРЕННЯ НА ОСНОВІ ОПЕРАТОРА АДАМАРА В КВАНТОВИХ МЕРЕЖАХ

Артем Харченко

CRYPTOGRAPHIC TRANSFORMATIONS BASED ON THE HADAMARD OPERATOR IN QUANTUM NETWORKS

Artem Kharchenko

*Харківський національний університет радіоелектроніки, пр. Науки, 14, м. Харків,
61166, Україна*

Abstract. *The paper presents a model for message encryption in quantum networks using the Hadamard operator. The use of this operator is considered as a fundamental tool for implementing superposition in the process of transforming classical bits into quantum states. An encryption protocol is proposed that can serve as a basis for secure message exchange between users in a quantum network.*

Розвиток квантових технологій відкриває нові можливості для побудови захищених каналів зв'язку. Одним із найбільш універсальних операторів у квантовій обробці інформації є оператор Адамара, який дозволяє перетворювати базові стани кубітів у їхні суперпозиції. Цей механізм є основою багатьох криптографічних протоколів. У даній роботі наведено модель шифрування, яка базується на застосуванні оператора Адамара як елемента криптографічного перетворення. Таким чином ми можемо перетворити класичне повідомлення у квантову форму та забезпечити високий рівень захисту під час передачі даних у квантовій мережі.

Запропонована схема шифрування базується на попередньо узгодженому класичному ключі, що генерується випадковим чином. Кожен біт повідомлення передається у вигляді квантового стану, причому застосування або незастосування оператора Адамара залежить від значення відповідного біта ключа.

Однією з головних переваг даного методу є його простота та ефективність. Він може бути реалізований на базових квантових схемах з одним кубітом. Крім того, використання суперпозицій під час шифрування забезпечує стійкість до прослуховування. Якщо зломисник намагається перехопити квантовий сигнал без знання ключа, він не зможе точно визначити, у якому базисі знаходиться кубіт. У результаті вимірювання призводить до втрати інформації або внесення помилок. Це дозволяє сторонам виявити факт прослуховування при порівнянні частини отриманих даних.

Бібліографія

1. Azuma, K., Economou, S. E., Elkouss, D., Hilaire, P., Jiang, L., Lo, H. K., & Tzitrin, I. (2023). Quantum repeaters: From quantum networks to the quantum internet. *Reviews of Modern Physics*, 95(4), 045006.
2. Gehér, G. P., McLauchlan, C., Campbell, E. T., Moylett, A. E., & Crawford, O. (2024). Error-corrected Hadamard gate simulated at the circuit level. *Quantum*, 8, 1394.
3. Renner, M. J., & Brukner, Č. (2022). Computational advantage from a quantum superposition of qubit gate orders. *Physical Review Letters*, 128(23), 230503.