楕円曲線暗号の効率的な実装に関する研究

永田　智芳 (0710902)

北陸先端科学技術大学院大学 情報科学研究科

2010 年 8 月 7 日

キーワード: 楕円曲線暗号，スカラー倍算，多倍長演算，OpenSSL，ARM.

楕円曲線暗号は小さな鍵サイズでも安全性が高く，処理速度が速く，消費電力が低く，メモリ使用量も少ないため，従来の暗号に比べて注目されている．楕円曲線暗号を効率的に実装するためには，楕円曲線上のスカラー倍算を高速に処理することが重要である．スカラーの大きさは多倍長で 160 ビット以上に及ぶため，多項式時間で計算することが不可欠であり，高速化の研究が進められてきた．

多項式時間で計算する方法は，Binary Method に始まり，Sliding Window 法，そしてオープンソースの暗号ライブラリである OpenSSL の楕円曲線ライブラリには，Interleaving Exponentiation と呼ばれる方法が採用されている．

どのようなスカラー倍算アルゴリズムであっても，内部で実行される演算は楕円加算と楕円２倍算である．楕円加算と楕円２倍算の計算量を少なくするための研究も進められており，最新の成果を利用することによって，OpenSSL のスカラー倍算は高速化することが可能である．

楕円加算と楕円２倍算の内部で実行される演算は，多倍長 mod 演算である．楕円曲線暗号で使用する定義体は，素数 p を法とする有限体であるから，高速な法演算を実行するためのアルゴリズムも研究されてきた．Incomplete Reduction という方法は，高速に Mod 演算を行なうために，ビット単位ではなく，ワード単位で計算を行なっている．Incomplete Reduction を導入することによって，楕円加算と楕円２倍算は高速化することが可能である．

多倍長 mod 演算の内部で実行される演算は，多倍長演算である．多倍長演算は何度も繰り返し実行されるため，その高速化がスカラー倍算の実行時間に与える影響は大きい．多倍長演算を高速化する方法として，条件分岐の削減や演算のマージが提案されている．既存研究では x86 プロセッサ上で実験を行なっているが，同様の方法を他のプロセッサにも応用することが可能である．特に ARM プロセッサは，携帯電話等の小型機器に実装されており，低消費電力，省メモリといった特徴を持つ楕円曲線暗号が力を発揮すべきプラットフォームである．

ARM9 を利用して多倍長演算の実験を行なったところ，多倍長２乗算の速度が遅いことが分かった．原因はメモリアクセスの回数が多いことであった．その問題を解決するために，ARM が得意とするシフト演算と，複数ワードのデータをまとめて転送する命令を利用し，演算のマージを提案する．提案方法はメモリアクセスの回数を８割近く削減し，実行速度を 20%以上高速化するという結果を得た．また，同じく ARM アーキテクチャを採用している iPhone において，提案方法を実験した．従来の実装に対して提案方法は，約 80%の高速化を達成した．さらに，最新の楕円加算と楕円２倍算の公式を使って，スカラー倍算を実行したところ，従来の方法に対して 63.09%の実行時間に短縮するという結果を得た．