雑音通信路に基づく紛失通信の効率について

井坂　元彦、清水　勇樹

紛失通信は、電子選挙などを含むマルチパーティプロトコルにおいて安全に関数評価を行う上で有用である。本稿では、情報理論的な安全性を有する紛失通信を雑音通信路に基づいて構成する場合の効率に関する議論を行う。

キーワード　　紛失通信、白色ガウス雑音通信路、情報理論的安全性

On the Efficiency of Oblivious Transfer Based on Noisy Channels

Motohiko ISAKA and Yuki SHIMIZU

We consider a cryptographic primitive called oblivious transfer which is useful in the context of secure multiparty computation. Noisy channels are utilized to achieve information theoretically secure oblivious transfer rather than resorting to a certain computational assumption. The information theoretic efficiency of the protocol based on the additive white Gaussian noise channel is investigated.

Key words oblivious transfer, additive white Gaussian noise channel, information theoretic security