システム情報工学研究科修士論文概要

年 度	平成 25 年度	学位名	修士(工学)
専 攻	知能機能システム 専攻	著者氏名	菊池 駿

指導教員氏名　古賀 弘樹

論文題目

新しい安全性基準に基づくシャノン暗号における符号化定理

論文概要

暗号の安全性の概念として攻撃者に対して計算能力の制限をしない情報理論的安全性がある. 基本的な共通鍵暗号方式であるシャノンの暗号方式は情報理論的安全性に基づいており, 暗号文からは平文の情報が全く漏れない完全秘匿が定義されている. 近年, 平文の推定成功確率に基づく安全性が提案された. この安全性では攻撃者が暗号文を見た後でも最も推測しやすい平文の確率は変わらない.

本稿では, 3種類の安全性基準を提案し, それぞれの安全性に対する暗号文と鍵のレートの達成可能領域を調べる. 1つ目の安全性基準として, 平文の推定成功確率に基づく安全性を微小な復号誤りを許した場合への拡張を行う. また, リスト復号器を攻撃者の復号器として考え, 1に近い確率で元の平文がリストに含まれるためのリストの大きさに基づく 2 種類の安全性を提案する. また, リストの大きさに基づく安全性の1つとシャノンが定義した条件付きエントロピーに基づく安全性, 拡張した推定成功確率に基づく安全性の関係を調べる.

本稿では提案した3種類の安全性に対する暗号文と鍵のレートの達成可能領域が, 条件付きエントロピーに基づく安全性と一致することを示す. また, 暗号がリストを用いた安全性を満たしたとき, その暗号が条件付きエントロピーに基づく安全性, 拡張した推定成功確率に基づく安全性を満たすことを示す.

審査日　平成 26 年 1 月 29 日

審査員	(大学名 職名)	(学位)	(氏名)
主査	筑波大学 准教授	博士(工学)	古賀 弘樹
副査	筑波大学 教授	工学博士	丸山 勉
副査	筑波大学 教授	工学博士	森田 昌彦