情報理論的に安全な乱数の生成装置の開発と乱数配送の暗号化アルゴリズムの開発

企業／システム工学㈱
研究者／高木相（日本大学工学部情報工学科教授）

本開発テーマの目標としているところは、匿名のクライアントの要求に応じてランダムなビット列（乱数）を生成し、それを安全に供給する暗号化アルゴリズムの開発である。

乱数源として物理乱数を用い、その統計的性質の検定を行うとともに安全な動作のための必要なハードウェア的な方法を施す。則ち、物理乱数はPN接合の逆バイアスなどによる熱雑音を増幅し、それを適当な帯域通過フィルタ比較器を通し２値の乱数にする。

乱数生成装置を試作した。この乱数の配送については、共通鍵方式と公開鍵方式の２つの方式において利用出来るようにソフトウェアの開発を行った。