Oblivious Transfer from the Additive White Gaussian Noise Channel

Motohiko ISAKA

We consider the use of the additive white Gaussian noise channel to achieve information theoretically secure oblivious transfer. A protocol for this primitive that ensures the correctness and privacy for players is presented together with the signal design. We also study the information theoretic efficiency of the protocol, and some more practical issues where the parameter of the channel is unknown to the players.

key words: oblivious transfer, additive white Gaussian noise channel, information theoretic security, oblivious transfer rate