The University of Osaka
Institutional Knowledge Archive

Title	代数的手法を用いた情報セキュリティ技術に関する研究
Author(s)	李, 壬永
Citation	大阪大学, 1989, 博士論文
Version Type	
URL	https://hdl.handle.net/11094/36430
rights	
Note	著者からインターネット公開の許諾が得られていないため、論文の要旨のみを公開しています。全文のご利用をご希望の場合は、大阪大学の博士論文についてをご参照ください。

The University of Osaka Institutional Knowledge Archive : OUKA

https://ir.library.osaka-u.ac.jp/

The University of Osaka

【21】

氏名・（本籍）	李（り） 壬（いむ） 永（よん）
学位の種類	工学博士
学位記番号	第 8660 号
学位授与の日付	平成元年3月24日
学位授与の要件	工学研究科通信工学専攻 学位規則第5条第1項該当
学位論文題目	**代数的手法を用いた情報セキュリティ技術に関する研究**
論文審査委員	（主査） 教授 森永 規彦 教授 倉薗 貞夫　教授 中西 義郎　教授 北橋 忠宏 教授 手塚 慶一

論文内容の要旨

本論文は，代数的手法を用いた情報セキュリティ技術に関する研究の成果をまとめたものであり，4章から構成されている。

第1章は序論であり，本研究に関連する分野において従来より行われてきた研究について概説し，本研究の目的ならびに工学的意義を明らかにしている。

第2章では，代数的手法を用いた同報通信について論じている。まず，グループ単位による同報通信を対象として，整数環上の中国人剰余定理を用いた多重化・多重分離法に基づく暗号化方式を提案し，暗号化方式の演算回路を統一的にそのまま利用し得るような秘密鍵配送方式を提案している。本章の後半部においては，本方式を用いることにより，送信者が特定の受信者に対して不正行為を行うことが極めて困難であり，送信者の不正行為に対する同報性の確認が不必要であることを明らかにし，離脱者が生じた場合においても他の受信者の秘密鍵を変更する必要がないことおよび本方式における安全性について考察し，他の方式との比較を行っている。

第3章では，（K，N）しきい値法の一つの実現法としてStone符号を用いた手法を提案している。まず，構成法について述べ，その構成法が（K，N）しきい値法の条件を満たすことを示し,またピースに誤りが生起した場合においても本手法を用いることにより，誤り訂正あるいは検出が可能になり，もとの情報が再生できることを明らかにしている。更に，本手法に対する安全性について考察を行い，階層構造を有するグループにおいても本手法の適用が可能であることを述べ，本手法を用いることにより得られる特性を明らかにしている。

第4章は結論であり，本研究により得られた主要な成果を総括して述べている。

論文の審査結果の要旨

本論文は，暗号方式ならびに秘密鍵保管法に代数的手法を応用した情報セキュリティに関する理論的研究をまとめたものであって，次のような成果を上げている。

(1) 同報通信を対象として，整数環上の中国人剰余定理を用いた多重化・多重分離法に基づく暗号化方式を新しく提案し，本手法によれば，送信者による不正行為が困難であること，離脱者が生じた場合でも他の受信者の秘密鍵を変更する必要のないこと，演算装置の統一化が図れること等を明らかにしている。

(2) 秘密鍵保管法の１つである（K，N）しきい値法の実現法として，代数的バースト誤り訂正符号であるStone 符号を用いた手法を提案し，その構成法が（K，N）しきい値法の条件を満たすことを明らかにすると共に，分散情報に誤りが生じた場合の対策として拡張（K，N）しきい値法を提案し，誤りの訂正が可能であることを明らかにしている。

以上のように本論文は，代数的手法を用いた情報セキュリティ技術に関する新しい知見を与えており，通信工学，特に暗号理論の発展に寄与するところが大きい。よって本論文は博士論文として価値あるものと認める。