4V-06

楕円曲線暗号におけるスカラー倍算の効率化

板場 千明† 木下 俊之‡

東京工科大学 バイオ・情報メディア研究科†
コンピュータサイエンス専攻

概要：現代の公開鍵暗号は解読までの時間が現実的でないことを安全性の根拠としているが、近年ではコンピュータの性能向上により解読時間が短縮され、従来の暗号強度では安全性が不十分になりつつある．そこで注目されているのが楕円曲線暗号である．従来の RSA と同程度の安全性を、より短い鍵長で実現できることが特徴である．楕円曲線暗号では、楕円曲線上の点 P のスカラー倍算が主演算として使われるため、スカラー倍算の効率化はそのまま楕円曲線暗号の効率化に繋がる．

スカラー倍算の効率化手法のひとつに、事前計算テーブル法がある．この方法は、メモリに余裕のあり鍵生成の度に楕円曲線を変更しない場合には効率が良い．本研究では、事前計算テーブル作成の速さを重視し、点 P の二倍点と三倍点を同時に求める Double-Triple 演算を主に用いた新しいテーブル作成法を提案する．

Chiaki Itaba† Toshiyuki Kinoshita†
Graduate School of Bionics, Computer and Media Science
School of Computer Science

Abstract

The elliptic curve cryptography is based on the addition and the subtraction of some points on an elliptic curve. The point obtained by repeating the addition and subtraction on the elliptic curve is called a scalar multiple point, and it is used as a key of the elliptic curve cryptography. The scalar multiplication is repeatedly used in the procedure sequence and is the most important calculation in the elliptic curve cryptography. We call scalar multiplication when the formula $Q=kP$ stands for two points P, Q on the elliptic curve and an integer k. Therefore, the speed-up of the scalar multiplication directly causes speed-up of the elliptic curve cryptography. when the elliptic curve and the base point are hardly changed, the scalar multiplication can be sped up by using the pre-calculation table.

In the this report, we propose a making algorithm of the pre-calculation table mainly using Double-Triple (DT) operation that does the double and triple multiplication at the same time.

1. はじめに

近年、コンピュータの性能が向上し、暗号解読時間が短縮され、RSA などの従来の公開鍵暗号では安全性が不十分になりつつある．そこで注目されているのが楕円曲線暗号である．楕円曲線暗号は公開鍵暗号の一種で、有限体上の楕円曲線による離散対数問題を用いることで一方向性を強めて、高い安全性を実現する．他の公開鍵暗号と比べて用いる数式は難解だが、より短い鍵長で同等の安全性を実現できるという利点がある．このため容量の少ない組み込みソフトなどでの活用も期待されている．

2. 背景

楕円曲線暗号は、加法公式を用いることで楕円曲線上の点の加減算が可能となる．この加法公式を繰り返すこと求めた点をスカラー倍点と呼ぶ．スカラー倍点は楕円曲線暗号においては鍵として利用され、復号化の度に頻繁にこの演算が使用される．このためスカラー倍算の効率化は、楕円曲線暗号における重要な課題となっている．

3. 楕円曲線と加法公式

素体 F_p 上で定義される次の式

$y^2=x^3+ax+b\ (a, b \in F_p)$

は Weierstrass 型の楕円曲線と呼ばれ、楕円曲線暗号に用いられる[4]．このとき 2 点 P, Q の加法公式は $R=P+Q$ で表され、以下の手順で求められる．まず楕円曲線上の 2 点 P, Q を通る直線 l と楕円曲線の交点を R'とする．交点がない場合は、R'は無限遠点とする．次に R'の x 軸に関する対称点を R とする．図 1 に加法公式の概要を示す．図はアフィン平面上で表しているため、R'と無限遠点を結ぶ直線と楕円曲線の交点が R となる．

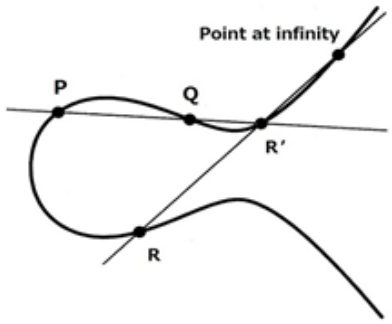

図 1　楕円曲線上の加法公式

4. 研究目的

スカラー倍算効率化の手法の一つに、事前計算テーブル法がある．これはスカラー倍算を予め計算して、テーブルに記憶して方法である。テーブルを作成する手間はかかるが、鍵生成の度に楕円曲線を変更しない場合には効率が良い．本研究は、事前計算テーブル作成を効率的に行う手法を提案する

5. LG 法

奇数倍点を効率よく求める事前テーブルの計算方法である[1]．最初に 3 倍点を求め、次に 2 倍の計算を繰り返し、これに Conjugate Addition 演算（以下 CADD、加算と減算を同時に求める演算）を適用して新しい奇数倍点を得る．偶数倍点や得られなかった奇数倍点は加法公式で求めてテーブルを完成させる．テーブルの最大奇数点が 2^n-1 倍点の場合、CADD だけで全ての奇数倍点を求められることが特徴である．図 2 に LG 法の概要を示す．図では初期の点を P とし、$\{P, 3P, \ldots, 13P\}$ を求めている．

6. PCAS 法

LG 法を改良した方法である[1]．CADD で求めた奇数倍点の中から 2 倍を繰り返す点を新しく設定し、事前テーブルの最大奇数点が 2^n-1 倍点でない場合でも、CADD のみで全ての奇数倍点を求めることができる．テーブルの最大点によっては LG 法と同じ結果になる場合もある．図 3 に PCAS 法の概要を示す．図では $\{P, 3P, \ldots, 27P\}$ を求めている．

7. 提案手法

Double-Triple 演算（以下 DT、2 倍点と 3 倍点を同時に求める演算）を用いることで、同時に多くの奇数倍点を求める方法である．最初に 3 倍点を求め、そこから DT を繰り返す．DT で得た 2 倍点から、CADD を用いて奇数倍点を求める．その他の点は加法公式で求めて、事前テーブルを完成させる．図 4 に提案手法の概要を示す．図では $\{P, 3P, \ldots, 27P\}$ を求めている．

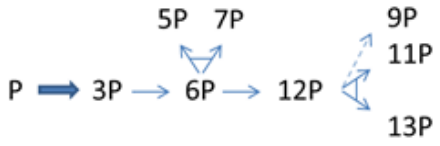

図 2　LG 法

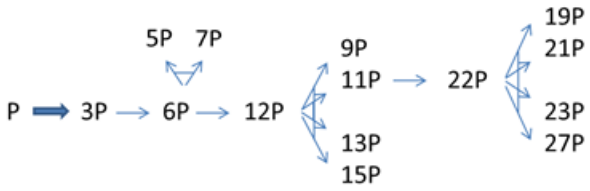

図 3　PCAS 法

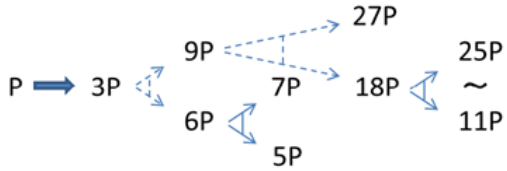

図 4　提案手法

8. まとめ

提案手法では、テーブル完成までの速度を重視している．しかし DT で求めた 3 倍点がテーブルの最大点を越えた場合に無駄な計算が発生してしまうなど、効率の面で改善の余地がある．今後の課題として、既存手法を組み合わせることでより効率的な方法を提案する．

[参考文献]

[1] 高橋良太，宮地充子，“Perfect Conjugate Addition Sequence を用いた新たな事前計算テーブル計算手法について”，信学技報 2014 年 7 月
[2] 三宅秀享，宮地充子，“楕円曲線暗号におけるスカラー倍算の高速化に関する考察”，信学技報 2002 年 3 月
[3] 笹原大地，宮地充子，“効率的な 3 倍算公式を用いたスカラー倍手法の提案”，情報処理学会研究報告 2010 年 12 月
[4] J.H.シルヴァーマン，J.テイト，“楕円曲線論入門，”丸善出版，1995 年 11 月
[5] 有田正剛，境隆一，只木孝太郎，趙晋輝，松尾和人,“暗号理論と楕円曲線—数学的土壌の上に花開く暗号技術—”，森北出版、2008 年 9 月
[6] 中村次男，笠原宏，“暗号の仕組みと実装”，日本理工出版，2009 年 6 月
[7] 宮地充子，“代数学から学ぶ暗号理論—整数論の基礎から楕円曲線暗号の実装まで—”，日本評論社，2012 年 3 月
[8] 日立製作所，“楕円曲線暗号における事前計算テーブル作成装置”，特許公報 2006 年 2 月