新しい演算を導入した楕円曲線暗号の検証

b1014195 大谷笙互
指導教員 :白勢正明

Verification of Elliptic Curve Cryptography Introduced New Operation

Shogo Otani

概要 : 楕円曲線暗号とは，現在最も主流な公開鍵暗号である．楕円曲線暗号は RSA 暗号に比べて，短い鍵長で同等の安全性を持つことが知られている [1]．暗号技術において，鍵長が短くなればなるほど暗号処理の速度が速くなるが安全性が低下する．安全性を保ったままより短い鍵長で暗号技術を実現することが重要である．由良は，有限体上 M 関数 ($M : \mathbb{F}_p \times \mathbb{F}_p \to \mathbb{F}_p$) を定義した [2]．白勢は，これを有限体上楕円曲線へと拡張した．白勢は Me 関数 ($Me : E(\mathbb{F}_p) \times E(\mathbb{F}_p) \to E(\mathbb{F}_p)$) や Me 関数の繰り返しである Me-スカラー倍を定義し，暗号プロトコルへの応用を考察した [3][4]．本研究では，Me 関数を使った有限体上楕円曲線が暗号プロトコルの正当性と，処理速度を実験的に検証する．

キーワード : 楕円曲線暗号，公開鍵暗号，新しい演算

Abstract: Elliptic Curve Cryptography is the most current Public-key cryptography. It is known that Elliptic Curve Cryptography has equivalent security with $\mathbb{F}_p$ shorter key length than RSA[1]. The shorter key length is, the faster the speed of encryption processing and less the safety is. It is important to realize encryption technology with shorter key while maintaining safety. Yura defined M-function($M : \mathbb{F}_p \times \mathbb{F}_p \to \mathbb{F}_p$) on a finite field[2]. Shirase expanded this into a elliptic curve on a finite field. Shirase defined Me-function($Me : E(\mathbb{F}_p) \times E(\mathbb{F}_p) \to E(\mathbb{F}_p)$) and Me-scholar multiplication which is repetition of Me-function, considered applying to cryptographic protocols[3][4]. This article experimentally verifies correctness and processing speed of cryptographic protocols of elliptic curve on a finite field.

Keywords: Elliptic Curve Cryptography, Public-key cryptography, New Operation

1 研究背景

1985 年頃に発明された楕円曲線暗号という暗号技術がある．楕円曲線暗号とは, 楕円曲線上の離散対数問題の計算困難性によって安全性を保証している公開鍵暗号である．また, 発明当時主流であった RSA 暗号に比べ, 短い鍵長で同等の安全性を持つことが知られている [1]．そのため，SSL/TLS 通信における鍵共有や電子署名で広く使われている．現在の TLS の最新バージョンは 1.2 であるが，現在バージョン 1.3 の仕様策定が進んでいる．バージョン 1.3 では Forward Secrecy が導入されることがわかっている．Forward Secrecy とは，長期鍵 (long-term key) が暴かれたとしても過去のセッションキーの性質が失われないことを示す性質のことである．ここで，従来から使われている RSA 暗号による鍵共有は Forward Secrecy の性質を満たさないことが知られている．それに伴い，TLS 1.3 以降は RSA 暗号による鍵共有が廃止される予定である．これにより，楕円曲線暗号がさらに広く使われることが想定される．また，楕円曲線暗号において，より鍵長を短くする研究や暗号処理を高速化する研究が行われていて，より良い暗号技術への研究がされている．白勢によって定義された楕円曲線の新しい演算 $\oplus$ を用いた暗号プロトコルについても，その正当性や暗号処理速度を検証する必要がある．

2 目的と目標

2.1 目的

本研究は，楕円曲線の新しい演算 $\oplus$ が暗号プロトコルとして実際に使えるものかどうか検証することを目的とする．

2.2 目標

本研究の目標は，暗号を検証するプログラムを実装することである．そして検証プログラムを用いて実際に暗号プロトコルとしての正当性を実験的に確認する．次に，異なる鍵長を用いて暗号処理速度を調査をする．

3 楕円曲線

3.1 有限体上 $\mathbb{F}_p$

p を素数とすると，集合 $\mathbb{F}_p = \{0, 1, ...p-1\}$ は有限体になることが知られている．つまり，$\mathbb{F}_p$ の要素間で四則演算ができる．

3.2 楕円曲線

楕円曲線とは，無限遠点 $O = (\infty, \infty)$ を含む非特異な 3 次曲線であり，素体 $\mathbb{F}_p$ 上の楕円曲線は次の方程式で示される．

$$y^2 = x^3 + ax + b (a, b \in \mathbb{F}_p, \Delta_E = 4a^3 + 27b^2 \neq 0)$$

この式は Weierstrass 標準形と呼ばれている．

3.3 楕円曲線の加算

楕円曲線上の有理点同士は加算や減算ができ，次のように定義される．
2 点 $P, Q \in \mathrm{E}$ とする．次に，P, Q を通る直線を L とするとする．E と L の P, Q ではないもう一つの交点を $P * Q$ とする．このとき，$P * Q$ の x 軸に対称な点を $P + Q$ と定義する (Fig.1)．

3.4 楕円曲線のスカラー倍

楕円曲線上の点 P と整数 n に対して，スカラー倍は

$$nP = \underbrace{P + P + \cdots + P}_{n \text{ 個}}$$

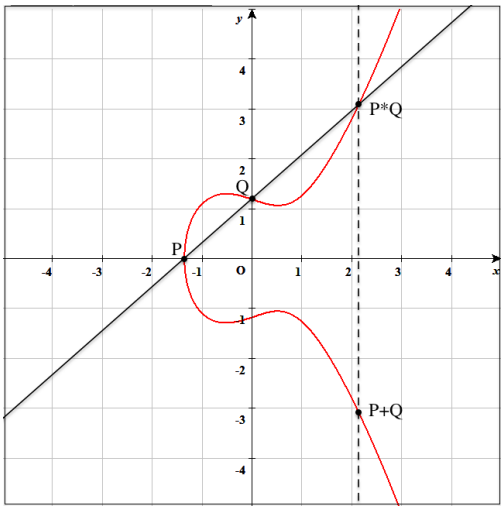

Fig. 1 楕円曲線のグラフ

と定義される．スカラー倍算は加算の繰り返しによって実装される．実装方法としてよく用いられているのはバイナリ法である．Table 1 にそのアルゴリズムを記す．

Table 1 バイナリ法

アルゴリズム 1
入力：$P \in \mathbb{F}_p$, $n = (1, n_{l-2}...n_0)_2 \in \mathbb{N}$ 出力： $Q \in \mathbb{F}_p$
1. $Q = P$ 2. for $i = l - 2$ down to 0 3. $Q = Q + Q$ 4. if $n_i = 1$ then $Q = Q + P$ 5. end for 6. return Q

このとき，P と nP から n を求めるような問題は楕円曲線離散対数問題 (ECDLP) と呼ばれており，ECDLP を解くことは困難であるという性質を利用した暗号が楕円曲線暗号である．

4 楕円曲線暗号

楕円曲線暗号の一つである ECElGamal 暗号を例に説明する．ECElGamal 暗号は鍵生成，暗号化，復号の 3 つのステップによって実現されている公開鍵暗号方式である．以下に ECElGamal 暗号のアルゴリズムを記す．

Table 2 ECElGamal 暗号の鍵生成

アルゴリズム 2
入力：素数位数 l のベースポイント $G \in E(\mathbb{F}_p)$
出力：公開鍵 Y，秘密鍵 x
1. 乱数 $x \in \mathbb{Z}_l$ を生成する
2. $Y \leftarrow xG$
3. return Y，x

Table 3 ECElGamal 暗号の暗号化

アルゴリズム 3
入力：平文 m，公開鍵 Y
素数位数 l のベースポイント $G \in E(\mathbb{F}_p)$
出力：暗号文 (U, c)
1. 乱数 $r \in \mathbb{Z}_l^*$ を生成する
2. $U = (u_x, u_y) \leftarrow rG$
3. $V = (v_x, v_y) \leftarrow rY$
4. $c \leftarrow v_x$ XOR m
5. return (U, c)

Table 4 ECElGamal 暗号の復号

アルゴリズム 4
入力： 暗号文 (U, c)，秘密鍵 x
素数位数 l のベースポイント $G \in E(\mathbb{F}_p)$
出力：メッセージ m
1. $V = (v_x, v_y) \leftarrow xU$
2. $m \leftarrow v_x$ XOR c
3. return m

5 有限体上 Me 関数

5.1 Me 関数

Me 関数は以下のように定義される [3].

- $P = Q$ のとき
  - $P = Q = P \oplus P = P$
- $P \neq Q$ のとき
  - $P \oplus Q = 2P - Q$
    ($P - Q$ の y 座標が平方元のとき)
  - $P \oplus Q = 2Q - P$
    ($P - Q$ の y 座標が非平方元のとき)

5.2 Me-スカラー倍

Me 関数を暗号プロトコルで使う場合には，Me 関数によるスカラー倍の類似を定義する必要がある．従来のスカラー倍算は,

$$nP = \underbrace{P + P + \cdots + P}_{n \text{ 個}}$$

と表される．しかし，Me 関数で考えると,

$$nP = \underbrace{P \oplus P \oplus \cdots \oplus P}_{n \text{ 個}} = P$$

となり，スカラー倍算は意味をなさない．そこで，補助元 Z を指定して，アルゴリズム 5 の出力を Me スカラー倍と定義する．

Table 5 Me-スカラー倍の計算方法

アルゴリズム 5
入力：$P \in \mathbb{F}_p$，$Z \in \mathbb{F}_p$，$n = (n_{l-1}...n_0)_2 \in \mathbb{N}$
出力： $Q_{n,z,1}$ or $Q_{n,z,2} \in \mathbb{F}_p$
1. $Q = P$
2. for $i = l - 2$ down to 0
3. $Q = (Z + Q) \oplus Q$ (タイプ 1) $Q = (Z \oplus Q) \oplus Q$ (タイプ 2)
4. if $n_i = 1$ then $Q = Q \oplus P$
5. end for
6. return Q

従来の ECDLP の類似として，Me スカラー倍を $Q, Z, Q_{n,z,1}$ から n を求める問題を MeDLP と定義する．MeDLP が困難ならば，従来のスカラー倍を Me-スカラー倍に置き換えた暗号系を考えることができる．本研究では，それを実装し暗号プロトコルとしての正当性を確かめ，処理速度を比較する．

MeDLP の困難性の検証は不十分であるが，列 $\{Q_{n,z,1} : n = 1, 2, 3\cdots\}$ は周期性を持たないと考えられているため，[4]

1. MeDLP を解く量子アルゴリズムが存在しない
2. 誕生日攻撃を適用できない

である可能性がある．

特に，2 が正しい場合，鍵長を半分にできる．よって，処理速度を図る実験では鍵長に 128bit や 256bit のものを用いる．

6 実験

実験に使用するプログラムの作成には PARI/GP を用いる．PARI/GP とは，高速に演算を行う関数を持つ PARI という C 言語ライブラリと，対話型に動作するコマンドラインインタフェースのプログラムである gp からなる．まずは実装したプログラムに様々なパラメータを与えて暗号処理をすることで，暗号処理の正当性を検証する．暗号処理の正当性が確認できたならば，暗号処理時間を比較実験する．

7 評価手法

7.1 暗号プロトコルとしての正当性

第一に，Me-スカラー倍算を用いた有限体上楕円曲線暗号が暗号プロトコルとして実用可能かどうか評価する．評価基準としては，ランダムに生成した乱数について Me-スカラー倍算を行い実際に演算が行われているかどうか検証する．

7.2 暗号処理速度

第二に，従来のスカラー倍算の手法と Me-スカラー倍算の手法の両方のアルゴリズムを同じ環境で実行する．それぞれのプログラムで 128bit と 256bit の鍵長を用いることによって生じる 4 種類の結果を記録しその速度差を比較する．

8 展望

現在，暗号プロトコルとしての実用可能性を評価するためのプログラムを作成中である．これが完成次第，実験に取り掛かる．また，それと並行して，暗号処理速度について評価できるプログラムを作成する．

9 結言

本研究では Me-スカラー倍を用いた楕円曲線暗号が暗号プロトコルとして実用可能かどうか，またその処理速度や周期性について検証する．結果によっては従来の楕円曲線暗号から大きく進歩した暗号プロトコルになる可能性があるため，今後も検証が必要である．

参考文献

[1] 安田雅哉 (やすだまさや), 伊豆哲也 (いずてつや), 下山武司 (しもやまたけし), 小暮淳 (こぐれじゅん). 楕円曲線暗号の攻撃評価. 情報処理学会創立 50 周年記念 (第 72 回) 全国大会．3-569，570. 2010.

[2] 由良文孝 (ゆらふみたか). 有限体上のソリトン方程式における入れ子構造を持つソリトン解について 日本応用数理学会論文誌．Vol．24，No．4，2014，pp．317 336.

[3] 白勢政明 (しらせまさあき). 有限体上 M 関数を用いた M-スカラー倍算の提案とその性質及び応用

[4] 白勢政明 (しらせまさあき). 有限体上 M 関数の有限体上楕円曲線へ拡張とその応用