新しい演算を導入した楕円曲線暗号の実装

Implementation of Elliptic Curve Cryptography Introduced New Operation

1014195　大谷笙互　Shogo Otani

指導教員　白勢政明

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．発明当時主流であった RSA 暗号に比べ，短い鍵長で高い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ビットコインの電子署名で広く普及している．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．しかし，量子コンピュータ[*1]の開発により，その安全性には疑問が呈されている．アメリカ国立標準技術研究所 (NIST) によると，量子コンピュータの開発により今後 20 年間で楕円曲線暗号の安全性が崩壊すると言われている [2]．これに対して，量子コンピュータの攻撃に耐えることのできるような，新しいアプローチでの暗号に関しての研究が盛んである．現在盛んな二つの暗号として，格子暗号と多変数暗号がある．しかし，どれも実用に足るものではなく，新たなアプローチの暗号技術が求められている．

2　目的

本研究の目的は，楕円曲線暗号に新たな演算を導入して改良することである．改良したものが暗号処理を正確に行うことができるかどうか検証する．楕円曲線を改良するアプローチには様々な階層がある．基礎的なものから順に，多倍長の計算，有限体上の計算，楕円曲線の式，加算・2 倍算，スカラー倍である．本研究では，加算・2 倍算，及びスカラー倍の階層に改良を加える．

[*1] 量子力学的な重ね合わせを実装したコンピュータで，離散対数問題を簡単に解くことができると言われている．

3　提案

スカラー倍算を改良するにあたり，新たな演算手法を定義する．本研究では，由良によって定義された M 関数を用いる [3]．これを楕円曲線上の 2 点 P, Q に置き換え，整理すると，以下のように再定義することができる [4].

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

次に，この M 関数を用いたスカラー倍算を考える．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，M 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，ベース Z を指定して,

$$(Z + P) \oplus P \tag{1}$$
$$(Z \oplus P) \oplus P \tag{2}$$

を計算する．これにより，$\oplus$ を用いたスカラー倍を実現し，M-スカラー倍と名付ける．この考えに基づき，M-スカラー倍を用いた暗号を実装する．

4　実装方法

実装方法としては，バイナリ法を参考にする．バイナリ法を用いたスカラー倍算を表 1 に記す．また，M-スカラー倍算を用いたアルゴリズムに改良したものを表 2 に記す．また (1) を用いた計算をタイプ 1 とし，出力を $Q_{n,z,1}$ とする．同様に，(2) はタイプ 2 として $Q_{n,z,2}$ とする．

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

表 1　バイナリ法

アルゴリズム 1
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

表 2　M-スカラー倍を用いたバイナリ法

5　展望

本研究で検証はしないものの，M-スカラー倍算を用いた暗号では大きく 2 つのメリットがあると推測される．1 つ目は，従来の楕円曲線暗号と比較してさらに半分の鍵長で楕円曲線暗号と同等の安全性を得ることができることである．従来の楕円曲線暗号の攻撃方法 (離散対数問題の計算方法) として有名な方法に，ρ 法がある．ρ 法とは，楕円曲線暗号の周期性を利用している．しかし，M-スカラー倍算を用いた暗号には周期性がないことが予測されている．よって，さらに半分の鍵長になることが期待される．2 つ目は，量子コンピュータによる攻撃にも耐えることのできる，耐量子暗号になるということである．楕円曲線暗号が量子コンピュータの開発で安全性が保証されなくなる理由は，離散対数問題を簡単に求めることができる量子アルゴリズムが発見されたためである [5]．M-スカラー倍算を用いた暗号は，この量子アルゴリズムに当てはまらないので，耐量子暗号になる可能性を持っている．

6　評価手法

本研究の評価手法として，まずは M スカラー倍算を用いた暗号を実装する．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，暗号処理を正確に行なっているかどうか検証する．

7　研究の経過

これまでの研究の経過としては，4，5 月に暗号に関する基礎研究を行った．6 月には M 関数及び M-スカラー倍の理解に努め，それと同時に卒業研究のテーマを確定した．7 月には楕円曲線暗号の実装を開始した．実装には，PARI/GP という計算機代数アプリケーションを用いた．PARI とは，C 言語のライブラリである．GP とは，対話型に動作するコマンドラインインタフェースである．しかし，M-スカラー倍算を用いた暗号は PARI/GP では実装が難しいことがわかり，現在 C 言語での実装に取り組んでいる．

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] Report on Post-Quantum Cryptography. NIST Interagency Report 8105．April，2016.

[3] 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.

[4] 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9 月発表予定.

[5] P．W．Shor．Algorithms for quantum computation: Discrete log and factoring．Proc．of the 35th Annual IEEE Symp．on Foundations of Computer Science，pp.124-134，1994.