Yang, Yu-Guang; Sun, Si-Jia; Wang, Yan
Quantum oblivious transfer based on a quantum symmetrically private information retrieval protocol.

Summary: Private information retrieval implies oblivious transfer in classical cryptography. Following this clue, we present a novel quantum one-out-of-two OT protocol based on a practical quantum symmetrically private information retrieval protocol Jakobi et al. (Phys. Rev. A 83, 022301 2011), with changes only in the classical postprocessing of the key. While unconditionally secure oblivious transfer is known to be impossible, we argue that an interesting degree of security can be achieved by means of quantum physical principles instead of unproven security assumptions in order to protect both the sender and the receiver. The proposed OT protocol is loss tolerant, practical and robust against quantum memory attack.

Keywords: oblivious transfer; all-or-nothing oblivious transfer; one-out-of-two oblivious transfer; symmetrically private information retrieval
doi:10.1007/s10773-014-2286-3