平成16年度 情報工学専攻修士論文要旨

高木 研究室	氏　　名	高 宮 英 泰
論　文　題　目	拡張ユークリッド法に基づく GF(2^m) 上の乗除算回路	

近年，インターネット等のディジタル通信システムの発展と普及にともない，ディジタル通信路を経由する情報の信頼性と安全性を確保することが重要となっている．一般に，情報の信頼性を向上させるために誤り訂正符号が，安全性を向上させるために暗号が用いられる．

ガロア体 GF(2^m) 上の算術演算は誤り訂正符号や公開鍵暗号の分野で重要な役割を果たしている．特に公開鍵暗号で用いられる場合，m は数百といった大きな値となる．GF(2^m) 上の乗算，除算は複雑で時間のかかる演算であり，その高速化が重要な課題となっている．VLSI 技術の発展にともない，時間のかかる演算を専用回路で実現することにより，演算を高速化することが可能となっており，各演算のための専用回路に関する研究が盛んに行われている．

携帯端末や電子決済に用いられる Smart Card 等に搭載される暗号処理回路では，高速性とともに省面積性が重要視される．これらの暗号処理回路では，種々の暗号に対応するために，GF(2^m) 上の複数の演算を行う必要がある．そのため，GF(2^m) 上の複数の演算を行う小面積の回路の開発が望まれている．

本研究では GF(2^m) 上の乗算，モンゴメリ乗算，除算を行うことのできる単一の回路を提案する．乗算はシフトと加算により計算する．モンゴメリ乗算は乗数の最上位ビットから順に参照する新しい方法により計算する．除算は拡張ユークリッド法を基にしたアルゴリズムで計算する．これら三つの演算はシフト，AND，Exclusive-OR 等の単純な演算の繰り返しにより実現できる．

拡張ユークリッド法に基づく除算回路の制御回路に若干の変更を加えるだけでこれらの三つの演算を行うことのできる回路を構成することが出来た．この回路を利用すれば，この三つの演算を個別に行う回路を組み合わせた場合と比較して総回路面積を大幅に節約できる．

この乗算/除算回路は規則正しいビットスライス構造を持ち，除算は 2m クロックサイクルで，乗算は m クロックサイクルで実行でき，回路の段数は定数であり m に依存しない．乗算/除算回路のハードウェア量は除算単体の回路よりもわずかに大きいだけで済む．