平成19年度 情報工学コース卒業研究報告要旨

高木 研究室	氏　　名	中野一輝
卒業研究題目	GF(2^m) 上の乗算と AES MixColumns 計算の共用回路	

近年、情報通信の発展に伴って、その安全性のために暗号技術がより重要となっている。暗号方式は大きく分けて公開鍵暗号と共通鍵暗号がある。公開鍵暗号は復号鍵を送信する必要がないが、暗号計算に時間がかかる。共通鍵暗号は暗号計算は速いが、暗号鍵と復号鍵が共通であるため、鍵を送る安全な伝送路が必要になる。これらの暗号方式は互いの長所に応じて使い分けられている。公開鍵暗号の一つとして楕円曲線暗号がある。これは従来の公開鍵暗号より短い鍵長で同程度の暗号強度をもつ。この暗号計算において誤り訂正などにも用いられる GF(2^m) 上の乗算が実行される。楕円曲線暗号で用いられる場合は m の値は数百といった大きな値である。この m の値が大きい乗算は計算時間が大きい演算であるため、専用回路の研究がされている。また、共通鍵暗号として米国暗号規格である AES 暗号が広く用いられている。AES 暗号の計算高速化のために、専用回路の研究がされている。この暗号計算において MixColumns 計算及び逆計算が実行される。また、公開鍵暗号と共通鍵暗号を組み合わせたハイブリッド暗号が広く用いられている。

本報告では、m の値が大きい GF(2^m) の乗算と AES 暗号における MixColumns 計算及び逆計算の共用回路を提案する。これらの別々の専用回路を合計した面積よりも、ほぼ同じ遅延で全体として小面積にすることを目的とする。提案回路は GF(2^m) 上の LSD 型ディジットシリアル乗算器を基に、GF(2^m) 上の乗算と MixColumns 計算及び逆計算を実行可能にする。ディジットシリアル乗算器は多項式基底における乗数と被乗数の部分積を D 個ずつ加算し、その和をレジスタに保存する。$\lceil m/D \rceil$ クロックですべての部分積を累算し、最後に $(m + D)$ ビットの累算結果を剰余計算する。

提案回路では、GF(2^8) の積和演算である MixColumns 計算及び逆計算を、従来のディジットシリアル乗算器における部分積加算部を変更することで実行する。これは m 個の部分積の計算順序を変更したものである。この変更により、部分積の和を保存するレジスタが大きくなるため、元にした乗算器では m 個の部分積を累算した後に実行していた剰余計算を、このレジスタに部分積の和を保存する前に実行することでこれを小さくする。また、AES 暗号はデータを分割して扱い、このデータすべてに MixColumns 計算及び逆計算を実行する必要がある。そこで提案回路では m の値が大きい GF(2^m) の乗算における被乗数のビット長が長いことを利用して、分割されたデータを複数入力する。これによって変更した部分積加算部において、複数の MixColumns 計算及び逆計算を並列に実行することができる。

楕円曲線暗号で用いる米国技術標準技術研究所で推奨されている m の値のうちに、$m = 233$ 及び 409 がある。評価を $m = 233$ 及び 409 の提案回路に対して行った。その結果、従来の MixColumns 計算及び逆計算の専用回路を別に追加した回路に比べて、レジスタが 15 ビット、EXOR ゲート数が $m = 233$ であれば 409 個、$m = 409$ であれば 703 個削減できる。また、どちらも GF(2^m) 上の乗算におけるクロックサイクル時間が EXOR ゲート 2 段分増加し、MixColumns 計算及び逆計算を実行するクリティカルパスのゲート段数が専用回路よりも AND ゲート 1 段増加する。以上の結果から、GF(2^m) の乗算と AES 暗号における MixColumn 計算の共用回路は別々に設計した専用回路を構成するよりもゲート数を減らすことが可能であり、両方の計算を使用する場合有用であるといえる。