氏名	佐竹賢治（さたけけんじ）
学位(専攻分野)	博士（工学）
学位記番号	博甲第144号
学位授与の日付	平成9年3月25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 Communication and Storage Systems with High Security and High Reliability**
審査委員	（主査）教授 笠原正雄 教授 柴山潔　教授 三木博雄　助教授 若杉耕一郎

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記録・通信システムの構築に資するための基本的な手法について研究したものである。以下に示す6章から構成されている。

第1章序論は本論文で遂行した研究内容に関する研究分野およびその背景を示している。

第2章は高速暗号通信システムを構築することを目的に、代表的な公開鍵暗号として知られるRSA（Rivest-Shamir-Adleman）暗号に適用可能な高速演算法を提案している。本章で述べる高速べき乗剰余演算法を用いたRSA暗号においては全数探索的攻撃を受けた場合、その安全性を10^{17}を十分越える探索数に設定という条件のもとに、鍵サイズを10進数で20桁（すなわち電話番号の2戸分）にまで縮小することが可能になることを明らかにしている。

第3章～第5章では高容量通信を可能にする重畳符号について考察している。

第3章では理論上あるいは実用上重要な誤り訂正符号の一つとして知られているBCH符号で構成した重畳符号は、高効率復号法として広く知られている“KH復号法”の適用が可能であり、この復号法を用いた場合同程度の復号誤り率および符号長という条件のもとに、単一のBCH符号に比べ符号長1000以上の範囲において高符号化率を実現し得ることを具体例とともに明らかにしている。

第4章では重畳符号を構成する被重畳符号をさらに重畳符号で構成した多次元の多次重畳符号化について考察している。このような多次重畳符号についても、“KH復号法”を繰り返し使用するが可能なこと、並びに符号化率の点において一次の重畳符号より有利となる符号が構成可能となること等を明らかにしている。さらに多次重畳符号の段数を適切に設定することにより、通信路（メモリ）のシンボル誤り率毎に最大の符号化率を実現し得る重畳符号の構成が可能となることを明らかにしている。

第5章では“KH復号法”に軟判定復号法を効果的に併用することを試み、重畳符号に対し有効となる新しい復号法を提案している。この結果、比較的短い符号長においても高効率な重畳符号が構成可能となることを明らかにしている。

第6章は結論であって、情報記録・通信システムの安全性および信頼性向上のために、本論文が寄与しうる事項を総括して述べている。

論文審査の結果の要旨

マルチメディア社会の進展とともに、高安全性と高信頼性とが保障された情報記録・通信システムを構築することが重要なテーマになっている。本論文は、暗号理論と符号理論をそれぞれ基盤にして、高安全

性・高信頼性を確保する手法について研究したものである。すなわち、本論文は、暗号化の鍵を公開することを可能にした画期的な方式として、近年多くの注目を集めている公開鍵暗号方式について、主として、

(i) 公開鍵暗号使用の際に必要となる公開情報の効果的な削減法

(ii) 公開鍵暗号に共通の短所とされる過大な暗号化・復号時間の短縮法

について研究を進めている。さらに高信頼性の確保という立場から、有力な手法として知られている重畳符号について、主として

(iii) 重畳符号に対して有力な復号法として知られているKH復号法のパフォーマンスの解析

(iv) 上記(iii)に基づき、最適な符号の探索

(v) 新しい復号法の提案とそのパフォーマンスの解析

を行っている。主な成果は次の通りである。

(1) 実用上の十分な安全性を確保した上で、代表的な公開鍵暗号として知られているRSA暗号の公開情報のサイズに比べ、1/10程度に削減する手法を明らかにしている。

(2) 上記手法によって、暗号化、復号に要する時間を、RSA暗号に比べ約1/10に圧縮することが可能であることを明らかにしている。

(3) 重畳符号を多次元に拡張し、KH復号法を適用した場合の解析を厳密に行っている。そして、これに基づいて、最適な重畳符号を明らかにしている。発見された符号のほとんどは、従来の代表的な誤り訂正符号であるBCH符号よりも優れた符号化率を有することを明らかにしている。

(4) KH復号法に基づいた新しい軟判定復号法を提案し、現在、代表的な軟判定復号法として知られるChase復号法よりも、優れることを明らかにしている。

以上のように、本論文は情報記録・通信システムの高安全性・高信頼性を獲得するための手法について研究し、それぞれについて厳密な解析を行っている。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3編、掲載決定の論文1編および本学紀要の論文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、4編は、申請者が筆頭著者であり、残る1編は2番目の著者である。その業績は、情報記録・通信工学の進歩に寄与するところが大であり、本論文は博士論文として価値あるものと認める。