氏　名	境（さかい）　隆一（りゅういち）
学位(専攻分野)	博　士　（工　学）
学位記番号	博　甲　第　95　号
学位授与の日付	平成 7 年 3 月 24 日
学位授与の要件	学位規則第 4 条第 1 項該当
研究科・専攻	工芸科学研究科情報・生産科学専攻
学位論文題目	**Construction of Digital Communication and Storage Systems with High Security and High Reliability** （安全性と信頼性を考慮したディジタルシステムの構成に関する研究）
論文審査委員	（主査） 教授 笠原正雄　教授 田村　博 教授 吉田靖夫　教授 柴山　潔　教授 三木博雄

論文内容の要旨

本論文は高安全性と高信頼性とが保証された情報通信（記録）システムを構築するために、公開鍵暗号方式並びに誤り訂正符号に関する研究を行い、その成果をまとめたものである。本論文は 6 章から構成されている。

第 1 章は序論であり、本研究の動機について述べ、さらに本研究の背景、関連研究分野における位置付け等について述べている。

第 2 章では ID（Identification）情報に基づいた予備通信を必要としない鍵共有方式について、新しい方式を提案している。本提案方式に対する従来の攻撃法に関しては安全であることを証明するとともに、想定し得る有力な攻撃法を自ら考案し、この手法に関して詳細な解析を行っている。その結果、提案方式は従来の ID 情報に基づく鍵共有方式に比べて結託閾値を大幅に改善し得ることを示している。

第 3 章では公開鍵暗号の代表例としての RSA（Rivest-Shamir-Adleman）暗号の鍵生成法について考察している。RSA 暗号においては暗号化鍵、復号鍵のサイズが暗号処理時間に直接関係する。このため鍵のサイズ、特に復号鍵のサイズを縮小することが望まれているが、第 3 章では安全性を損なうことなく暗号化鍵のサイズと復号鍵のサイズの和を従来に比べ 4 / 5 程度に縮小し得る方法を提案し、本手法の有効性について考察している。

第 4 章では暗号理論、符号理論の分野で、最近、はなやかな脚光を浴びている楕円曲線に注目し、暗号への応用という立場から基本的な考察を行っている。これらの考察を踏まえて、共通の法を用いることを可能にする RSA 暗号タイプの新しい公開鍵暗号方式を提案し、その安全性について考察している。

第 5 章では情報通信（記録）システムの高信頼化のための有力な手法として知られる畳み込み符号について、主として最良符号の探索という立場から研究を行っている。すなわち拘束長の大きい範囲でも比較的容易に重み分布を導出できるアルゴリズムを提案し、これに基づいて拘束長19以下という従来にない広い範囲で多数の最良符号を発見している。

第 6 章は結論であって、本研究で得られた成果を総括している。

論文審査の結果の要旨

情報化社会の進展とともに、高安全性と高信頼性とが保証された情報通信（記録）システムを構築する

ことが重要な課題となりつつある。本論文は暗号理論及び符号理論をそれぞれ基盤にして、高安全性及び高信頼性を確保する手法について研究したものである。本論文は、まず初めに、高安全性の確保という立場から画期的な暗号方式として、近年注目を集めている公開型暗号方式に関し研究を行っている。

最初にIDに基づいた予備通信を必要としない鍵共有方式について新しい方式を提案し、想定し得る有力な攻撃法を自ら考案し、これに対する安全性について考察している。またRSA暗号の安全性を損なうことなく、暗号化鍵のサイズと復号鍵のサイズの和を従来の4/5程度に縮小し得る方法を提案している。さらに楕円曲線上でRSA型公開鍵暗号方式を提案するとともに、本方式によって共通の法を用いることが初めて可能になったことを明らかにしている。

次に高信頼性の確保という立場から最有力な手法とされ、また公開鍵暗号への応用も考えられている誤り訂正符号に着目し、主として最良畳み込み符号の探索について研究している。拘束長が19以下という従来にない広い範囲で、畳み込み符号の重み分布を求め、これによって最良畳み込み符号を多数発見している。

以上のように、本論文は情報通信（記録）システムの高安全性、高信頼性を確保するための手法について研究し、新しい画期的な手法をいくつか見い出している。本論文の主要な内容はレフェリーシステムの確立した学術雑誌に掲載されたもの2編、及び掲載決定の論文1編に基づいている。上記の掲載あるいは掲載決定の論文においては、全て申請者が筆頭著者である。以上を踏まえて、審査委員会は申請者の業績は情報通信工学に寄与するところが大であることを認め、申請論文は博士（工学）の学位授与に値すると判定した。