報告番号	※甲　　第　　号

主　論　文　の　要　旨

論文題目　ガロア体GF(2^m)上の算術演算のハードウェア支援による実現に関する研究

氏　名　小林 克希

論　文　内　容　の　要　旨

ガロア体 GF(2^m) は、暗号や誤り訂正符号等の需要なアプリケーションに用いられている。それらのアプリケーションの高速実現のために、GF(2^m) 上の算術演算の効率的な実現が重要である。本論文では、GF(2^m) 上の算術演算の効率的な実現手法を3つ提案する。これらの手法は、高速化かつ低消費電力化のため、ハードウェア支援による実現という観点に基づいている。

本論文では、まず第2章において GF(2^m) 上の算術演算、拡張ユークリッド法、及びこれまでに提案されている GF(2^m) 上の逆元計算用のハードウェアアルゴリズムについて説明する。次に、第3章で GF(2) 上の多項式乗算命令を用いた実現に適した GF(2^m) 上の逆元計算のためのソフトウェアアルゴリズムを提案する。現在までに提案されている暗号向けの命令セット拡張の中で、楕円曲線暗号や AES 暗号向けのものは、、GF(2^m) 上の乗算の高速化のために GF(2) 上の多項式乗算命令を含んでいる。第3章で提案するアルゴリズムでは、従来提案されているアルゴリズムの連続する数反復分の計算を行列で表現し、その行列と GF(2) 上の多項式乗算命令で逆元計算の高速な実行を可能とする。プロセッサのワードサイズが 32 ビットかつ m の値が 571 であるとき、提案アルゴリズムは従来のアルゴリズムと比較して、GF(2) 上の多項式乗算命令と XOR 命令の個数が平均で半分程度となった。

第4章では、高速な GF(2^m) 上の除算回路設計のために、剰余計算の並列化によって高速化された除算ハードウェアアルゴリズムを提案する。このアルゴリズムでは、従来の除算ハードウェアアルゴリズムの2反復分の計算を1反復で実行するのと同時に、演算の順序を変更して2つの剰余計算を並列にすることによって高速に除算が可能となる。第4章で提案されるアルゴリズムに基づいた除算回路は、1サイクルの遅延は従来のものと同程度であるにも関わらず、必要なクロックサイクル数が従来提案されている回路の半分となる。論理合成により、提案アルゴリズム

の基づく回路の計算時間を見積ったところ、従来の除算回路と比較して35%以上小さかった。

第5章では、GF(2^m)上の乗算と逆元計算の複合回路設計のためのハードウェアアルゴリズムを提案する。楕円曲線暗号ではGF(2^m)上の乗算と逆元計算の両方が必要となるが、mの値が巨大であるため、両方の演算のための回路を実現すると面積が巨大となってしまう。そこで、回路のハードウェア量を削減するために、乗算と逆元計算のためのアルゴリズムの類似点に着目し、複合回路のためのアルゴリズムを設計した。このアルゴリズムに基づく回路では、乗算と逆元計算でほとんどのハードウェアが共用される。これまでに提案されている複合回路と比較しても、第5章で提案するアルゴリズムに基づく複合回路は面積が15%以上小さいという結果が論理合成によって得られた。

最後に、ハードウェア支援はGF(2^m)上の算術演算の効率的な実現に適するという結論を第6章にて述べる。また、アルゴリズムの類似性や並列化への着目が、回路の小面積化、高速化に有効であるといえる。本研究を通し得られた知見は、GF(2^m)上の算術演算はもちろん、他の重要なアプリケーションに必要な演算のハードウェア支援による実現の効率化に貢献すると期待できる。