ガウス雑音通信路に基づく情報理論的安全性について

河田　誠也、服部　一章、井坂　元彦

加法的白色ガウス通信路を利用した情報理論的に安全な鍵共有について検討する。送信者から受信者および第三者への通信路における雑音が独立である状況において、メッセージ認証のある公開通信路を用いた鍵共有のためのプロトコルを示し、送受信者間で達成可能な秘密鍵レートについて議論を行う。

キーワード　　情報理論的安全性、加法的白色ガウス通信路、鍵共有

On Unconditional Security from the Gaussian Channel

Seiya KAWATA, Kazuaki HATTORI, and Motohiko ISAKA

Cryptographic power of noise on communication channels has been recently well recognized. In this paper, we study the use of noisy channels for secret key agreement together with an authenticated but insecure public channel. A protocol for key agreement is presented so that the two parties can share a common secret information about which negligible amount of information is revealed to other third parties. We discuss the signal design, security and the achievable rate of the protocol.

Key words secret key agreement, additive white Gaussian noise channel, information theoretic security