# Cryptographic Primitives Based on Discrete-Input AWGN Channels

Motohiko Isaka and Yuki Shimizu

Two cryptographic primitives, commitment and oblivious transfer, are devised based on the additive white Gaussian noise channel and discrete input alphabet. We present protocols and analyze the security and information theoretic efficiencies.