Computer Security Symposium 2022 in Kumamoto

同種写像暗号CSIDHのHesse曲線による構成

小濱 大輝 (株式会社エクサ)
○野本 慶一郎 (九州大学大学院数理学府)
池松 泰彦 (九州大学マス・フォア・インダストリ研究所)
縫田 光司 (九州大学マス・フォア・インダストリ研究所, 産業技術総合研究所)
小林 真一 (九州大学大学院数理学研究院)

目次

耐量子計算機暗号について

■ 現在普及している公開鍵暗号技術は, 量子コンピュータを用いた
Shorのアルゴリズムにより多項式時間で破られてしまう.

■ 大規模な量子コンピュータの実用化に備えて, **耐量子計算機暗号**の
研究・開発が必要.

2016	NIST(米国標準技術研究所)は耐量子計算機暗号の標準化公募を開始.
2020	第3ラウンド選出暗号の発表.

同種写像暗号方式SIKEを含む

主な耐量子計算機暗号

- 格子暗号
- 符号ベース暗号
- 多変数多項式暗号
- **同種写像暗号**

SIKEとCSIDH

■ 2022年7月, **SIKE**において基盤となっている鍵共有プロトコル**SIDH**に対する深刻な鍵復元攻撃[1]が提案された.

■ その攻撃法は, 同じく楕円曲線を用いる鍵共有プロトコルである**CSIDH**には適用不可.

CSIDH

虚二次体のorder $\mathcal{O}$に付随するイデアル類群の, ある超特異楕円曲線の$\mathbb{F}_p$-同型類の集合$\mathcal{E}\ell\ell_p(\mathcal{O})$への作用に基づく鍵共有方式.

---

[1] W. Castryck, T. Decru, An efficient key recovery attack on SIDH (preliminary version), Cryptology ePrint Archive 2022/975.

先行研究と本研究

提案者	楕円曲線	定義方程式	素数p
Castryck, et. al.[2] (**オリジナル**)	Montgomery曲線	$\mathcal{M}_A: y^2 = x^3 + Ax^2 + x$	$p \equiv 3 \bmod 8$
Moriya, Onuki, Takagi[3]	Edwards曲線	$\mathcal{E}_d: x^2 + y^2 = 1 + dx^2y^2$	

公開鍵

モジュラー曲線の理論を元に, CSIDHを構成できないか？

Hesse曲線を用いたCSIDHの構成に成功.

[2] W. Castryck, et. al., CSIDH: An Efficient Post-Quantum Commutative Group Action, Advances in Cryptology – ASIACRYPT 2018, pp. 395–427 (2018).
[3] T. Moriya, H. Onuki, T. Takagi, How to Construct CSIDH on Edwards Curves, Topics in Cryptology – CT-RSA 2020, pp. 512–537 (2020).

先行研究と本研究

提案者	楕円曲線	定義方程式	素数p
Castryck, et. al.[2]	Montgomery曲線	$\mathcal{M}_A: y^2 = x^3 + Ax^2 + x$	$p \equiv 3 \bmod 8$
Moriya, Onuki, Takagi[3]	Edwards曲線	$\mathcal{E}_d: x^2 + y^2 = 1 + dx^2y^2$	
本研究	**Hesse曲線**	$\boldsymbol{\mathcal{H}_d: X^3 + Y^3 + Z^3 = dXYZ}$	$\boldsymbol{p \equiv 2 \bmod 3}$

使用可能な素数は異なる

- Hesse曲線はEdwards曲線と違い, 一般にMontgomery曲線と同型ではない.
- したがって, Hesse曲線を用いたCSIDHは, 新しい楕円曲線のクラスに対する鍵共有プロトコルである.

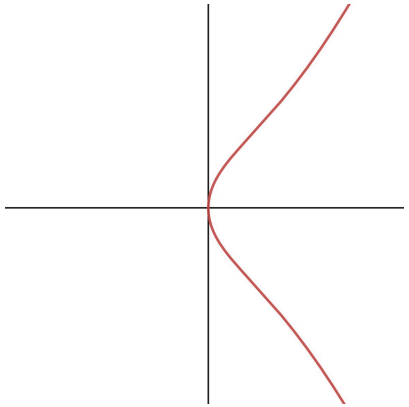
目次

楕円曲線の定義

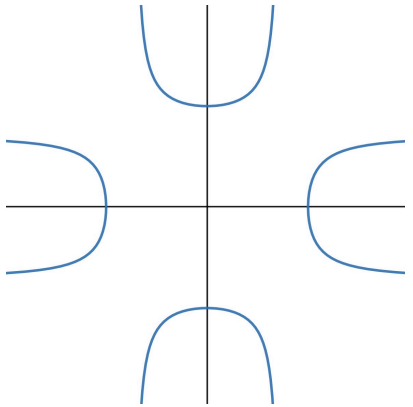
E: 体K上の**楕円曲線** ⟺

- E: K上定義された種数1の非特異射影代数曲線.
- K-有理点 $O_E \in E(K)$ が存在する.

■ $E(K)$: O_Eを単位元としてアーベル群の構造が入る.



Montgomery曲線
$\mathcal{M}_0$: $y^2 = x^3 + x$



Edwards曲線
$\mathcal{E}_2$: $x^2 + y^2 = 1 + 2x^2y^2$

■ 一般に, K上の楕円曲線は非特異なWeierstrass方程式

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

で定義される曲線にK上同型である.

同種写像

E, E': K上の楕円曲線

$$\phi: \begin{array}{ccc} E & \to & E' \\ (x,y) & \mapsto & (f_1(x,y), f_2(x,y)) \end{array} : K\text{上の}\textbf{同種写像} \iff \begin{array}{l} \bullet\ f_1, f_2: K\text{係数の有理関数} \\ \bullet\ \phi(O_E) = O_{E'} \end{array}$$

例　(i) $P \mapsto [n]P := P + \cdots + P$　(n倍写像)

(ii) $\pi_p: E/\mathbb{F}_p \to E/\mathbb{F}_p, (x,y) \mapsto (x^p, y^p)$　(**p-Frobenius準同型**)

■ $\mathrm{End}_p(E) := \{\phi: E \to E \mid \mathbb{F}_p\text{上の同種写像}\}$　(E: $\mathbb{F}_p$上の楕円曲線)

超特異楕円曲線

■ $E/\mathbb{F}_p$: 超特異楕円曲線 $\Leftrightarrow E[p] := \mathrm{Ker}[p] = \{O_E\}$

■ $p \geq 5$ならば，「$E/\mathbb{F}_p$：超特異 $\Leftrightarrow \#E(\mathbb{F}_p) = p + 1$」

Hesse曲線の定義・性質

Hesse曲線

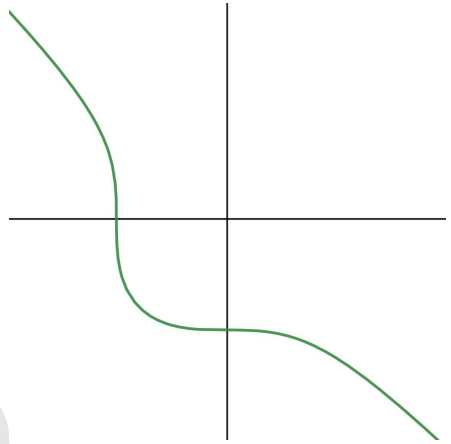
$$\mathcal{H}_d\colon X^3+Y^3+Z^3=dXYZ\ (d^3\neq 27)$$

ただし, $O=O_{\mathcal{H}_d}=[0:-1:1]$

■ $p\equiv 2 \bmod 3$ならば, 以下が成り立つ.

- $\mathcal{H}_0/\mathbb{F}_p\colon X^3+Y^3+Z^3=0$は超特異.
- $\mathcal{H}_0(\mathbb{F}_p)[3]=\{O,[1:0:-1],[1:-1:0]\}$.

$\mathcal{H}_0$: 公開鍵



$x^3+y^3+1=0$

定理

$E/\mathbb{F}_p$: 楕円曲線 ($p\equiv 2 \bmod 3$)とする. このとき

$$\exists P\in E(\mathbb{F}_p)[3]\setminus\{O_E\}\Longrightarrow \exists d\in\mathbb{F}_p\ \exists\phi\colon E\simeq\mathcal{H}_d \text{ over } \mathbb{F}_p.$$

特に$\phi(P)=[1:0:-1]$と取れば, $d\in\mathbb{F}_p$は一意的.

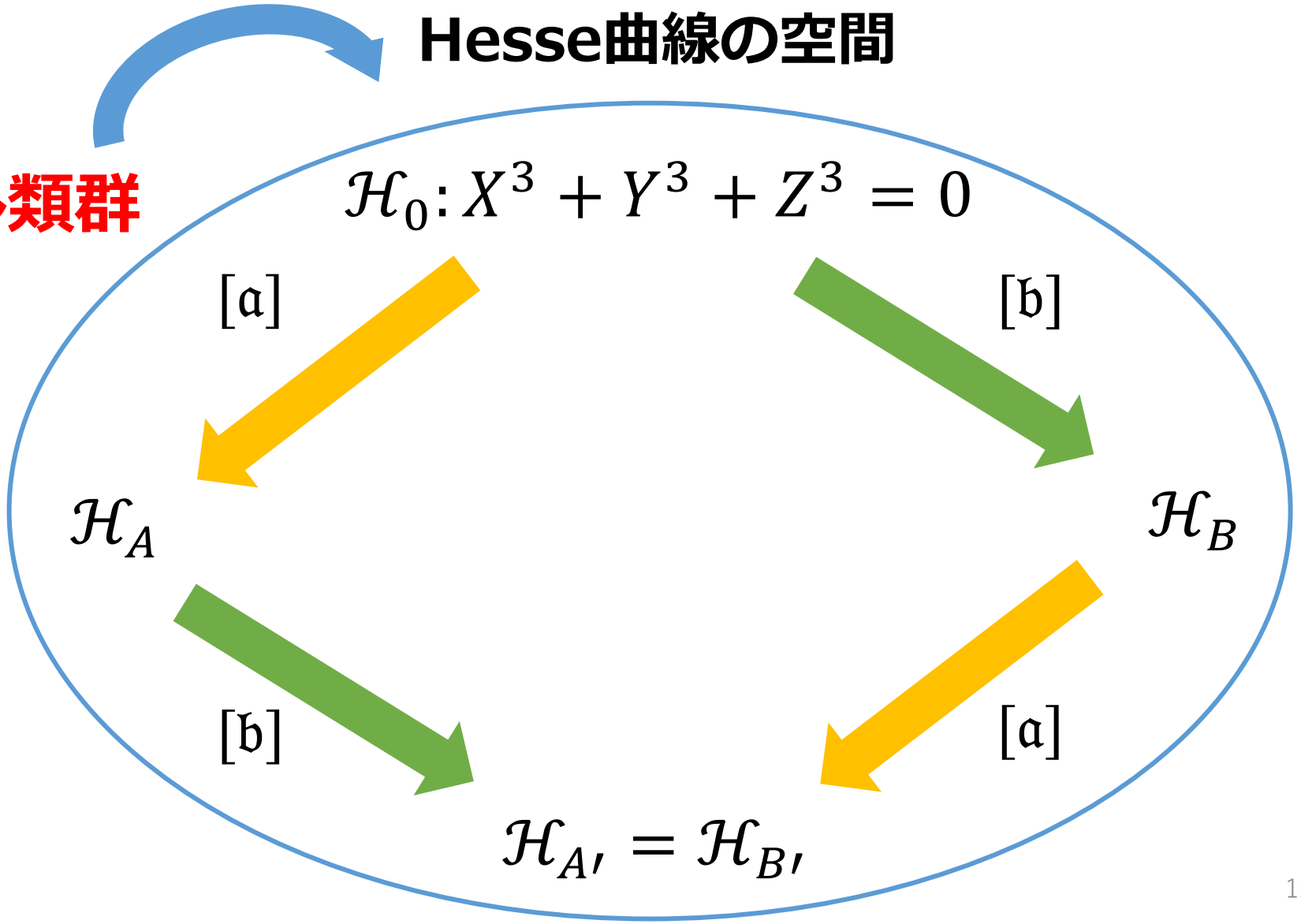
目次

Hesse曲線を用いたCSIDHのイメージ図

$Cl(\mathcal{O})$: **イデアル類群**

Ψ

$[\mathfrak{a}], [\mathfrak{b}]$



イデアル類群の定義

$\mathcal{O}$: 代数体Kのorder

$I(\mathcal{O}) = \{\mathcal{O}$の可逆な分数イデアル$\}$

$P(\mathcal{O}) = \{0$でない単項イデアル$\}$

例

$K = \mathbb{Q}(\sqrt{-p})$

$\mathcal{O} = \mathbb{Z}[\sqrt{-p}], \quad \mathbb{Z}\left[\frac{-1+\sqrt{-p}}{2}\right], \quad \cdots$

$\mathrm{Cl}(\mathcal{O}) := I(\mathcal{O})/P(\mathcal{O})$ **イデアル類群**

どのように作用の実現をする？

具体的にd'を与えるには？

- イデアル類群は有限群.
- $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O})$の代表元は整イデアルとして取れる.
- 適当な条件の下, イデアル類群は楕円曲線の集合に作用する.
- 作用により$\mathcal{H}_d$から$\mathcal{H}_{d'}$が構成できる.

作用計算のアイデア1

■ Hesse曲線に対するイデアル類群の作用を以下で定義.

$$[\mathfrak{a}]\,\mathcal{H}_d := \mathcal{H}_d/\mathcal{H}_d[\mathfrak{a}], \qquad \mathcal{H}_d[\mathfrak{a}] := \bigcap_{\alpha\in\mathfrak{a}} \mathrm{Ker}(\alpha)$$

$$\begin{array}{c} \mathbf{End}_p(\mathcal{H}_d) \simeq \mathcal{O} \\ \cup \\ \pi_p \end{array}$$

$\mathbb{Q}(\sqrt{-p})$のorder

■ CSIDHでは, $\ell \mid p+1$を満たす奇素数ℓに対する, 以下のイデアルの作用を考える.

$$\mathfrak{l} := (\ell, \pi_p - 1), \qquad \bar{\mathfrak{l}} := (\ell, \pi_p + 1)$$

$$\mathcal{H}_d[\mathfrak{l}] = \left\langle \left[\frac{p+1}{\ell}\right] P \right\rangle \qquad P \in \mathcal{H}_d(\mathbb{F}_p) \text{ s.t. } \left[\frac{p+1}{\ell}\right] P \neq O$$

$$\mathcal{H}_d[\bar{\mathfrak{l}}] = \left\langle \left[\frac{p+1}{\ell}\right] Q \right\rangle \qquad Q \in \mathcal{H}_d(\mathbb{F}_{p^2}) \text{ s.t. } \left[\frac{p+1}{\ell}\right] Q \neq O \text{ かつ } \pi_p(Q) = -Q$$

作用計算のアイデア2

■ イデアル類群の作用及び, $[\mathfrak{a}]\,\mathcal{H}_d \simeq \mathcal{H}_{d'}$となる$d' \in \mathbb{F}_p$は**Veluの公式**を用いて実装.

定理 (Hesse曲線におけるVeluの公式)[4]

$F = \{[s_i : t_i : 1]\}_{i=1}^{n} \cup \{O\}$: $\mathcal{H}_d$の有限部分群 ($3 \nmid \#F = n+1$, $\forall i,\ s_i t_i \neq 0$).

このとき写像

$$P \mapsto \left[\prod_{R\in F} X(P+R) : \prod_{R\in F} Y(P+R) : \prod_{R\in F} Z(P+R)\right]$$

は$\mathrm{Ker}\,\phi = F$となる同種写像ϕ: $\mathcal{H}_d \to \mathcal{H}_{d'}$を定める.

$$d' := \frac{(1-2n)d + \sum_{i=1}^{n} \frac{1}{s_i t_i}}{\prod_{i=1}^{n} s_i}$$

---

[4] Broon, F. L. P., Dang, T., Fouotsa, E. and Moody, D.: Isogenies on twisted Hessian curves, Journal of Mathematical Cryptology, Vol. 15, No. 1, pp. 345–358, (2021).

目次

Hesse曲線を用いた鍵共有プロトコル

公開鍵	条件
素数p	$p \equiv 2 \bmod 3$
$n \in \mathbb{Z}$	$n > 0$
5以上の素数$\ell_1, \ldots, \ell_n$	$\forall i, \ell_i \mid p+1$
$m \in \mathbb{Z}$	
$\mathcal{H}_0/\mathbb{F}_p : X^3 + Y^3 + Z^3 = 0$	

秘密鍵	条件
Alice: $(e_1, e_2, \ldots, e_n) \in \mathbb{Z}^n$	各成分は区間$[-m, m]$に属するように一様ランダムに生成
Bob: $(d_1, d_2, \ldots, d_n) \in \mathbb{Z}^n$	

プロトコル

Alice

$[\mathfrak{l}_1^{e_1}\mathfrak{l}_2^{e_2}\cdots\mathfrak{l}_n^{e_n}]\mathcal{H}_0 \xrightarrow{\simeq} \mathcal{H}_A$

$A \in \mathbb{F}_p$を送る

$[\mathfrak{l}_1^{e_1}\mathfrak{l}_2^{e_2}\cdots\mathfrak{l}_n^{e_n}]\mathcal{H}_B \xrightarrow{\simeq} \mathcal{H}_{A'}$

Bob

$[\mathfrak{l}_1^{d_1}\mathfrak{l}_2^{d_2}\cdots\mathfrak{l}_n^{d_n}]\mathcal{H}_0 \xrightarrow{\simeq} \mathcal{H}_B$

$B \in \mathbb{F}_p$を送る

$[\mathfrak{l}_1^{d_1}\mathfrak{l}_2^{d_2}\cdots\mathfrak{l}_n^{d_n}]\mathcal{H}_A \xrightarrow{\simeq} \mathcal{H}_{B'}$

セッション鍵: $S := A' = B'$

選択パラメータと実験結果

■ 標準的なCSIDHの安全性解析に基づいて, パラメータを設定する.

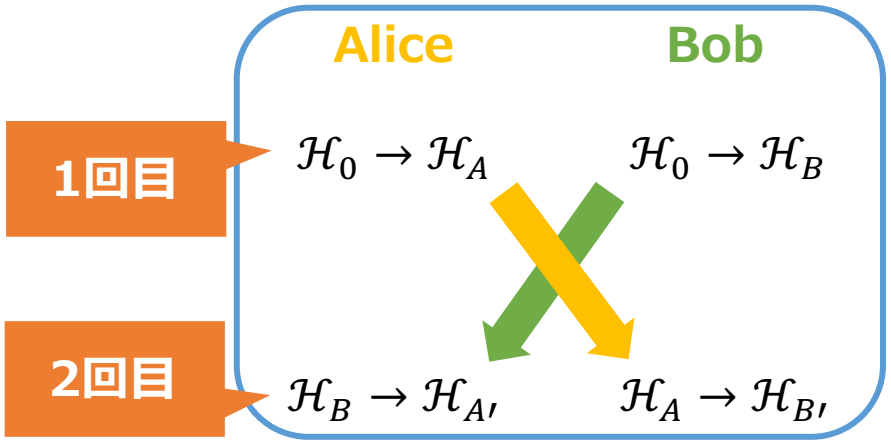
p	$\lceil \log_2 p \rceil$	n	m	Aのサイズ
$12\ell_1\ell_2\cdots\ell_{73}-1$	511	73	5	512bit

ただし, $\ell_1, \ldots, \ell_{72}$は5以上の素数を小さい順に72個並べたもの, $\ell_{73} = 587$.

■ Aliceによる公開鍵からセッション鍵の生成を1000回行った際の実行時間の平均.

	1回目の群作用	2回目の群作用
時間	3,931ms	3,929ms

16GBメモリ 3.20GHz Apple M1チップを用いたMagmaでの実装



参考

論文[1]のTable 2において, オリジナルなCSIDHでの
10000回の鍵共有の実行平均は 40.8ms であったと報告されている.

目次

結論

- モジュラー曲線の理論のアイデアを用いて, **Hesse曲線**を用いたCSIDHを構成した.
- その構成では, **位数3の$\mathbb{F}_p$-有理点の存在性**に基づく, Hesse曲線の表示の一意性が重要である.
- 128bit安全性に対する実装実験を行った. (素朴な実装ではオリジナルの約100倍の実行時間となった.)

Future Work

・モジュラー曲線の理論を用いたHesse曲線以外の楕円曲線に対するCSIDHの構成

・計算処理の大幅な高速化