An Unconditionally Secure Protocol Based on Lattices over the Gaussian Channel

Motohiko Isaka

We propose to achieve an information theoretically secure oblivious transfer using lattice partitions based on the additive white Gaussian noise channel. A Protocol is presented and the security and efficiency is discussed.