УДК 004.27:004.056

ПОВЫШЕНИЕ КРИПТОСТОЙКОСТИ ПРОТОКОЛА КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА ДЛЯ МИНИМИЗАЦИИ ВОЗМОЖНОСТИ ПЕРЕХВАТА ДАННЫХ

Ляшенко К.А. (Донской государственный технический университет, г. Ростов-на-Дону)

Научный руководитель Черкесова Лариса Владимировна –
д.ф.-м.н., профессор кафедры «Кибербезопасность информационных систем»
(Донской государственный технический университет, г. Ростов-на-Дону)

Введение. Доклад посвящен проблемам в области квантовой криптографии, а именно, к её конкретному разделу, касающемуся разработке квантовых криптографических протоколов, над созданием которых учёные различных стран работают уже почти сорок лет. Данная технология способна сформировать новый уникальный облик телекоммуникационных сетей связи будущего. Однако, при этом никто с полной уверенностью не может гарантированно спрогнозировать, как будет выглядеть полностью сформированная инфраструктура квантового интернета, и к какому итогу она может привести. Автор выдвигает новую гипотезу относительно возможности универсального усовершенствования квантовых протоколов распределения ключа на примере модификации классического квантового протокола BB84.

Основная часть. Известно, что принцип неидеального копирования фотонов уже давно экспериментально применяется в каналах связи [1–6], что позволяет передавать информацию на значительно большие расстояния. Однако для квантового распределения ключей существуют иные требования по качеству исполнения отдельных компонентов. Автор ставит перед собой задачу исследования квантовой оптической памяти на основе фотонов и псевдо–фотонов, на предмет возможности сохранения в них информации. Основываясь на полученных данных, можно выявить теоретические ограничения, а также найти способы их нивелирования и нейтрализации, как для фотонов, так и для их воссозданных копий на основе псевдо–фотонов.
Использование выдвинутой автором идеи основано на теории рукотворного воссоздания фотонов и их дальнейшего использования в процессе передачи данных, что позволяет в значительной мере снизить возможность осуществления потенциальных угроз, а также избежать ситуаций, связанных с уязвимостями квантовых протоколов. Предлагаемый метод является комбинированным. Применение ложных состояний фотонов и создание множество ловушек для злоумышленников позволяет добиться такого увеличения ресурсов, затрачиваемых хакером на атаку, что это в итоге сделает её невыгодным занятием. Смоделированные копии фотонов, помимо своей основной задачи, становятся приманкой для хакера, способной загнать его в ловушку, подтверждая его присутствие в канале связи. При этом процесс обрыва канала связи перестанет быть неизбежным, что позволит избежать прерывания функционирования линии связи.

Выводы. Предлагаемая автором модификация, на примере классического квантового протокола BB84, вполне могла бы применяться для квантового распределения ключей, поскольку применяемый принцип неидеального копирования не нарушает законов физики, и при этом позволяет значительно повысить криптостойкость конкретного квантового протокола. Работоспособность предлагаемой модификации требует доказательств с помощью серии практических экспериментов с использованием специфического квантового оборудования.

Список использованных источников:

1. Nang Paing, S.; Setiawan, J.W.; Tariq, S.; Talha Rahim, M.; Lee, K.; Shin, H. Counterfactual Anonymous Quantum Teleportation in the Presence of Adversarial Attacks and Channel Noise. Sensors 2022, 22, 7587. [CrossRef] [PubMed]

2. Gisin, N. Quantum Randomness. Non–Locality, Teleportation and Other Quantum Wonders; Alpina non–fiction: Moscow, Russia,2018; 208p.

3. Wang, Y.; Hu, M.-L. Quantum Teleportation and Dense Coding in Multiple Bosonic Reservoirs. Entropy 2022, 24, 1114. [CrossRef][PubMed]

4. Wen, X.; Chen, Y.; Zhang, W.; Jiang, Z.L.; Fang, J. Blockchain Consensus Mechanism Based on Quantum Teleportation. Mathematics 2022, 10, 2385. [CrossRef]

5. Lucamarini, M.; Yuan, Z.; Dynes, J.; Shields, A. Overcoming the Rate–Distance Limit of Quantum Key Distribution without Quantum Repeaters. Nature 2018, 557, 400–403. [CrossRef] [PubMed]

6. Jian-Long Liu, Xi-Yu Luo, Yong Yu, Chao-Yang Wang, Bin Wang, Yi Hu, Jun Li, Ming-Yang Zheng, Bo Yao, Zi Yan, Da Teng, Jin-Wei Jiang, Xiao-Bing Liu, Xiu-Ping Xie, Jun Zhang, Qing-He Mao, Xiao Jiang, Qiang Zhang, Xiao-Hui Bao, Jian-Wei Pan. A multinode quantum network over a metropolitan area https://doi.org/10.48550/arXiv.2309.00221

Автор _____ Ляшенко К.А

Научный руководитель,
д.ф.–м.н., профессор
кафедры «Кибербезопасность
информационных систем» ДГТУ _____ Черкесова Л.В