【19】

氏名・（本籍）	森（もり）　井（い）　昌（まさ）　克（かつ）
学位の種類	工　学　博　士
学位記番号	第　8658　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	**有限体演算の高能率化とその符号・暗号理論への応用に関する研究**
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，有限体上での各種演算の高能率化とその符号理論および暗号理論への応用に関する研究の成果をまとめたものであり，7章から構成されている。

第1章では，有限体理論と符号理論および暗号理論との関連を系統的に述べ，本研究の意義，所在を明らかにしている。

第2章では，ベクトル表現されたGF(q^m) 上の除算がGF(q)上のm次離散時間ウィナーホップ方程式を解くことと等価であることを証明し，更にこの離散時間ウィナーホップ方程式について得られた結果を検討することにより，ビットシリアル型乗算アルゴリズムが，より一般的に，しかも見通し良く導出されることを明らかにしている。

第3章では，部分体を用いてGF（2^m）の逆元を効率よく求める算法を提案すると共に，この算法を応用してGF（2^m）の逆元を生成するm入力m出力の組合せ論理回路を構成する方法を提案している。

第4章では，GF(2)上の多項式間の剰余演算および整数上での剰余演算の高速化手法を提案している。

第5章では，誤り位置多項式がその根として0を有する場合のゴッパ符号の復号問題との関係を明らかにしている。

第6章では，素数を法とする有限体上の離散対数問題を応用した公開鍵暗号の一方式を提案し，この暗号系の評価を行い，他の公開鍵暗号との関係を明らかにしている。

第7章は結論であり，本研究で得られた主要な成果について総括を行っている。

論文の審査結果の要旨

本論文は，有限体上での各種演算等の高能率化アルゴリズムの開発とその符号・暗号理論への応用に関する理論的研究をまとめたものであって，以下のような成果を上げている。

(1) ベクトル表現されたＧＦ（q^m）上の除算がＧＦ(q)上のm次離散時間ウィナーホップ方程式を解くことと等価であることを証明すると共に，これによればビットシリアル型乗算アルゴリズムが，より一般的に，見通し良く導出されることを明らかにしている。

(2) ＧＦ（2^m）の逆元を生成するm入力m出力の組合せ論理回路を構成する方法を提案し，本方法が，ＧＦ（2^m）がその部分体としてＧＦ（2^2）をもつ場合に有用であることを示している。

(3) 誤り訂正符号，暗号等の符号化・復合化アルゴリズムの基幹をなす有限体上の演算であるＧＦ(2)上の多項式間の剰余演算の高速化手法を提案している。

(4) 誤り位置多項式が根として0を有する場合のゴッパ符号の復合問題と，与えられた系列を生成する最小段数の線形帰還シフトレジスタ合成問題との関係を考察し，誤り位置多項式がその根に0を有する場合でもゴッパ符号が復号できることを明らかにしている。

(5) 素体ＧＦ(P)上の離散対数問題を応用した公開鍵暗号の一方式を提案し，他の公開鍵暗号と比べて，復号化変換はほぼ同等であるものの，並列処理技法が一層容易に適用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，有限体上での各種演算の高能率化アルゴリズムの開発ならびにその符号・暗号理論への応用に関して新しい知見を与えており，通信工学，特に符号・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。