平成17年度 情報工学コース卒業研究報告要旨

高木 研究室	氏　　名	小 林 謙 太
卒業研究題目	素数生成のための倍数判定回路	

近年、情報技術の発展や情報通信ネットワーク基盤の整備により、暗号を用いた様々なシステムが実現されるようになった。例えば、電子商取引や住民基本台帳ネットワークシステムでも公開鍵暗号が用いられており、また今後 e-Japan 構想の流れに沿って全国規模の電子選挙が実現される可能性が高いと考えられる。現在用いられている公開鍵暗号方式は、RSA 暗号を初めとしてそのほとんどが素数をもとに鍵を構成しており、これらの巨大なシステムを支えるためには確実かつ高速に巨大な素数を生成することが必要となる。例えば RSA-2048 では 1024 bit の素数を 2 つ生成する必要があり、数十万人分の素数を生成するには高速なプロセッサを用いても 1 日以上を要する。

鍵に利用される素数は攻撃者に推測されない程度にランダムである必要がある。このような素数を生成する方法として、乱数生成と素数判定を用いて素数を得る方法がある。これには、素数と判定されるまで 巨大な奇数の生成を繰り返す Random Choice 法と、一度巨大な奇数を生成し 素数と判定されるまで 2 ずつ加算していく Incremental Search 法がある。素数判定は乱数生成や多倍長四則演算などに比べ非常に時間を要し、素数生成の計算時間の大部分を占めている。素数判定の実行回数を減らす方法として、小さな奇素数による試し割りを行う試行除算法が挙げられる。これにより多くの合成数を短時間でふるい落とすことができる。例えば 300 以下の奇素数で試行除算を行うと 8 割以上の数が合成数と判定できる。どのくらいの素数までの試行除算を行うと全体の計算時間が最小となるかは、実装および実行環境に依存する。

本研究は 1024 bit の素数生成を高速化することを目的とし、試行除算を行う回路を提案する。提案回路では試行除算のみを行い、他の処理はプロセッサが行うものとする。提案回路はおおまかに分けると制御部と剰余計算回路からなる。剰余計算回路は減算シフト型除算を行う順序回路である。提案回路は入力を受けとると、あらかじめ定めた m 個目までの奇素数について割り切れるかを計算し、いずれかで割り切れたかどうかを出力する。入力は 1024 bit と大きいため分割して行う。入力は開始時に 1 度行えば済むよう RAM に保存し、さらに除数である素数をあらかじめ ROM に保持しておく。これによりプロセッサとのデータ転送のオーバーヘッドを削減している。また、提案回路中の剰余計算アルゴリズムの桁選択の方法を、剰余が 0 かどうか判定する用途に限定し最適化することで、判定回路の面積を小さく抑えた。メモリを除いた提案回路を東大版 VDEC ROHM0.35μm のライブラリにより論理合成した結果、最大遅延が 4ns 以下、面積は 0.4mm^2 以下であった。

提案回路による試行除算を、プロセッサによる素数判定などの処理と並行して行う方法が、全体の実行時間を最小にする提案回路の使用方法である。素数判定の計算時間に対し、回路での試行除算の計算時間を十分小さく抑えると、試行除算処理に要する時間を回路への入力オーバーヘッドに置き換えることができる。

プロセッサのみで素数生成を行う場合の計算時間を測定するため、Random Choice により素数生成を行うプログラムを GMP ライブラリを用いて作成し実験した。素数判定には Miller-Rabin Test を用いた。すると 1.2GHz Pentium M プロセッサにおいて提案回路を並列に用いた場合、プロセッサのみで処理する場合に比べて、試行除算の計算時間を 25% 以下にでき、それに伴い素数生成全体の処理時間を計算上 90% 以下にできるという結果を得た。