# On Secret Key Agreement from the Additive White Gaussian Noise Channel

Motohiko Isaka and Seiya Kawata

It is known that noise on communication channels can be a powerful resource for certain cryptographic purposes, basically by utilizing the randomness to ensure the secrecy. In this paper, we study information theoretically secure key agreement through the use of the additive white Gaussian noise channel and public discussion. We present a protocol for key agreement that defines the computation and communications between the two communicating parties to share a common secret information, about which negligible amount of information is revealed to other third parties. We discuss the signal design, secrecy and the achievable rate of the protocol.