先端科学技術研究科　修士論文要旨

所属研究室 （主指導教員）	情報セキュリティ工学 （林　優一 （教授））		
学籍番号	2011271	提出日	令和 4年 1月 21日
学生氏名	森本　康太		
論文題目	RNS表現を用いたペアリング計算におけるBEEAに適した逆元演算器の高エネルギー効率実装に関する研究		

要旨

近年IoTデバイスの利用拡大に伴い、人や機器への物理的な危害やプライバシデータの流出などの危険性が高まっており、安全かつ便利に使えるペアリング暗号が注目されている。しかし、ペアリング暗号は従来のRSA暗号などの暗号技術に比べて計算速度が遅いため普及を妨げている。特にIoTデバイスでは、計算リソースに制約があることから、エネルギー効率が重要な指標となる。RNS表現を用いた専用回路実装はエネルギー効率に優れているが、フェルマーの小定理を用いた逆元計算での剰余乗算がボトルネックとなっている。この解消には逆元計算に剰余乗算を必要としないBEEAを用いることが有用であると考えられるが、RNS表現では大小比較の計算コストが高いため、これを多用するBEEAはこれまで採用されていない。一方、大小比較の計算量を削減できる符号判定アルゴリズムが近年提案されており、BEEAを用いた逆元計算の高速化が見込まれるが、実際のアーキテクチャに対しては未検討である。本論文では、これまで適用されてこなかった新たな逆元計算アルゴリズムBEEAを既存のペアリング計算回路に適用することで、よりエネルギー効率に優れたペアリング計算回路を提案する。また、FPGAでの実装結果から既存のペアリング計算回路と性能比較を行う。