3ZB-9

RSA 鍵ペア生成高速化のためのハードウェアの設計

高田 淳† 浜辺 直輝† 小島 正典† 柴田 浩†
†大阪工業大学 情報科学部

1． まえがき

RSA(Rivest Shamir Adleman)暗号は IC カードで採用されているが[1]，ソフトウェア処理では鍵発生に 15 秒程度の時間がかかる[2]．IC カードの発行が集中したときの待ちを解消するため，処理時間の短縮が望まれている．

鍵の発生は素数発生と鍵ペア生成に分けられ，素数発生にかかる時間は短い[3]．したがって鍵ペア生成をハードウェアにより高速化することで，より高速に鍵生成が可能であると考える．

そこで本稿では，鍵ペア生成を ALU(ハード)で行うプロセッサのアーキテクチャを提案し，FPGA でこのプロセッサを構成して高速化を検証する．

2． RSA 鍵生成アルゴリズム

ランダムに生成された 2 素数から公開・秘密両鍵を生成するには Fig.1 に示す最小公倍数，及び拡張ユークリッド法による演算を行う必要がある．

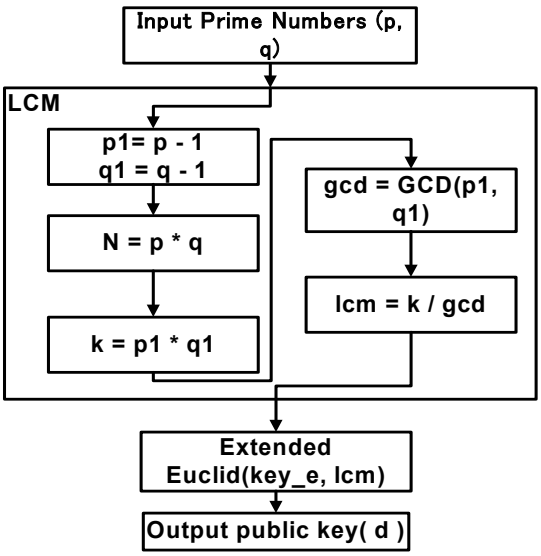

Fig.1 RSA Key Generation Algorithm

A design of Hardware for High-Speed RSA Key Pair Generation

† Faculty of Infomaion Science , Osaka Institute of Technology

そのため，CPU では要求する鍵長が増加する程に部分演算処理が増加し，多倍長整数による演算が必要となり演算処理時間が長くなる．ソフトウェアでは 1024bit の除算 1 回に約 17,000 サイクル程度がかかる．

3． 最小公倍数演算器

最小公倍数(LCM)を出力する演算器の構成を Fig.2 に示す．

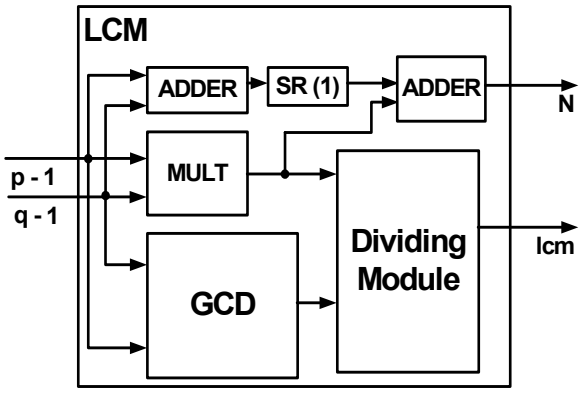

Fig.2 Least Common Multiple

2 数の乗算値と最大公約数(GCD)から LCM を出力するため，GCD をユークリッド互除法を順序回路のループ構造によって実現する．しかし，多ビットの乗剰余算回路を組み合わせ回路で行うと 1 サイクルが長くなり，システム全体の動作スピードが低下する．また使用ゲート数が増加し回路が大きくなる．そこで，小規模化かつ高速に演算を進めるために除算及び剰余算を行う回路を別途構成して搭載し，2 数の乗算，N の生成及び GCD の演算を並列して行う(Fig.3)．また，この LCM 回路の演算サイクルはおおよそ鍵長 n ビットの 2 倍に比例する．

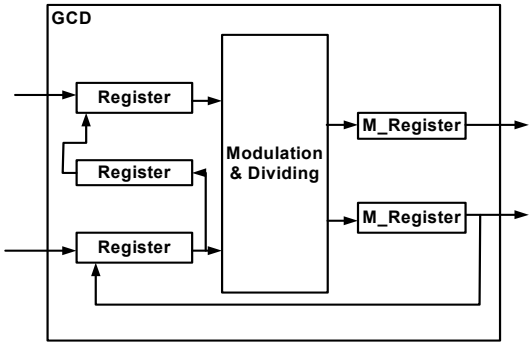

Fig.3 Greatest Common Divisor

4． 拡張ユークリッド演算器

拡張ユークリッド互除法は Fig.2 のユークリッドアルゴリズムの拡張であり，同様の手順で鍵Ｅの逆元(鍵 D)を導き出す．ソフトウェアで行う場合，乗除及び剰余を多倍長演算で行い，拡張ユークリッド演算全体で平均 10,000,000 サイクル程と考えられる．拡張ユークリッド演算のアルゴリズム(Fig.4)から，最もゲート使用率の高い乗算部を 8×8 の部分積の順序回路として構成しパイプライン処理を行う．乗算には 1024bit で 256 サイクル必要とし，演算器全体で 60,000 サイクルになると考えられる．

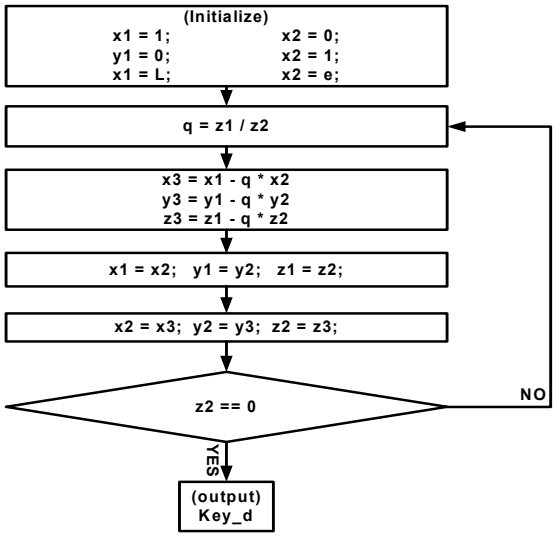

Fig.4 Extended Euclid Algorithm

5． RSA Key Generater

Fig.5 にこれらの演算器を用いたシステム構成を示す．システム全体ではソフトウェアで 64bit の鍵を生成する場合，平均して 15,000 サイクル程度になるが，Fig.5 に示したアーキテクチャを用いて平均 2,700 サイクルで鍵の生成が完了した．これによりソフトウェアに対して 5 倍の速度で生成が完了していると示される．

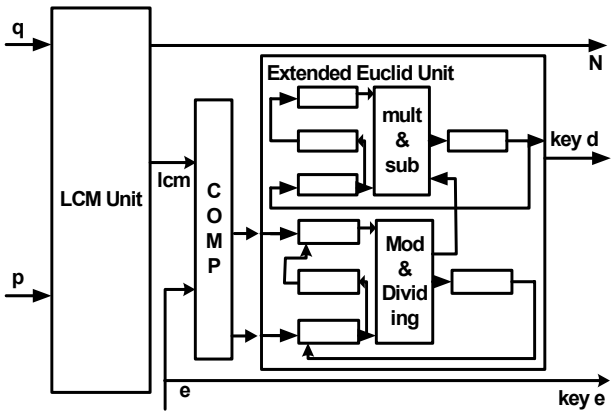

Fig.5 RSA Key Generater

しかしこの時のシステム全体のゲート数はおおよそ 85,000 ゲートと非常に大きいものになってしまった．そこで Fig.6 のように演算回路を乗除・剰余算器及び加減算器のそれぞれをモジュール化し，LCM と拡張ユークリッド演算器でシェアリングしてシステム全体の稼働率を高めるように変更する．

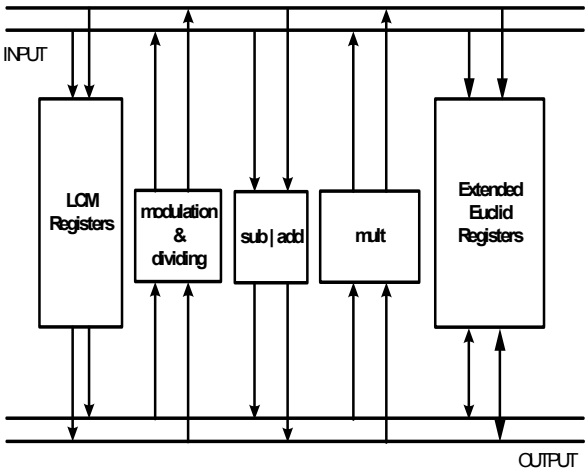

Fig.6 Sharing ALU Architecture

6． むすび

RSA の鍵生成において，素数発生をソフトウェアで，その他を ALU(ハード)で実行するプロセッサのアーキテクチャを提案した．FPGA でこのプロセッサを構成し 5 倍の速度で鍵生成ができることを検証した．

謝辞

本研究に際し，ご助言下さった諸先輩方に感謝いたします．

文　　献

[1] 大山 永昭： 次世代 IC カードシステムと暗号技術，情報処理通信学会誌 Vol.83 No.2 pp91-95

[2] Neal R. Wagner：“The Laws of Cryptography The RSA Cryptosystem”， http ://www.cs. utsa.edu/~wagner/laws/RSA.html

[3] 情報処理振興事業協会(IPA)： 素数生成アルゴリズムの調査・開発 調査報告書，http://www.ipa.go.jp/security/fy14/cripto/prime_num/invest.pdf