Quantum Oblivious Key Distribution (QOKD) system enables two parties to share a set of keys only known by them. This system guarantees the communication between them perfectly secured, even if an eavesdropper has access to one or more of these keys, its presence is detected and the compromised keys are immediately destroyed.

A QOKD system enables two parties to have symmetric secrete keys, i.e. the two parties have exactly the same keys even if they are physically far one from each other. Furthermore, this system also provides to the two parties a possibility of have symmetric or asymmetric oblivious keys, i.e. the two parties may have each the same set of keys, but one of them does not know everything about them, whereas the other knows all information about the set. This way, these sets can have the same number of right and random bits [1] or a different number of right and random bits [2] depending on the protocol that it is being implemented.

A QOKD system can be used in cryptology or in secure multi party computation systems, since it enables a key distribution perfectly secured as a traditionally Quantum Key Distribution (QKD) systems as proofed for BB84 Quantum Key Distribution Protocol [3].

# References

|  |  |
| --- | --- |
| [1] | C. Crépeu, "Quantum Oblivious Transfer," *Journal of Modern Optics,* vol. 41, pp. 2445-2454, 1994. |
| [2] | M. Xu, R.-h. Shi, Z.-y. Luo and Z.-w. Peng, "Nearest private query based on quantum oblivious key distribution," *Quantum Information Processing,* vol. 16, p. 286, 24 October 2017. |
| [3] | P. W. Shor and J. Preskill, "Simple Proof of the BB84 Quantum Key Distribution Protocol," *Phys. Rev. Lett.,* vol. 85, pp. 441--444, July 2000. |