加法的連続雑音通信路を用いた 2 者間プロトコル

服部　一章、河田　誠也、井坂　元彦

加法的連続雑音通信路を利用した紛失通信の実現法について議論する.

キーワード　情報理論的安全性、加法的通信路、紛失通信

A Two Party Protocol Based on Additive Continuous Noisy Chanenls

Kazuaki HATTORI, Seiya KAWATA, and Motohiko ISAKA

Oblivious transfer is an important cryptographic primitive in secure multiparty computation.　In this paper, we consider the use of additive continuous noisy channels to provide information theoretically secure oblivious transfer without relying on any computational assumptions.　We present two approaches toward this goal.

Key words　oblivious transfer, additive continuous noisy channel, information theoretic security