BN 曲線決定方法の効率について

小林 真理子

1　はじめに

近年、通信やメール等の暗号化のために公開鍵暗号を用いるようになってきた。最近では、特に楕円曲線上のペアリング写像を用いるペアリング暗号が注目されている。ペアリング写像とは、楕円曲線の 2 点から有限体の元へ双線形写像である。ペアリング暗号により、ID 情報を公開鍵にできる ID ベース暗号、地位や所属のような属性情報を公開鍵にできる属性ベース暗号、復号の時刻を指定できるタイムリリース暗号等のこれまでは実現が困難であった新しい暗号方式が実現されている。ペアリング暗号には効率的なペアリングを持つ楕円曲線を利用する必要がある。有限体 $\mathbb{F}_p$ 上の楕円曲線が効率的なペアリング写像を持つためには

1. 位数 $\#E(\mathbb{F}_p)$ が大きな素数 r を因子に持つ
2. $r|p^k-1$ を満たす最小の正整数 k が適切な値
3. $\rho = \log p/\log r$ が 1 に近い

が必要である。例えば現状の標準的なセキュリティレベルである 128 ビットセキュリティのペアリング暗号に最適な k は $k=12$ であり、$r \approx 256$ である。一般に k は非常に大きな値となり、上記条件を満足する曲線を発見するのは困難な課題である。$k=12$ を持つペアリング暗号に適した楕円曲線の構成法を Barreto と Naehrig [1] が提案している。この方法によって構成された楕円曲線を BN 曲線と呼ぶ。BN 楕円曲線は $E_b : y^2 = x^3 + b$ という形式をしているが、構成法にしたがって得られた $\mathbb{F}_p$ 上で $b \in \mathbb{F}_p$ の値をランダム選ぶと、1/6 の確率で BN 楕円曲線となる。BN 曲線となる b の値は数回の試行錯誤によって決定可能であるが、これとは別に白勢 [4] は $b = 2^i 3^j \in \mathbb{F}_p$ の場合の (i,j) に対する $\#E(\mathbb{F}_p)$ の表を与えた。この表を用いることでより効率的に BN 曲線となる b を決定可能であると考えられる。そこで本研究では従来の b の決定法と白勢法を実装し、実験によりその効率を比較する。

2　BN 楕円曲線

本節では BN 楕円曲線を定義する。$z \in \mathbb{Z}$ に対して

$$p = 36z^4 + 36z^3 + 24z^2 + 6z + 1$$

が素数になるとき、p を BN 素数という。この p を位数とする有限体 $\mathbb{F}_p$ 上の楕円曲線

$$E_b : y^2 = x^3 + b,\ b \in \mathbb{F}_p$$

をランダムに選択すると曲線の位数が 1/6 の確率で z を用い

$$\#E(\mathbb{F}_p) = n = 36z^4 + 36z^3 + 18z^2 + 6z + 1$$

となる。このとき n を BN 位数、E_b を BN 楕円曲線という。BN 楕円曲線は $k=12$ となる。

本研究では、まず $z=5$ として b を小さい数値から順に当てはめて位数 $\#E(\mathbb{F}_p)$ を観察した。ここで、$p = 36z^4+36z^3+24z^2+6z+1 = 27631$, $n = 36z^4+36z^3+18z^2+6z+1 = 27481$ である。

b を 1 から 30 まで試していくと、楕円曲線 $y^2 = x^3 + b$ の位数は以下のような結果となる。

$\#E(\mathbb{F}_p)$	b
27300	$1, 8, 9, 10, 11$
27451	$7, 12, 15$
27481	$6, 17, 23, 26, 28$
27783	$2, 16, 18, 20, 22, 25, 29$
27813	$4, 5, 21$
27964	$3, 13, 14, 19, 24, 27, 30$

上記結果では、6 種類の位数が出現している。全ての b について位数を確認すれば、それぞれの位数に対する b の数は同じになり、BN 曲線になる b の確率は 1/6 となる。この結果から、BN 曲線となる確率だけでなく、楕円曲線の位数が 6 通りあることが見てとれるが、実際に位数は z に対して以下の 6 通りあることが分かっている。

$$\begin{cases} n_0 = n_0(z) = 12z^2(3z^2+3z+1) \\ n_1 = n_1(z) = 36z^4+36z^3+18z^2+1 \\ n_2 = n_2(z) = 3(12z^4+12z^3+10z^2+2z+1) \\ n_3 = n_3(z) = 4(9z^4++9z^3+9z^2+3z+1) \\ n_4 = n_4(z) = 3(12z^4+12z^3+10z^2+4z+1) \\ n_5 = n_5(z) = 36z^4+36z^3+18z^2+6z+1 \end{cases}$$

上記の式を実験で確かめた数値と同じであるかを $z=5$ として確認する。まず、n_5 は BN 位数であり 27481 となる。また、n_0 から n_4 に対しても以下の通りになる。

$$\begin{cases} n_0 = n_0(5) = 27300 \\ n_1 = n_1(5) = 27451 \\ n_2 = n_2(5) = 27783 \\ n_3 = n_3(5) = 27964 \\ n_4 = n_4(5) = 27813 \\ n_5 = n_5(5) = 27481 \end{cases}$$

これにより、その他の位数の式もそれぞれ実験結果と一致することが理解できる。

3　BN 楕円曲線の構成

ここでは、BN 曲線の構成法を説明する。BN 曲線を構成するには z をランダムに選択し、対応する p が素数であるかどうかを判定する。素数であれば、p は BN 素数になるので $\mathbb{F}_p$ 上で BN 曲線を得ることができる。もし素数でない場合には、z を選び直す。また、実際には暗号の安全性に対する要請から p のみならず n も素数になるように z を選択する。z のサイズは p の式から必要な p のサイズの 1/4 程度に取ればよいことが分かる。Algorithm 1 に BN 曲線の構成法を示す。Algorithm 1 では p, n, z を求めているが、対応する BN 曲線 E_b を求めていない。E_b の構成法は次節で示す。

Algorithm 1 BN 素数と BN 位数

Input: p のビット数 N
Output: p, n, z
  while true do
    $z \in [1, 2^{N/4}]$ をランダムに選択
    $p \leftarrow 36z^4 + 36z^3 + 24z^2 + 6z + 1$
    $n \leftarrow 36z^4 + 36z^3 + 18z^2 + 6z + 1$
    if p と n が素数 **then**
      p, n, z を出力

4　BN 楕円曲線の b の値の決定

Algorithm 1 で得られた p, n, z に対して $\mathbb{F}_p$ 上の E_b を考えると、E_b が BN 曲線のとき任意の有理点 $P \in E_b(\mathbb{F}_p)$ に対して $nP = O$ を満足する。ここで、O は E_b の無限遠点である。一方、p が十分に大きいときには、E_b が BN 曲線でないとき $nP = O$ を満足する点は O 以外には存在しない。そこで、BN 曲線を構成する b を Algorithm 2 によって構成可能である。Algorithm 2 のループ回数は平均 6 回であるが、停止しない可能性もある。

Algorithm 2 BN 楕円曲線 (従来法)

Input: p, n
Output: b
  while true do
    $b \in \mathbb{F}_p$ をランダムに選択
    $E_b \leftarrow$ 楕円曲線 $y^2 = x^3 + b$
    E_b 上の有理点 $P \in E(\mathbb{F}_p) \setminus \{O\}$ をランダムに選択
    if $nP = O$ **then**
      b を出力

Algorithm 2 とは別に、白勢 [4] の求めた位数表を用いて b を求めることができる。Algorithm 3 にその方法を示す。白勢法はパラメータ z の法 36 における値によって BN 楕円曲線となるか判断する。これにより 36 通りの場合分けだけで結果を得ることができるため高速に計算可能であると期待される。しかし、この方法では b の値を決められない場合がある。

5　実験

実験により Algorithm 2, 3 の効率を比較した、実験には Core i7-5930K 3.5GHz 上の Sage を利用した。

実験は 256 ビットと 512 ビットの p に対して行った。各ビット 10 個の異なる p に対して実験を行なった。p の値に関しては Algorithm 1 を用いて計算した。表 1 に 10 個の異なる p に対する平均時間を示す。

	従来法	白勢法
256 ビット	$279.47ms$	$90.17\mu s$
512 ビット	$2.84s$	$80.61\mu s$

表 1: 従来法と白勢法の比較

従来法と白勢法による 256 ビットと 512 ビットの平均時間から効率を比較する。表 1 から白勢法の方が計測時間が速く、効率化されていることがわかる。256 ビットでは白勢法が 3.1×10^3 倍速く BN 曲線を見つけることができる。512 ビットでは白勢法が 3.5×10^4 倍速くなる。白勢法では、ビット数を増やしても計測時間はほとんど変わらないが、従来法はビット数が増えると計測時間もかかってしまう。結果から白勢法の方が効率的である。

Algorithm 3 白勢法

Input: z
Output: b
  $zl \leftarrow z \pmod{36}$
  if $zl = 2, 11, 14, 23, 26, 35$ **then**
    $b = 2$
  else if $zl = 3, 13, 17, 21$ **then**
    $b = 3$
  else if $zl = 5, 25, 30$ **then**
    $b = 6$
  else if $zl = 1, 29$ **then**
    $b = 12$
  else if $zl = 6, 15$ **then**
    $b = 18$
  else if $zl = 7, 10, 19, 22, 31, 34$ **then**
    $b = 32$
  else if $zl = 33$ **then**
    $b = 243, 486, 972, 1944, 3888, 7776$
  else if $zl = 34$ **then**
    $b = 32$
  else if $zl = 0, 4, 8, 9, 12, 16, 18, 20, 24, 27, 28, 32$ **then**
    b の値を決定できない

6　まとめ

本稿では、楕円曲線の構成の効率化に対して従来の BN 楕円曲線の構成と白勢法を比較した。結果として、従来法は白勢法よりも時間がかかることがわかった。従来法は有理点をランダムに選択して BN 曲線となる値を探索しているため、ビット数が増えると計測時間もかかってしまう。白勢法はパラメータを mod 36 とした結果によって BN 曲線であるか判断している。これにより 36 通りから当てはまる BN 曲線を探索するため、ビット数を変えても計測時間はほとんど変わらない結果となった。比較から白勢法が BN 曲線の構成の効率化となる。しかしながら、白勢法は楕円曲線の b の値を決定できない場合がある。このことから従来法も使う必要がある。

参考文献

[1] P. Barreto, M. Naehrig,“Pairing-friendly elliptic curves of prime order,” SAC 2005, LNCS 3897，pp.319-331，2006.

[2] K. Rubin, A. Silverberg,“Choosing the Correct Elliptic Curve in the CM Method,” Math. Comp., 79，pp.545-561，2010.

[3] W. Stein, ”Elementary Number Theory: Primes, Congruences, and Secrets,” Springer，2009.

[4] 白勢政明,“Barreto-Naehrig 体上の楕円曲線 $y^2 = x^3 + 2^i 3^j$ の位数,” 信学技報 ISEC2011-6，pp.37-44，2011.

[5] イアン・F・ブラケ、ガディエル・セロッシ、ナイジェル・P・スマート、鈴木治郎 (訳),「楕円曲線暗号」, Pearson Education Japan，2001 年.

[6] 佐々木良一 (監修)、手塚悟 (編著)、白勢政明 (第 4 章),「情報セキュリティの基礎」, 共立出版，2011 年.