称号及び氏名	博士（理学）　小牟田　綾
学位授与の日付	平成 22 年 3 月 31 日
論　文　名	「Pairing-based cryptography and construction of pairing-friendly elliptic and hyperelliptic curves (ペアリング暗号とペアリングフレンドリ楕円・超楕円曲線の構成)」
論文審査委員	主査　高橋　哲也 副査　石井　伸郎 副査　馬野　元秀

論文要旨

p を素数, C を $\mathbb{F}_p$ 上定義された種数 g の超楕円曲線, J_C を C のヤコビ多様体, $J_C(\mathbb{F}_p)$ をヤコビ群, $J_C[\ell]$ を ℓ-ねじれ点のなす J_C の部分群とする. J_C 上の Weil pairing は次のような双線形・非退化写像である.

$$e_\ell : J_C[\ell] \times J_C[\ell] \to \mu_\ell \subset \overline{\mathbb{F}}_p^*.$$

ここで, ℓ は素数, は μ_ℓ は 1 の ℓ 乗根全体のなす部分群である. また, $\mu_\ell \subset \mathbb{F}_{p^k}^*$ となるような, 最小の拡大次数 k を ℓ に関する埋め込み次数という.

1984 年に Shamir により ID 情報を公開鍵とする Identity-based Encryption (IBE) が提案され, 2001 年に Boneh と Franklin により Weil pairing を用いて IBE を効率よく実現するプロトコルが提案された. それから, Pairing-based cryptosytem (PBC) が注目され, 様々な安全性根拠に基づく暗号方式が多く提案されるようになった. 同時に, PBC に適した曲線の構成が必要となった. その安全性を保証するために次の条件が必要である.

1. $J_C(\mathbb{F}_p)$ の素数位数部分群の位数 ℓ が適度に大きく, $J_C[\ell]$ 離散対数問題が計算困難であること.
2. p^k が適度に大きく, $\mathbb{F}_{p^k}^*$ 上の離散対数問題が計算困難であること.

また, 実装の観点から,

3. 埋め込み次数 k が適切に小さいこと.
4. $\rho = g \log p / \log \ell$ が適切に小さいこと.

という条件を満たすことが求められる. これらの条件を満たす曲線を pairing-friendly という.

$\chi(t)$ を C の p-乗 Frobenius 写像の特性多項式としたとき, J_C が ℓ に関する埋め込み次数 $k(>1)$ を持つための条件は

$$\chi(1) \equiv 0 \pmod{\ell}$$
$$\Phi_k(q) \equiv 0 \pmod{\ell}$$

である.

pairing-friendly 曲線の構成法に関する既存の研究には, 楕円曲線については Miyaji らによる MNT 曲線, Cocks-Pinch 法, Brezing-Weng 法, Freeman らによる cyclotomic family などがある. 超楕円曲線については, Freeman らの構成法 Kawazoe, Takahashi らの構成法がある. Freeman らは, 任意の埋め込み次数に対する種数 2 の pairing-friendly 超楕円曲線の構成を与えている. ρ 値は 8 程度である. また, 種数 2 の場合は, ある埋め込み次数に関しては, $6 \le \rho < 8$ を達成している. Kawazoe らの構成法では, $y^2 = x^5 + cx$ のタイプの種数 2 の超楕円曲線のヤコビ群の explicit な公式を与えその構成法は任意の埋め込み次数に対して $3 \le \rho \le 4$ の構成法である. しかしながら, absolutely simple ではない. このように, 超楕円曲線に関しては, 構成法が少ない.

本論文では
1. Cheon の攻撃アルゴリズムを考慮した pairing-friendly 楕円曲線の構成法
2. $y^2 = x^5 + c$, $y^2 = x^9 + cx$ のタイプの超楕円曲線の位数公式を用いた pairing-friendly な超楕円曲線の構成法について述べている.

2002 年に Mitsunari らにより, q-weak Diffie-Hellman 問題に基づいた traitor tracing scheme が提案された. また, 2004 年に Boneh と Boyen は, q-strong Diffie-Hellman 問題に基づいた short signature scheme を提案した. どちらの scheme も pairing 写像を用いている. 2006 年に, Cheon は q-weak/strong Diffie-Hellman 問題を効率よく解くアルゴリズムを提案した. このアルゴリズムは, 楕円曲線の部分群の位数を ℓ としたとき, $\ell - 1$ または $\ell + 1$ の因子を用いた攻撃法である. また, 2007 年に Kozaki らは, Cheon のアルゴリズムの改良版を与えた. このアルゴリズムは, 因子 $d|(\ell - 1)$ に対して, q-weak Deffie-Hellman 問題を $O\left(\sqrt{\ell/d} + \sqrt{d}\right)$ 回の群演算で解くことができる.

先に述べた cyclotomic family は, 位数を表す多項式を円分多項式 $\ell(x)$ で与えているため, $\ell(x)-1$ は可約である. よって, ある整数 x_0 に対して, $\ell = \ell(x_0)$ が素数となるとき, $\ell - 1$, $\ell + 1$ の因子を考慮した楕円曲線の構成が必要になる. 本論文では, ρ の値を小さくしたまま, 位数を表す円分多項式の次数の小さくした構成法を与え, Cheon のアルゴリズムに対する安全性を保つために因子の満たすべき条件の考察を行い構成アルゴリズムを与えた. そのアルゴリズムで用いた, pairing-friendly 楕円曲線の構成法の特徴を以下に述べる. Freeman らの cyclotomic family では ρ が小さく, $\sqrt{-D}, \zeta_k \in \mathbb{Q}(\zeta_{hk})$ となるような円分体を考え, nk 次円分多項式 $\Phi_{hk}(x)$ を位数を表す式 $\ell(x)$ として用いている. 筆者の構成法では, 埋め込み次数 $k = 2n$ に対し円分体の拡大を行わずに, ρ の値を $\ell(x) = \Phi_k(x)$ となるように工夫を行った. ρ の値は, $\rho \sim (n+2)/(n-1)$ であり, 特に, $n \equiv 1 \pmod 4$ のとき, $\rho \sim (n+1)/\varphi(n-1)$ である. この値は, Freeman らの cyclotomic family の ρ 値と同じ, あるいは同程度を実現している. これらにより, Cheon のアルゴリズムに対してできるだけ安全性を損なわないような曲線を Freeman らの構成法より多く生成できることを計算実験により示した.

また本論文では, $y^2 = x^5 + c$, $y^2 = x^9 + cx$ の形の pairing-friendly 超楕円曲線の構成法も与えている. その構成法とは, 位数公式を用いた方法である. 以下, 構成法について述べる.

p を奇素数とする. h を正整数, $\tau \in \{0, 1\}$, $c \in \mathbb{F}_p^*$ としたとき, $H_{h,\tau,c}$ を $y^2 = x^\tau(x^h + c)$ で定義される超楕円曲線とする. そして, $H_{h,\tau,c}$ のヤコビ多様体を $J_{h,\tau,c}$ とする. まず, 超楕円曲線 $H_{h,\tau,c}$ のヤコビ群の位数公式を求める. Jacobstahl sum$\phi_{h,r}(c) = \sum_{x \in \mathbb{F}_{p^r}^*} \eta_2(x)\eta_2(x^h + c)$ を用いると, $H_{h,\tau,c}$ 上の $\mathbb{F}_{p^r}$ 有理点の集合 $H_{h,\tau,c}(\mathbb{F}_{p^r})$ の濃度は次のように表すことができる.

$$\#H_{h,0,c}(\mathbb{F}_{p^r}) = p^r + 1 + \eta_2(c)(\phi_{h,r}(c^{-1}) + 1)$$
$$\#H_{h,1,c}(\mathbb{F}_{p^r}) = p^r + 1 + \phi_{h,r}(c)$$

また, 種数 2 の超楕円曲線の p-乗 Frobenius 写像の特性多項式は $\chi(t) = t^4 - s_1t^3 + s_2t^2 - ps_1t + p^2$. で表され, そのヤコビ群の位数は $\chi(1)$ であることが知られている. よって $\#J_{5,0,c}$ は $\#J_{5,0,c}(\mathbb{F}_p) = \chi(1) = s_2 - s_1(p+1) + p^2 + 1$ となる. さらに $\#H_{5,0,c}(\mathbb{F}_p)$ と $\#H_{5,0,c}(\mathbb{F}_{p^2})$ は, この特性多項式の係数 s_1, s_2 で表され, Jacobstahl sum を用いて s_1, s_2 を表すことができる. ここで, $p \equiv 1 \pmod{2h}$ となる素数 p に対して, Haneda らの結果より,

$$\phi_{h,r}(c) = (-1)^{r-1}\hat{\eta}(-1)\hat{\eta}^{h+1}(c)\sum_{j=0}^{h-1}\hat{\eta}^{2j}(c)K(\eta^{2j+1})^r$$

と計算することができるので, $H_{5,0,c}$ のヤコビ群の位数公式は, ある条件を満たす整数 u, v, z, w に

対して,

$$\begin{aligned}\chi(1) &= u^2 - 10uz + up + u + 15v^2 + 10vw - 20vz \\ &\quad +5vp + 5v + 15w^2 - 20wz + 5wp + 5w \\ &\quad +5z^2 - 5zp - 5z + p^2 + 1.\end{aligned}$$

と表すことができる. また, $H_{8,1,c}$ のヤコビ群の位数公式は, Haneda らにより, explicit な式が与えられている. この 2 つの公式を用いて, 種数 2 と 4 の pairing-friendly 超楕円曲線の条件をあげ, 構成アルゴリズムを与えた. それぞれの ρ 値は, 前者は 8 程度, 後者は 16 程度と見積もることができる. また, これらのアルゴリズムを用いて, たくさんの曲線を構成することができた. 種数 4 の pairing-friendly 超楕円曲線の構成法としては今までで初めてのものである.

審査結果の要旨

1984年に Shamir が提案した ID-based 暗号は、IDを管理するセンターが個人 IDを公開鍵として使うことができ、利用者間での鍵交換を必要としない新しい暗号方式であり、この方式は楕円曲線上の Weil ペアリングを用いて 2000年に Boneh-Franklin、境・大岸・笠原によって実現された。この楕円曲線（超楕円曲線）のペアリングを用いて実現される暗号はペアリング暗号と呼ばれるが、この暗号に適した楕円曲線（超楕円曲線）を見つけることは、当該研究分野で最も重要な課題の１つである。

本論文の１、２、３章では、問題の背景と本論文の構成、暗号で使われる一般的な概念の定義、楕円曲線・超楕円曲線のペアリングに関する理論について記述されている。４章ではペアリングに適した楕円曲線に関して次の（１）（２）の結果が示されている。

（１）ペアリング暗号に適した楕円曲線の構成について、これまでの最良であった Freeman-Scott-Teske の構成法を一部改良した構成法を提案し、その構成法でより多くのペアリング暗号に適した楕円曲線を構成できることを示した。

（２）Cheon アルゴリズムと呼ばれる楕円曲線暗号の新しい攻撃法に対する対策を提案し、この対策で（１）の構成が Cheon アルゴリズムによる攻撃に対して安全性を失わない楕円曲線を実際に生成することを示した。

５章では、ペアリングに適した超楕円曲線に関して次の（３）の結果が与えられている。

（３）$y^2 = x^5 + c$, $y^2 = x^9 + c\ x$ の形のペアリング暗号に適した超楕円曲線の構成法を位数公式を用いて与えている. 前者は、拡大体で楕円曲線に分解しない種数２の超楕円曲線であり、$y^2 = x^5 + c\ x$ の形の曲線からペアリング暗号に適した曲線を見つける今まで知られている方法より安全性が高いと考えられる。$y^2 = x^9 + c\ x$ は種数 4 の超楕円曲線で種数 4 のペアリング暗号に適した曲線の構成は今まで知られておらず、重要な結果である。

上記の（１）（２）（３）は当該研究分野において、今後の発展も見込める重要な結果であり、論文の構成・内容も学位論文としてふさわしい内容であり、博士（理学）の学位を授与することを適当と認める。