Efficient Oblivious Transfer from Algebraic Signaling over the Gaussian Channel

Motohiko Isaka

We study the use of the additive white Gaussian noise channel to achieve oblivious transfer which is an important cryptographic primitive in multiparty computation. An efficient protocol for unconditionally secure oblivious transfer is presented. We show that channel input alphabets with a certain algebraic structure and their partitions are useful in achieving privacy for players and ensuring high efficiency of the protocol. Security and information theoretic efficiency of the protocol is investigated.