Известия НАН Армении, Физика, т.60, №3, с.314 (2025)
DOI: 10.54503/0002-3035-2025-60.3-314

OBLIQ: A NOVEL PROTOCOL FOR OBLIVIOUS TRANSFER

M.K. Srivastava[1*], P.K. Singh[1], S.K. Singh[2]

[1]Department of Computer Science and Engineering, Madan Mohan Malviya University of Technology, Gorakhpur, Uttar Pradesh, India,273010
[2]Department of Computer Science and Engineering, IIT(BHU), Varanasi, Uttar Pradesh, India, 221005

[*]e-mail: mksgkp@gmail.com

(Поступила в редакцию 2 сентября 2025 г.)

Oblivious transfer is a type of message transfer in which a sender transmits one out of many potential pieces of information to the receiver, but she has no knowledge about the actual piece of information being received by the receiver. Oblivious transfer is a deceptively simple scheme that has many possible applications such as secure multiparty computation, private set intersection, federated learning, zero-knowledge proofs, accessing sensitive data etc. Security of most classical oblivious transfer protocols is based upon the unproven assumptions about the computational complexity of certain number theoretic problems such as integer factorization. So, existing classical protocols for oblivious transfer are only computationally secure and not unconditionally secure. Although many quantum oblivious protocols have been proposed lately, they are not simple and easy to implement. In the present work we propose a quantum oblivious transfer protocol that is efficient, simple and easily implementable with the existing quantum technology.

ЛИТЕРАТУРА

1. Agarwal, A., Bartusek, J., Khurana, D., and Kumar, N., *Adv. Cryptol. – EUROCRYPT*, 2023, vol. 14004, p. 363.
2. Damgård, I.B., Fehr, S., Salvail, L., and Schaffner, C., *SIAM J. Comput*., 2008, vol. 37 no. 6, p. 1865.
3. Erven, C., Ng, N., Gigov, N., Laflamme, R., Wehner, S., and Weihs, G., *Nat. Commun.*, 2014, vol. 5, p. 3418.
4. Lupo, C., Peat, J.T., Andersson, E., and Kok, P., *Phys. Rev. Res*. 2023, vol. 5 no. 3, p. 033163.
5. Bernstein D.J. and Lange, T., *Nature* 2017, vol. 549 no. 7671, p. 188.
6. Lo, H.-K., *Phys. Rev. A*, 1997, vol. 56 no. 2 p. 1154.
7. Mayers, D., *Phys. Rev. Lett*., 1997, vol. 78 no. 17, p. 3414.
8. He, G.-P., and Wang, Z.-D., *Phys. Rev. A*, 2006, vol. 73, p. 012331.
9. He, G.-P. and Wang, Z.-D., *Phys. Rev. A*, 2006, vol. 73, p. 044304.
10. Sarkar, S., Srivastava, V., Mohanty, T., Debnath, S.K., and Mesnager, S., *Clust. Comput*., 2024, vol. 27, no. 10, p. 14037.
11. Yang, Y.-G., Sun, S.-J., Xu, P., and Tian, J., *Quantum Inf. Process*., 2014, vol. 13, no. 3, p. 805.
12. Gao, F., Liu, B., Wen, Q.-Y., and Chen, H., *Opt. Express*, 2012, vol. 20, no. 16, p. 17411.