平成１４年度　情報工学コース卒業研究報告要旨

高木 研究室	氏　　名	大西 康弘
卒業研究題目	$\mathrm{GF}(2^m)$ 上の多倍長乗算を容易にする生成多項式	

現在、キャッシュカードなどの磁気カードが普及しているが、今までよりも読み書きできるデータ量が多く、セキュリティの高いシステムとして、LSI チップが埋め込まれたスマートカードが注目を集めている。

セキュリティを高めるために暗号が使われる。スマートカードにおける公開鍵暗号の方式として有限体上での楕円曲線暗号方式が注目されている。楕円曲線暗号は RSA 暗号に比べ暗号強度が同程度の場合、鍵長が大幅に短くなる。RSA 暗号の鍵長として、現在最も使われている 1024 ビットの鍵長の暗号強度は、楕円曲線暗号では 160 ビットの鍵長の強度と同程度である。今後、より高い暗号強度が求められ、楕円曲線暗号ではおよそ 200 から 250 ビットの鍵長が必要とされる。

スマートカードが搭載しているプロセッサとして、8 ビットまたは 16 ビットのものが最も普及している。楕円曲線暗号の処理には $\mathrm{GF}(2^m)$ の乗算が必要であり、長ビットの演算を行わなければならない。そのために、データを 8 ビットごとに分割し、8 ビットプロセッサで繰り返し処理する必要がある。有限体上の乗算における剰余の計算には生成多項式を使うため、生成多項式の選び方により演算のコストが異なってくる。ワード単位を 8 ビットとして $\mathrm{GF}(2^m)$ 上の乗算を行うとき、$\mathrm{GF}(2)$ 上の多項式である $x^{8n} + f_7(x)$(ただし、n は整数であり、$f_7(x)$ は定数項が 1 の 7 次以下の多項式を表す) という生成多項式が存在すれば、有限体上のワード単位の乗算が容易になる。

本報告では、有限体上のワード単位の乗算を容易にする生成多項式 $x^{8n} + f_7(x)$ の探索を行った。$x^{8n} + f_7(x)$ という形の多項式は次数 n ごとに 128 個存在するが、そのような多項式の中には明らかに既約でないと言えるものが存在するため既約判定アルゴリズムによる判定を行う前に、既約でない多項式を除くことができる。このような枝刈りを行うことで既約判定を行う多項式を 56 個に削減できる。その結果、次数 $8n$ が 160 から 256 の範囲について $x^{8n} + f_7(x)$ という形の有限体上のワード単位の乗算を容易にする生成多項式が求まった。