論文の内容の要旨

論文題目　Fast Computation Algorithms for Elliptic Curve Cryptosystem
(楕円曲線暗号系の高速演算法に関する研究)

氏名　小林　鉄太郎

本文
公開鍵暗号の実現には、落とし戸つき一方向性関数が必要であるが、従来、RSA 暗号・RSA 署名などの素因数分解問題に基づく方式が多く使われてきた。しかし、近年の計算機やネットワークの発達により、分散コンピューティングによる素因数分解アルゴリズムが進歩している。
このため、素因数分解問題以外に安全性の根拠をもつ暗号系として、楕円曲線暗号が注目されている。楕円曲線の離散対数問題の困難さに安全性の根拠を置く公開鍵暗号やデジタル署名は，小さい鍵サイズで従来と同等の安全性が確保できるという利点があり、特にメモリ・帯域が少ないモバイルコンピューティングの分野に適している。

また、楕円曲線に特有の写像である pairing 演算を用いることで ID ベース暗号や他者間鍵共有、ブロードバンド暗号などを効率よく実現することができる。

楕円曲線暗号方式である、楕円 DSA 署名や楕円 ElGamal 暗号などを実装する場合、楕円曲線上の点のスカラー倍演算が主な処理となる。この部分の高速化手法については、大きくわけて
　１、楕円曲線演算の回数の低減
　２、楕円曲線演算の高速化
　３、有限体上の演算の高速化
の３つからなる。
本論文では特に上記の３項目それぞれに着目し，その最適化方法を提案する。

また、pairing 演算は通常の楕円暗号に比べて複雑であり、演算コストが大きい。そのため演算高速化の必要性はより大きいといえる。本論文は、楕円曲線スカラー倍と同様に、pairing 演算の高速化方法を提案する。