平成28年　1月　8日

電気・電子情報工学専攻	学籍番号	M123204
申請者氏名	鮎澤　勇介	

指導教員氏名	市川　周一 藤枝　直輝

論　文　要　旨（修士）

論文題目	高基数モンゴメリ乗算法によるべき乗剰余演算の高速化

個人情報の送信や電子貨幣での決済など，情報の秘匿化は不可欠の技術になりつつある．情報の秘匿化には暗号技術が使われており，中でも公開鍵暗号であるRSA (Rivest, Shamir, Adleman) は広く使われている．RSAはべき乗剰余演算を用いているが，汎用プロセッサによるソフトウェア処理では計算時間が長く消費電力も大きい．そのため，べき乗剰余演算を専用ハードウェア化する研究が盛んである．

べき乗計算後に剰余をとった場合，べき乗計算時のビット幅が拡大し，剰余演算のコストが増大するといった問題が生じる．この問題を解決するためにべき乗剰余演算にはバイナリべき乗剰余演算が広く使われている．バイナリべき乗剰余法には，計算を最上位ビットから行う右向き法と，最下位ビットから行う左向き法が存在する．バイナリべき乗剰余法はべき乗計算の途中で剰余を取るため，ビット幅は常に一定となる．

乗算剰余には1985年にMontgomeryによって提案されたモンゴメリ乗算法がある．モンゴメリ乗算法ではビットシフトとビット切り出しにより，乗算剰余を高速に計算する．モンゴメリ乗算法は高基数化が可能であり，バイナリべき乗剰余法の組み合わせも可能である．

本論文では再構成可能な論理LSI (Large Scale Integration) であるFPGA (Field Programmable Gate Array) を評価基盤とし，高基数モンゴメリ乗算法に対して2つの高速化手法を提案する．1つ目はバイナリ法の検討である．これまでの研究では回路規模を削減するために右向きバイナリ法が多く用いられてきた．左向きバイナリ法を用いることで，右向きバイナリ法に比べ回路規模が増大するが乗算剰余を並列に実行することができる．左向きバイナリ法をモンゴメリ乗算法に対応させ，評価を行った (Method 1)．2つ目は高基数モンゴメリ乗算法の検討である．べき乗剰余演算の入出力ビット幅で動作するモジュールとワード単位で動作するモジュールを分離し，クロック系統を分けることで高速化を図った．モジュールの分離にあわせて1ワード分レジスタを冗長に用意し，比較処理を減らした．また，モジュール間の結線で剰余や除算を行い評価した (Method 2)．Method 1，Method 2を単独で適応した場合と同時に適応した場合で組み合わせの有効性を確認した (Method 1+2)．

提案手法の有効性を示す評価指標には面積と実行時間の積であるAT積 (Area-Time Product) を用いた．実行時間は最悪の場合の計算時間を用いる．面積はSlice数を用いる．DSP (Digital Signal Processing) ユニット，BRAM (Block RAM) はSlice数へ換算して計算する．Slice数への換算はCAD (Computer Aided Design) ツールのフロアプランナーで確認できる面積比を使用する．

既存のアルゴリズムを使用した手法に対し，Method 1では処理時間が1/2となり，LUT (Look Up Table)，Registersの回路要素は最大で87.9 %増加した．Method 2では回路規模の増大無しで処理時間を25.1倍高速化することができた．Method 1+2では処理時間は最大で約50.8倍高速化した．比較対象とした3つの先行研究に対し，回路規模は最大となってしまったがAT積を用いた評価では最小の値となった．