平成１５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 克希
卒業研究題目	テーブルを用いた拡張ユークリッド法に基づく $\mathbf{GF}(2^m)$ 上の逆元算出アルゴリズム	

誤り訂正や公開鍵暗号などではガロア体 $\mathbf{GF}(2^m)$ が用いられており、特に公開鍵暗号で用いられる場合は m は数百といった大きな値となる。ガロア体 $\mathbf{GF}(2^m)$ 上の除算は他の演算に比べると計算時間が大きい演算であるため、逆元算出の高速化は重要な課題である。

本報告では、テーブルを用いた拡張ユークリッド法に基づく逆元算出アルゴリズムを提案する。提案アルゴリズムでは、拡張ユークリッド法に基づいた逆元算出アルゴリズムにおいて数回の反復で実行される演算を行列を用いて表現し、その行列をテーブルに保持しておく。そして、そのテーブルを用いることによって並列処理を行い、高速化を図る。従来の拡張ユークリッド法に基づいた逆元算出アルゴリズムでは、最上位ビットもしくは最下位ビットをチェックしてから演算を行なうという動作を繰り返す。一方、提案アルゴリズムでは、上位の数ビットを見ることによって、拡張ユークリッド法に基づいた逆元算出アルゴリズムにおける反復数回分の演算を並列に行うことができる。

提案アルゴリズムにおいて、従来の拡張ユークリッド法に基づいた逆元算出アルゴリズムでの反復 w 回分の演算を並列に行っていく場合、用いるテーブルのサイズはエントリ数が $(w+1)\cdot 2^{2w}$ で各エントリが $4\,(w+1)+\lceil \log_2(w+1)\rceil$ ビットとなる。ただし、w が偶数の場合はエントリ数を $(w/2+1)\cdot 2^{2w}$ に減らすことができる。並列処理が可能な演算を完全に並列に実行することができると仮定した場合、従来の拡張ユークリッド法に基づく逆元算出アルゴリズムの反復 w 回ではシフトが w 段、加算 (ビット単位の XOR) が最大で w 段必要となる。それに対し、提案アルゴリズムでは同様の演算をシフトが 2 段、加算が最大 $\lceil \log_2(w+1)\rceil+1$ 段で実行することができる。

発表実績

- 小林 克希, 高木 直史, 高木 一義, “テーブルを用いた拡張ユークリッド法に基づく $\mathbf{GF}(2^m)$ 上の逆元算出アルゴリズム”, 電子情報通信学会 総合大会, 2004 年 3 月 発表予定