World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:17, No:07, 2023

Non-Interactive XOR Quantum Oblivious Transfer: Optimal Protocols and Their Experimental Implementations

Authors : Lara Stroh, Nikola Horová, Robert Stárek, Ittoop V. Puthoor, Michal Mičuda, Miloslav Dušek, Erika Andersson

Abstract : Oblivious transfer (OT) is an important cryptographic primitive. Any multi-party computation can be realised with OT as a building block. XOR oblivious transfer (XOT) is a variant where the sender Alice has two bits, and a receiver, Bob, obtains either the first bit, the second bit, or their XOR. Bob should not learn anything more than this, and Alice should not learn what Bob has learned. Perfect quantum OT with information-theoretic security is known to be impossible. We determine the smallest possible cheating probabilities for unrestricted dishonest parties in non-interactive quantum XOT protocols using symmetric pure states and present an optimal protocol which outperforms classical protocols. We also "reverse" this protocol so that Bob becomes the sender of a quantum state and Alice the receiver who measures it while still implementing oblivious transfer from Alice to Bob. Cheating probabilities for both parties stay the same as for the unreversed protocol. We optically implemented both the unreversed and the reversed protocols and cheating strategies, noting that the reversed protocol is easier to implement.

Keywords : oblivious transfer, quantum protocol, cryptography, XOR
Conference Title : ICQCCIS 2023 : International Conference on Quantum Computer, Computing and Information Sciences
Conference Location : Zurich, Switzerland
Conference Dates : July 24-25, 2023