平成２８年度　卒業研究報告書概要

課程，学籍番号，氏名	課程：電気電子情報工学課程，学籍番号：B153266，氏名：本郷 誠人
工学分野名：情報通信システム	指導教員名：市川 周一，藤枝 直輝

題　　目：和

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手法の評価

（英 Evaluation of Acceleration Methods for Modular Exponentiation using High-Radix Montgomery Multiplication）

Abstract

There are many studies on dedicated hardware for modular exponentiation, which is used in public key cryptosystem RSA (Rivest, Shamir, Adleman). Ayuzawa proposed two acceleration methods for the high-radix Montgomery multiplication on FPGA (Field Programmable Gate Array), and evaluated their advantages with logic synthesis. The first idea was to parallelize modular multiplication by using right-to-left binary method (RL). The second was to use multiple clock signals (Multi). The purpose of this paper is to evaluate these two methods using place and route (PAR). An interface module, composed of serial-parallel and parallel-serial converters, was designed to reduce the number of pins. According to the evaluation results, the relative increase of LUT and Register by RL became smaller than the previous study. The execution time became eight times shorter using both RL and Multi, though the reduction ratio became smaller by adding the interface module. The AT product was reduced by 75.1 % using the both methods.

概　　要

RSA(Rivest，Shamir，Adleman)をはじめとした公開鍵暗号技術は，現在広く用いられている．RSA はべき乗剰余演算を利用しているが，汎用プロセッサによるソフトウェア処理は計算時間が長く，消費電力も大きいため，高速かつ低消費電力でべき乗剰余演算を行う専用ハードウェアの研究が行われている．

鮎澤(2016)は，乗算剰余を高速に行う手法のひとつである高基数モンゴメリ乗算法に対し，FPGA (Field Programmable Gate Array) への実装に適した 2 つの高速化手法を提案した．1 つ目はべき乗の算出法であるバイナリ法の採用である．先行研究においては回路規模の小さい右向きバイナリ法 (LR) が用いられてきたのに対し，左向きバイナリ法 (RL) を用いて乗算剰余を並列化した．2 つ目は高基数モンゴメリ乗算法の検討である．先行研究では単一クロックを用いていたのに対し，鮎澤は入出力ビット単位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け，複数クロック系統を使用ことで高速化した．鮎澤はこれらの組み合わせから LR_single，RL_single，LR_multi，RL_multi の 4 種類の高基数モンゴメリ乗算器を設計し，論理合成結果から提案手法の有効性を検証した．

本研究では，鮎澤の提案したべき乗剰余演算の高速化手法について，配置配線まで行った場合の有効性を評価する．入出力が数千ビットに及ぶ高基数モンゴメリ乗算回路を配置配線するため，シリアルパラレル変換とパラレルシリアル変換を行うインターフェイス回路を設計し，それを追加した場合と追加せずに入出力の制約を解除した場合で配置配線を行った．有効性の評価には面積と実行時間の積である AT 積を使用し，面積には Slice 数を，実行時間には最悪計算時間を用いた．DSP (Digital Signal Processing) ユニットはフロアプランナー上で表示される物理的な面積比から Slice 数に換算して面積評価値に含めた．

Slice の構成要素である LUT 数とレジスタ数は，インターフェイス回路の追加によりそれぞれ最大で 1.28 倍，2.52 倍に増加した．追加後の高基数モンゴメリ乗算器同士を比較すると，RL の適用による増加は，先行研究よりも小さくなった．

実行時間は，インターフェイス回路の追加の有無にかかわらず，RL の適用でおよそ半減し，multi の適用で約 1/4 となり，さらに両者を組み合わせて約 1/8 とすることも可能であることがわかった．しかしインターフェイス回路の追加により，配線遅延による制約で数%程度の実行時間削減率の低下が見られた．インターフェイス回路を追加して配置配線した場合の AT 積は，RL の適用で約 1.6 %，multi の適用で約 73.2 %減少し，これらを組み合わせた RL_multi では約 75.1 %の減少が見られた．

発表する際の課程を記入　電気・電子情報工学　課程　　発表番号　７９

（学籍が他課程所属の学生も発表する課程を記入すること）