同種写像グラフの数理
と
耐量子計算機暗号への応用

早稲田整数論セミナー

2022年 4月 22日

高島克幸
（早稲田大学 教育・総合科学学術院）

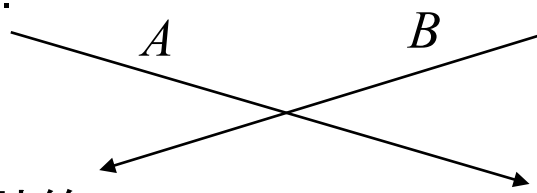
今日の目次

- イントロ: DH鍵共有 と 耐量子計算機暗号
- 楕円曲線同種写像グラフ と その暗号応用
  - CGLハッシュ関数 と SIDH鍵共有
  - SQISign 署名 [DKL+20]
  - 超特異楕円曲線同種写像グラフ $\mathcal{G}_1(\overline{\mathbb{F}_p}, \ell)$ と $\mathcal{G}_1(\mathbb{F}_p, \ell)$
  - 通常曲線同種写像グラフ と 格子暗号への応用 [BDPW20]
- 種数2曲線 同種写像グラフ と その暗号応用
  - CGLハッシュ関数 on $\mathcal{G}_2(\overline{\mathbb{F}_p}, 2)$
  - 超特殊 (superspecial) 種数2曲線 同種写像グラフ $\mathcal{G}_2(\overline{\mathbb{F}_p}, 2)$ 構造解析 [CS20, KT20, …]

ディフィ–ヘルマン (DH) 鍵共有

- 公開パラメータ：2000ビット素数 p, 但し $q := (p-1)/2$ も素数(p: 安全素数)
  $1 < g < p-1$ である g, 但し $g^q = 1 \bmod p$

Alice	Bob
q 未満の乱数 α ：Alice の秘密鍵	q 未満の乱数 β ：Bob の秘密鍵
$A = g^\alpha \bmod p$ を計算.	$B = g^\beta \bmod p$ を計算.
$K_{\text{Alice}} = B^\alpha \bmod p$ を計算.	$K_{\text{Bob}} = A^\beta \bmod p$ を計算.



- 共有鍵： $K_{\text{Alice}} = B^\alpha = (g^\beta)^\alpha = g^{\beta\alpha} = g^{\alpha\beta} = (g^\alpha)^\beta = A^\beta = K_{\text{Bob}}$
- 安全性: $(g, g^\alpha \bmod p)$ から α を計算する問題 (離散対数問題: DLP) の困難性を安全性の根拠とする.

残念ながら、量子計算機に対して安全ではない

耐量子計算機暗号

- 大規模量子計算機が実用化されれば，Shor の 素因数分解，離散対数計算アルゴリズムによって 実用化されている公開鍵暗号，e.g., RSA, (EC)DH, ペアリング暗号 が破られる

- 耐量子計算機暗号: PQC = ポスト量子暗号
  その候補
  - 格子暗号
  - 多変数多項式暗号
  - 符号ベース暗号
  - 同種写像暗号
  - 共通鍵暗号ベース署名

- 耐量子暗号は、まだ量子計算機でも効率的に計算できない計算問題の困難性 に基づいて構成される

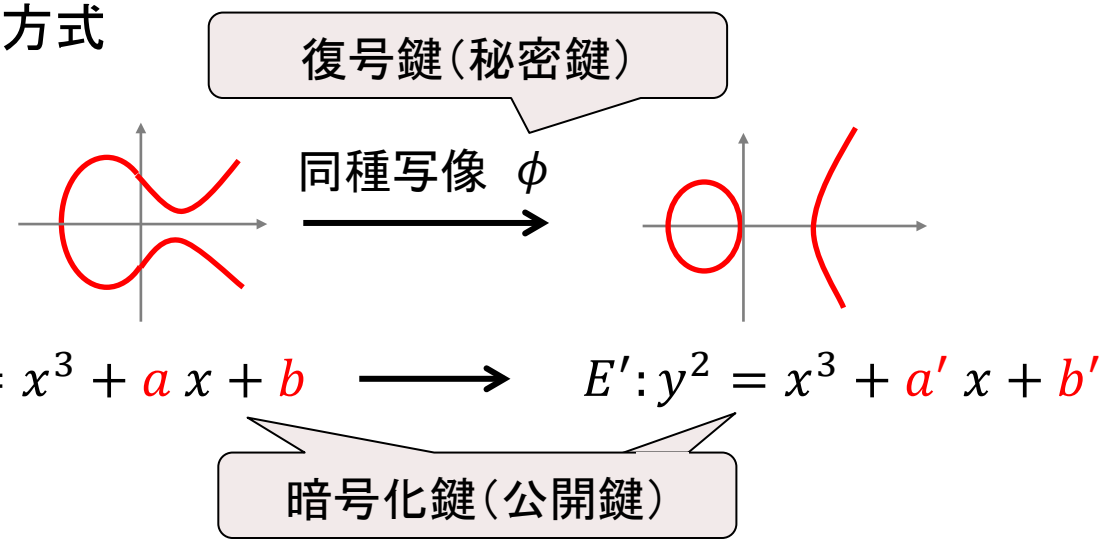
CGL ハッシュ関数
と
SIDH（ Supersingular Isogeny DH ）鍵共有

同種写像暗号の概要

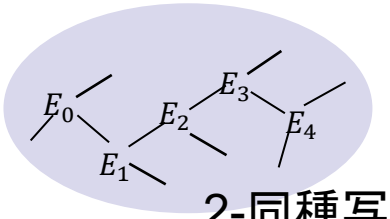
- 同種写像と呼ばれる 楕円曲線の変換 を利用して、

  暗号化鍵 = 変換前の楕円曲線 と 変換後の楕円曲線、
  復号鍵 = 変換方法（同種写像）

  とした暗号方式



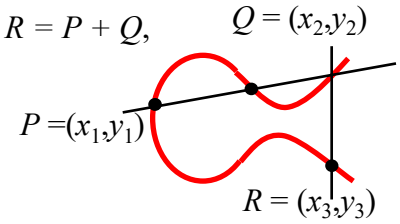
- 楕円曲線 E を 楕円曲線 E' に変換する同種写像を計算する問題（同種写像問題）の困難性に基づいた暗号
- 群のような代数系上でなく、同種写像のなすグラフ上でのウォークの繰り返しパターンを秘密鍵に使うことで、耐量子計算機暗号を実現



2-同種写像の繰り返し

$\phi = \psi_{e-1} \cdots \psi_0$

楕円曲線間の同種写像

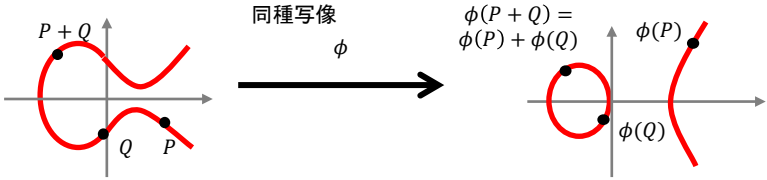


- 有限体 $\mathbb{F}_q$（$q = p^k, p \geq 5$）上の楕円曲線
  $E\colon y^2 = x^3 + ax + b \quad (a, b \in \mathbb{F}_q, \Delta := 4a^3 + 27b^2 \neq 0)$

$$j(E) := 1728 \cdot 4a^3/\Delta, \quad E_1/\overline{\mathbb{F}}_q \cong E_2/\overline{\mathbb{F}}_q \Leftrightarrow j(E_1) = j(E_2)$$

（Montgomery モデル：$E\colon by^2 = x^3 + ax^2 + x \ (a \neq \pm 2, b \neq 0)$）

- 2つの楕円曲線 E, E' に対して、同種写像 $\phi\colon E \to E'$ は、E 上の点 $P = (x, y)$ に対して、有理関数 f, g を使って、 $\phi(P) = (f(x, y), g(x, y))$ と、代数的に定義される（非定数）写像である
- 更に、2点 P, Q に対して、以下の等式が成立（準同型性）$\phi(P + Q) = \phi(P) + \phi(Q)$.



- Vélu の公式: 楕円曲線 E とその上の点 R に対して、$< R >$ を核とする（巡回）同種写像 $\psi_R\colon E \to E/< R >$ を効率的に計算する公式（アルゴリズム）
- 核 $< R >$ が位数 ℓ の巡回群の時，ℓ-同種写像という.

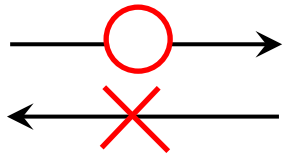
$E(\mathbb{F}_{q^s}) := \left\{(x, y) \in (\mathbb{F}_{q^s})^2 \mid y^2 = x^3 + ax + b\right\} \cup \{O_E\}$; $\mathbb{F}_{q^s}$−有理点群

$E[r] := \left\{ P \in E(\overline{\mathbb{F}}_q) \mid r \cdot P = O_E \right\}$; r−ねじれ点群

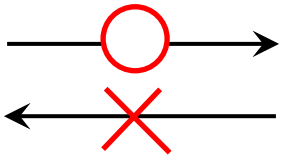
楕円曲線に関する３種の一方向性関数

○：容易
×：困難

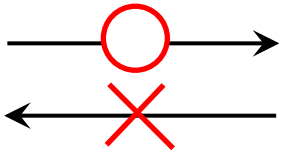
- スカラー倍算

(P, α)  $(P, \alpha P)$

- ペアリング

(P, Q)  $(P, e(P, Q))$

- 同種写像計算

(E, ϕ)  $(E, \phi(E))$

ϕ：同種写像を指定するデータ

楕円曲線に関する３種の一方向性関数

○：容易　　○：量子で容易

×：困難　　×：量子でも困難

- スカラー倍算

$$(P, \alpha) \quad \rightarrow \quad (P,\ \alpha P)$$

- ペアリング

$$(P, Q) \quad \rightarrow \quad (P, e(P, Q))$$

- 同種写像計算

$$(E, \phi) \quad \rightarrow \quad (E,\ \phi(E))$$

3種の一方向性関数が，3種の異なる特性をもつ暗号を生み出す

同種写像問題に対する解析(解読)アルゴリズム

同種写像問題

2つの同種な楕円曲線　E, E' に対して、$\phi: E \to E'$ となる 同種写像 ϕ（のコンパクトな表現）を計算せよ

- ϕ のコンパクトな表現は、例えば、$\deg(\phi)$ が小素数 ℓ_i によって、$\prod \ell_i$ となっている場合には、各ℓ_i次同種写像の像に現れる楕円曲線（j-不変量）の列挙で与えられる.

	古典計算機による 解読時間	量子計算機による 解読時間
通常 楕円曲線	$\tilde{O}(\sqrt[4]{p})$	$L_p[1/2, \sqrt{3}/2]$
超特異 楕円曲線 *	$\tilde{O}(\sqrt{p})$	$\tilde{O}(\sqrt[4]{p})$

* $E[p] = \{O_E\}$ となる楕円曲線 E

$\log p$ の準指数関数:　$L_p[\alpha, c] := \exp\left((c + o(1))(\log p)^{\alpha}(\log\log p)^{1-\alpha}\right)$

準指数時間 通常曲線同種写像問題 量子アルゴリズム [CJS14]

$\mathrm{Cl}(\mathcal{O}_\Delta)$: 判別式 $\Delta(<0)$ の虚 2 次 整環 (オーダー) $\mathcal{O}_\Delta$ のイデアル類群

$\mathrm{Ell}_p(\mathcal{O}_\Delta)$: $\mathcal{O}_\Delta$ を自己準同型環にもつ $\overline{\mathbb{F}_p}$ 上の楕円曲線の $\overline{\mathbb{F}_p}$-同型類全体

- 楕円曲線集合へのイデアル類群作用(CM作用):
  $[a] * E_0 :=$ [$\mathrm{Ker}(\phi_a) = \bigcap_{z\in a} \mathrm{Ker}(z)$ となる同種写像 ϕ_a の値域曲線 E_1]

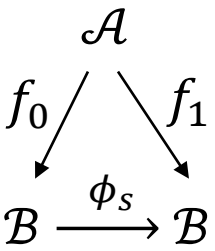
$$* : \ \mathrm{Cl}(\mathcal{O}_\Delta) \times \mathrm{Ell}_p(\mathcal{O}_\Delta) \longrightarrow \mathrm{Ell}_p(\mathcal{O}_\Delta)$$
$$([a], E_0) \mapsto E_1 = [a] * E_0$$

- 上記の群作用を用いて、アーベル群に対する 隠れシフト問題 に帰着
  (問題 $\phi_s : E_0 \mapsto E_1 = s * E_0$ に対して $f_0(x) := x * E_0$, $f_1(x) := x * E_1$)

単射な $f_0, f_1 : \mathcal{A} \to \mathcal{B}$ such that $\mathcal{A}$: 有限アーベル群、$\mathcal{B}$:有限集合

$f_0, f_1 : \mathcal{A} \to \mathcal{B}$ $\quad$ $f_1(x) = f_0(x \cdot s)$ for some $s \in \mathcal{A}$

にブラックボックスアクセスして、s を計算する問題



- その隠れシフト問題 を 二面体群 に関する 隠れ部分群問題 (DHSP) に帰着

DHSP には、準指数時間 量子アルゴリズムが知られている (Kuperberg, Regev)

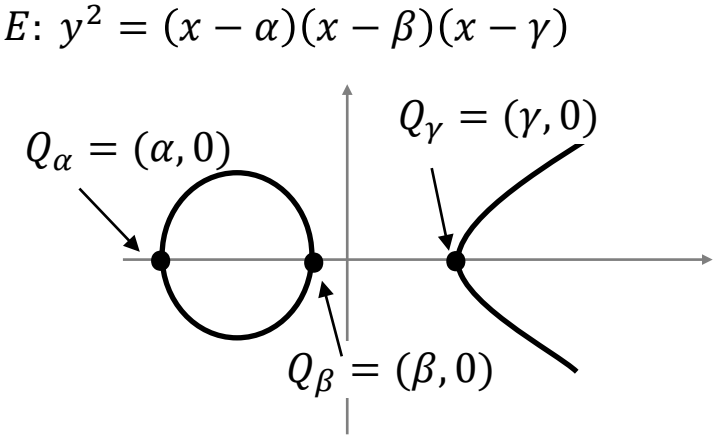
2-同種写像列計算

$Q=(x_Q,0)\neq O_E\in C\subset E[2]$ に対し，$\psi_C: E\ni(x,y)\mapsto(X,Y)\in E/C$ は，

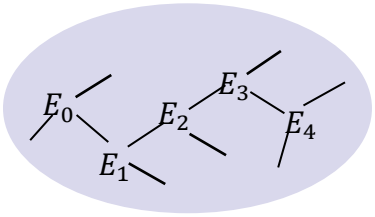
$$E/C: Y^2=X^3-(4a+15x_Q^2)X+(8b-14x_Q^3),$$
$$X=x+\frac{3x_Q^2+a}{x-x_Q},\quad Y=y-\frac{(3x_Q^2+a)y}{(x-x_Q)^2}\quad \text{となる.}$$

- Q（と O_E）以外の 2個の 2- ねじれ点は ψ_C で同じ点 Q' に写像され，$C'=\langle Q'\rangle$ を核とする $E'=E/C$ からの同種写像は E への 逆戻り（バックトラック）写像である.

$$E \underset{\psi_{C'}}{\overset{\psi_C}{\rightleftarrows}} E'$$



- 2^e- 同種写像計算では，各ステップでバックトラックしない 2 (= 3 – 1) 個の 2- 同種写像のいずれかを順次選択して計算していくことになる.



2-同種写像の繰り返し

$\phi=\psi_{e-1}\cdots\psi_0$

Charles-Goren-Lauter (CGL) ハッシュ関数

2−同種写像列 : $E_0 \xrightarrow{\psi_0} E_1 \xrightarrow{\psi_1} \cdots \xrightarrow{\psi_{e-2}} E_{e-1} \xrightarrow{\psi_{e-1}} E_e$

ハッシュ関数 h

$\omega := \{\omega_i\}_{0 \le i < e}$

↓

h

↓

$h(\omega)$

ハッシュ関数 h の安全性:

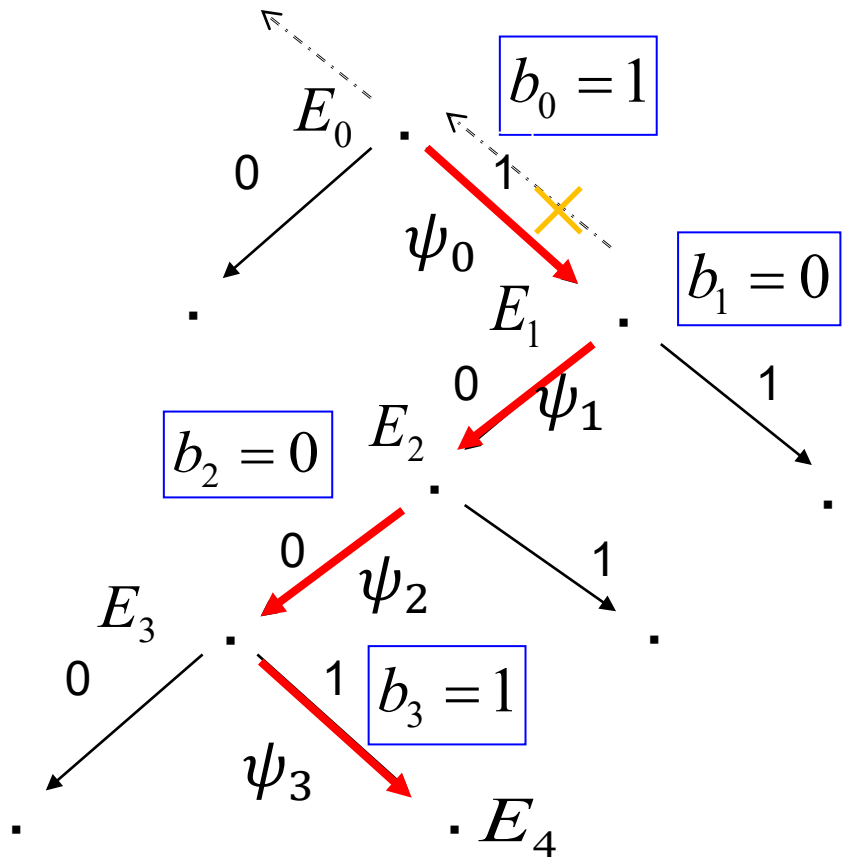
衝突計算困難性:

$h(\omega) = h(\omega')$なる

2入力 ω, ω' 計算困難

入力: E_0 , $\omega = b_0 b_1 b_2 b_3 = 1001$

出力: $j(E_4)$



$R_0 \in E[2^e]$ を核とする 2^e–同種写像計算

- 入力は、E_0 と $R_0 \in E[2^e]$

$$E_0 \xrightarrow{\psi_0} E_1 \xrightarrow{\psi_1} \cdots \xrightarrow{\psi_{e-2}} E_{e-1} \xrightarrow{\psi_{e-1}} E_e := E_0/\langle R_0 \rangle$$

- $E_1 := E_0/\langle 2^{e-1}R_0 \rangle$, $\psi_0 : E_0 \to E_1$, $R_1 := \psi_0(R_0)$ を Velu公式で計算

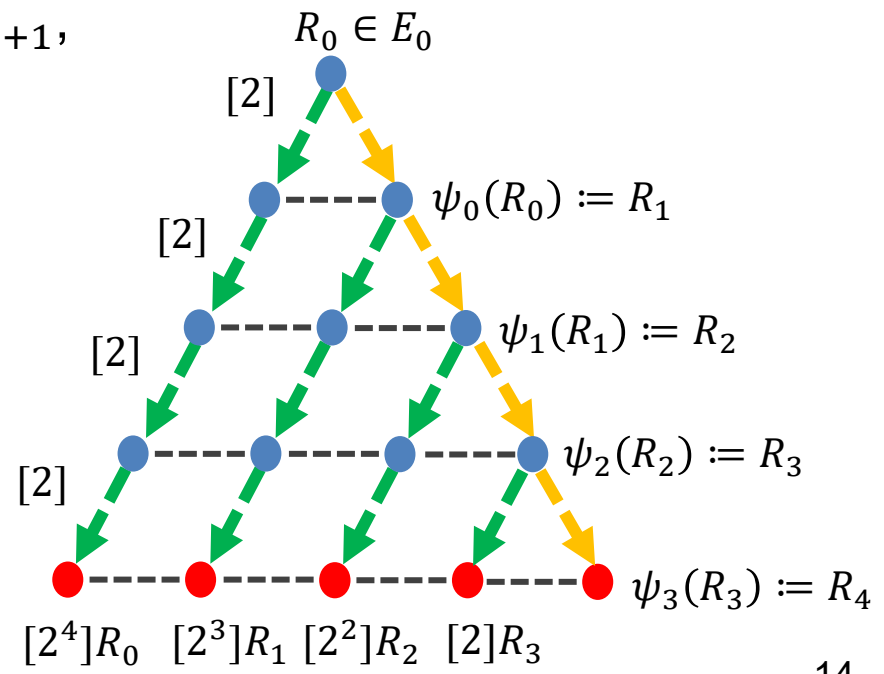
…

$E_{i+1} := E_i/\langle 2^{e-i-1}R_i \rangle$, $\psi_i : E_i \to E_{i+1}$,
$R_{i+1} := \psi_i(R_i)$ と順次計算して、

$E_e := E_{e-1}/\langle R_{e-1} \rangle$ を出力

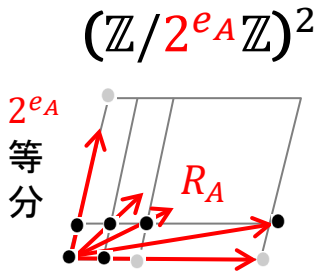
- optimal strategyと呼ばれる
効率的な計算法では、2 倍写像と
2–同種写像の計算回数：$O(e \log e)$

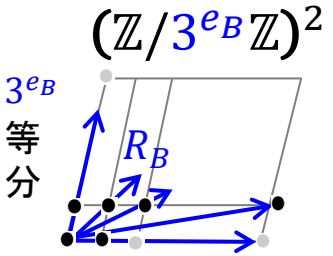
$e = 5, R_0 \in E_0[2^5]$ の場合



ランダムウォークに基づく SIDH鍵共有

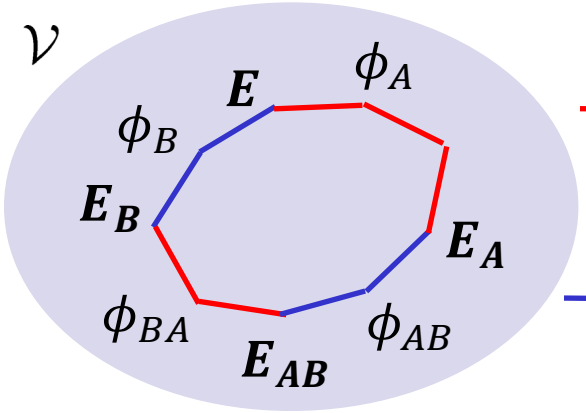
- $p+1=f\cdot 2^{e_A}3^{e_B}$ となる大素数 p
- $E(\mathbb{F}_{p^2}) \simeq (\mathbb{Z}/(p+1)\mathbb{Z})^2 \supseteq (\mathbb{Z}/2^{e_A}\mathbb{Z})^2 \oplus (\mathbb{Z}/3^{e_B}\mathbb{Z})^2$
  となる超特異楕円曲線 $E/\mathbb{F}_{p^2}$
  例: $y^2=x^3+x$ with $p=2^{e_A}3^{e_B}-1$





- $\mathcal{G}_1(\overline{\mathbb{F}_p},\ell)$:= $\overline{\mathbb{F}_p}$上の超特異楕円曲線間の ℓ−同種写像のなすグラフ.
- Alice は、グラフ $\mathcal{G}_1(\overline{\mathbb{F}_p},2)$ 内の道、ϕ_A,ϕ_{BA} を計算可能、
  Bob は、$\mathcal{G}_1(\overline{\mathbb{F}_p},3)$ 内の道、ϕ_B,ϕ_{AB} 計算可能 となるように設計.

$\mathcal{G}_1(\overline{\mathbb{F}_p},2) \cup \mathcal{G}_1(\overline{\mathbb{F}_p},3)$



$\mathcal{G}_1(\overline{\mathbb{F}_p},2)$内の道

$\mathcal{G}_1(\overline{\mathbb{F}_p},3)$内の道

$\ker\phi_A=\langle R_A\rangle \subset E[2^{e_A}]$
$\ker\phi_B=\langle R_B\rangle \subset E[3^{e_B}]$

$\ker\phi_{AB}=\langle\phi_A(R_B)\rangle$
$\ker\phi_{BA}=\langle\phi_B(R_A)\rangle$

$$\begin{array}{ccc} E & \xrightarrow{\phi_A} & E_A := E/\langle R_A\rangle \\ \downarrow{\scriptstyle \phi_B} & & \downarrow{\scriptstyle \phi_{AB}} \\ E_B := E/\langle R_B\rangle & \xrightarrow{\phi_{BA}} & E_{AB} := E/\langle R_A, R_B\rangle \end{array}$$

SIDH 鍵共有

- 公開パラメータ: 素数 p （ s.t. $p+1 = f \cdot 2^{e_A} 3^{e_B}$ ）
  超特異楕円曲線: $E(\mathbb{F}_{p^2}) \simeq (\mathbb{Z}/(p+1)\mathbb{Z})^2 \supseteq (\mathbb{Z}/2^{e_A}\mathbb{Z})^2 \oplus (\mathbb{Z}/3^{e_B}\mathbb{Z})^2$

  生成元: $E[2^{e_A}] = \langle P_A, Q_A \rangle$, $E[3^{e_B}] = \langle P_B, Q_B \rangle$

Alice

- $k_A \leftarrow \mathbb{Z}/2^{e_A}\mathbb{Z}$,
  $R_A := P_A + k_A Q_A$,
- $\phi_A : E \to E_A := E/\langle R_A \rangle$
  $\phi_A(P_B), \phi_A(Q_B) \in E_A$

Bob

- $k_B \leftarrow \mathbb{Z}/3^{e_B}\mathbb{Z}$,
  $R_B := P_B + k_B Q_B$,
- $\phi_B : E \to E_B := E/\langle R_B \rangle$,
  $\phi_B(P_A), \phi_B(Q_A) \in E_B$

$E_A, \phi_A(P_B), \phi_A(Q_B)$ →

← $E_B, \phi_B(P_A), \phi_B(Q_A)$

- $\phi_B(R_A) = \phi_B(P_A) + k_A \phi_B(Q_A)$
  $K_{\text{Alice}} := j(E_B/\langle \phi_B(R_A) \rangle)$

- $\phi_A(R_B) = \phi_A(P_B) + k_B \phi_A(Q_B)$
  $K_{\text{Bob}} := j(E_A/\langle \phi_A(R_B) \rangle)$

- 共有鍵: $K_{\text{Alice}} = j(E_B/\langle \phi_B(R_A) \rangle) = j(E/\langle R_A, R_B \rangle) = j(E_A/\langle \phi_A(R_B) \rangle) = K_{\text{Bob}}$
- 安全性: $E, P_B, Q_B, E_A, \phi_A(P_B), \phi_A(Q_B)$ から R_A を計算する困難性に基づく

SQISign 署名

SQISign 署名 [DKL+20]

- Short Quaternion and Isogeny Signatures

  （ https://eprint.iacr.org/2020/1240 から入手可能 ）

- 同種写像に基づく初めての「実用的な」署名方式.
  署名・鍵サイズ、署名生成・検証時間が、現在使われている方式と比べて遜色がなく、そのサイズの小ささは特筆すべき
  - 128ビット安全性(NIST-1レベル安全性)パラメータ

サイズ	署名生成鍵	署名検証鍵	署名
Bytes	16	64	204

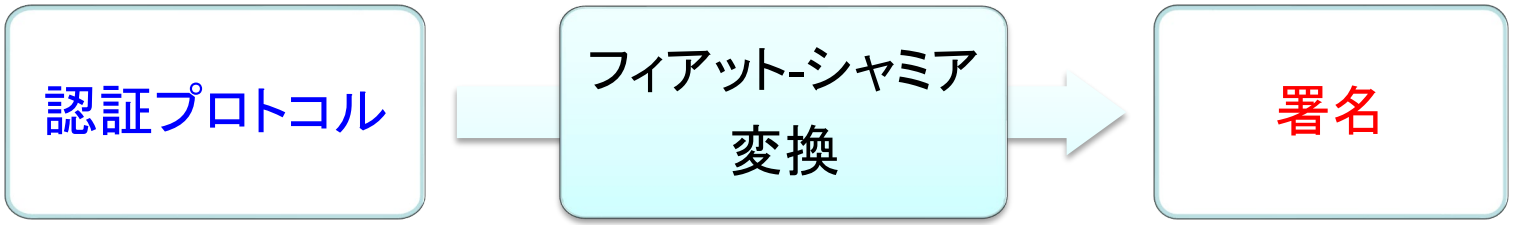
計算時間	鍵生成	署名生成	署名検証
msec	564	2,256	41

3.40GHz Intel Core i7-6700 (Skylake) CPU with Turbo Boost disabled

- [DLW21]で、同安全性で署名生成約 1 秒まで高速化に成功

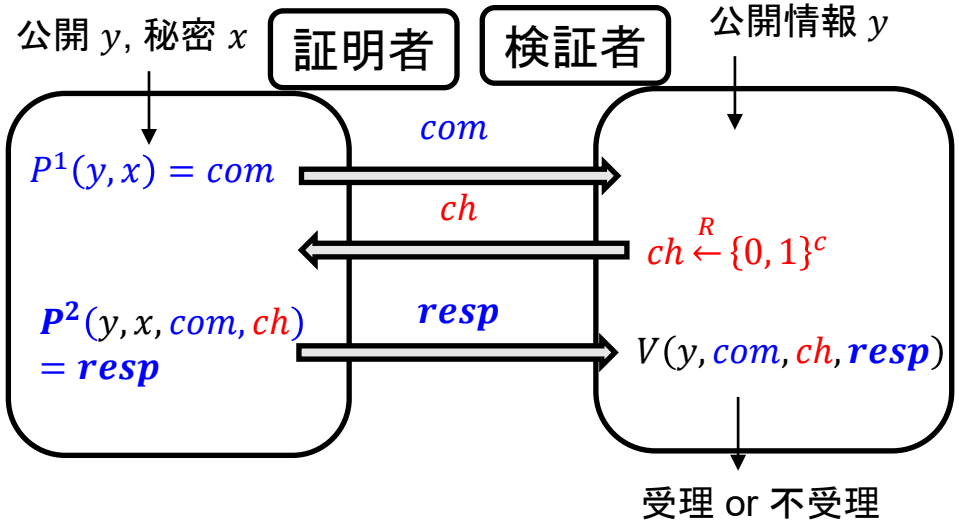
フィアット-シャミア 変換

- フィアット-シャミア変換では、最初に、認証プロトコル（Σ-プロトコル）を構成して、それを署名方式に一般的な変換法で変換している
- フィアット-シャミア（FS）変換：
  - 安全な認証プロトコル から、ランダムオラクルモデルにおいて安全な署名方式を構成する.
  - SQISign 署名は、FS変換で構成されるので、以下では、専ら、SQISign 用認証プロトコルを説明する.

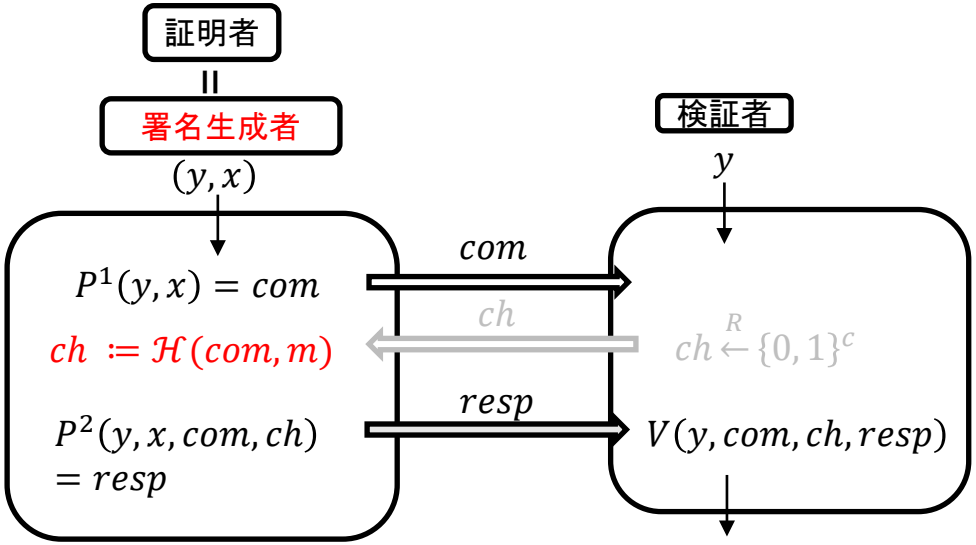


認証プロトコル と フィアット-シャミア変換

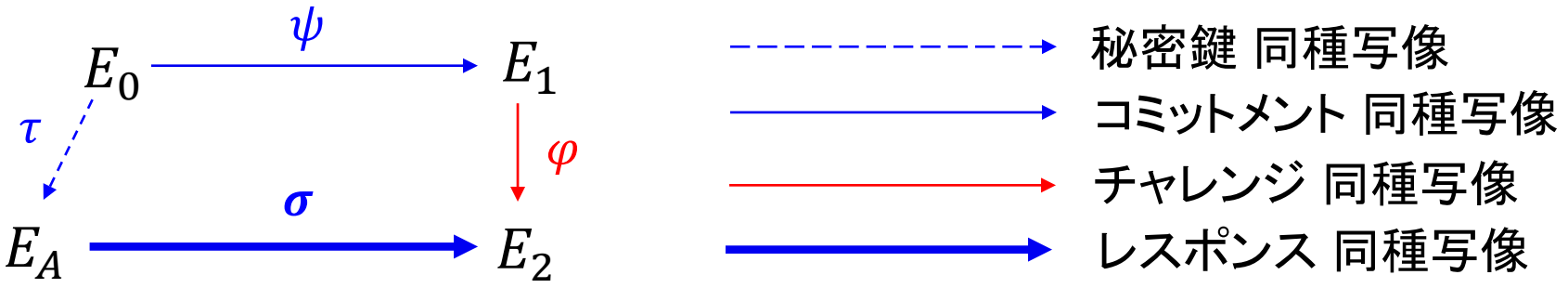
- 認証プロトコル：証明者と検証者間で、コミットメント com, チャレンジ ch, レスポンス $\boldsymbol{resp}$ を送りあい、証明者が秘密 x を知っていることを x を漏らさずに検証者に示す.



- ハッシュ関数 $\mathcal{H}$ を使って、$ch := \mathcal{H}(com, m)$ とすることで、証明者から検証者への非対話プロトコルになる.
- その ch 値に基づいて計算した $\sigma = (com, resp)$ がメッセージ m に対する署名.



SQISign用 認証プロトコル



【公開パラメータ】楕円曲線 E_0, E_A，（スムースな）奇数 D_c，　2べき $D = 2^e$

証明者は、ランダム同種写像 τ: $E_0 \to E_A$ を知っていることを、公開パラメータ以外は τ の情報を何も漏らすことなく（零知識で）証明する

【コミットメント】証明者は、ランダム同種写像 $\psi: E_0 \to E_1$ を生成する。

ψ を秘密にして、$com = E_1$ のみを検証者に送る。

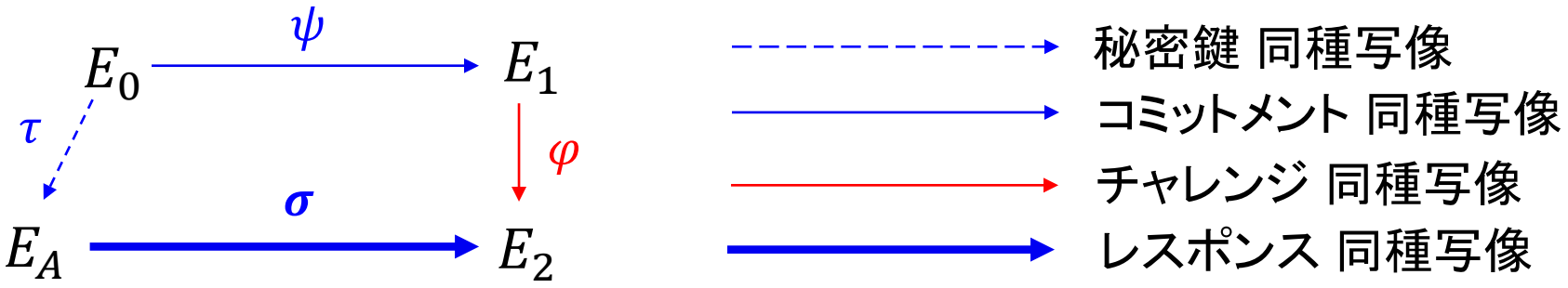
【チャレンジ】検証者は、奇数 D_c 次の巡回同種写像 $\varphi: E_1 \to E_2$ を生成する。

$ch = (\varphi: E_1 \to E_2)$ を証明者に送る。

【レスポンス】証明者は $\varphi \circ \psi \circ \hat{\tau}: E_A \to E_2$ から **2べき D 次のランダム同種写像 $\sigma: E_A \to E_2$** (s.t. $\hat{\varphi} \circ \sigma$ は巡回同種写像) を構成し $resp = \sigma$ を検証者に送る。

【検証】検証者は、$\sigma: E_A \to E_2$ が 次数 D であり、$\hat{\varphi} \circ \sigma$ が巡回同種写像であることを検証する。受理 or 不受理を出力する。

SQISign 認証プロトコル の安全性



【公開ﾊﾟﾗﾒｰﾀ】楕円曲線 $E_0, E_A \ldots$ 証明者は $\tau\colon E_0 \to E_A$ を知っていることを証明

【コミットメント】証明者は ψ を秘密にして、$com = E_1$ を検証者に送る。

【チャレンジ】検証者は、奇数 D_c 次 の巡回同種写像 $ch = \varphi$ を証明者に送る。

【レスポンス】証明者は、$\varphi \circ \psi \circ \hat{\tau}$ から計算した **2べき D次 ランダム同種写像**

$\boldsymbol{resp = \sigma\colon E_A \to E_2}$ (s.t. $\hat{\varphi} \circ \sigma$ は巡回同種写像) を検証者に送る。

- 正当性 [正しく実行すれば認証OK] は、構成より OK.
- 健全性 [τ を知らなければ認証NG] は、
  「スムース次数 自己準同型写像 計算問題」の困難性に帰着.
- ゼロ知識性 [上記以外 τ の情報漏らさず] は、いくつかのヒューリスティックな仮定の下に示されており、まだ今後、さらなる検討が必要.

SQISign署名 と Deuring 対応

- 超特異楕円曲線 E に対して自己準同型環 $\mathcal{O} = \mathrm{End}(E)$ を対応させる Deuring 対応に基づき、SQISign では $\mathbb{Q}$ 上の四元数環 $\mathcal{B}_{p,\infty}$ 内のイデアルに対し計算を行う。 ここで、$\mathcal{B}_{p,\infty} = \mathbb{Q} + \mathbb{Q}\,i + \mathbb{Q}\,j + \mathbb{Q}\,ij$, s.t., $i^2 = -1, j^2 = -p, ij = -ji$

楕円曲線サイド		四元数環サイド
超特異 j-不変量 $j(E)$	← →	$\mathcal{B}_{p,\infty}$内の極大整環 $\mathcal{O} \cong \mathrm{End}(E)$
同種写像 $\varphi: E \to E_1$		整 左$\mathcal{O}$-イデアル & 右$\mathcal{O}_1$-イデアル I_φ
自己準同型写像 $\theta \in \mathrm{End}(E)$		主イデアル $\mathcal{O}\theta$
同じ定義域・値域 $\varphi, \psi: E \to E_1$		同値なイデアル $I_\varphi \sim I_\psi$
次数 $\deg(\varphi)$		ノルム $n(I_\varphi)$
双対同種写像 $\hat{\varphi}$		共役イデアル $\overline{I_\varphi}$
超特異 j-不変量の集合		類集合 $\mathrm{Cl}(\mathcal{O})$
写像合成 $\tau \circ \rho: E \to E_1 \to E_2$		イデアル積 $I_{\tau\circ\rho} = I_\rho \cdot I_\tau$

- $p = 3 \bmod 4$ で, $E_0/\mathbb{F}_p : y^2 = x^3 + x$ with $\mathcal{O}_0 = \left\langle 1, i, \frac{i+j}{2}, \frac{1+k}{2} \right\rangle$ では  となるので、この 落とし戸 E_0 を利用して $\boldsymbol{resp = \sigma: E_A \to E_2}$ を計算！

楕円曲線同種写像グラフ
$\mathcal{G}_1(\overline{\mathbb{F}_p}, \ell)$, $\mathcal{G}_1(\mathbb{F}_p, \ell)$
と
その暗号応用

同種写像グラフ $\mathcal{G}_1(\overline{\mathbb{F}_p}, \ell)$ の構造解析 [LB20]

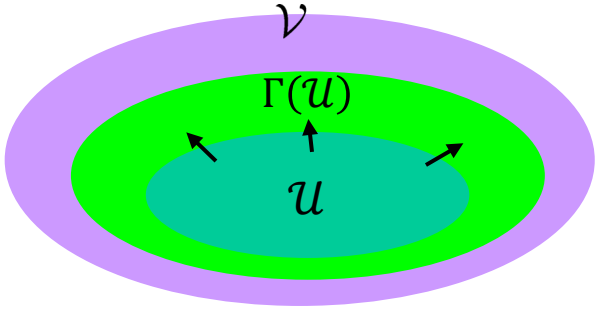
暗号解析では自己準同型環 $\mathcal{O} = \mathrm{End}(E)$ が「簡明な」楕円曲線の利用が鍵である.

- Love–Boneh は、$\deg(\alpha) \leq M$ である非整数倍自己準同型写像 α を持つ曲線を M–small 曲線と呼び、M–small 曲線に着目すると、$\mathcal{G}_1(\overline{\mathbb{F}_p}, \ell)$ 内に「解析可能な部分グラフ」が捉えられることを示した.
  - M–small 曲線の個数は、$O(M^{3/2})$ である.
  - M–small 曲線たちは、効率的に生成できる.
  - $M \ll p$ であれば、M–small 曲線の約半分は、超特異曲線である.
  - M–small 曲線の自己準同型環やそれら曲線間の同種写像は、効率的に計算可能.
  - M–small 超特異曲線たちは、基本判別式でインデックス付けされたいくつかのクラスターに分かれる.

同種写像グラフ $\mathcal{G}_1(\overline{\mathbb{F}_p}, \ell)$ の構造解析を進めて、暗号の安全性解析に貢献！

同種写像グラフに対する急撹拌性定理

楕円曲線とその ℓ- 同種写像のなすグラフ（同種写像グラフ）は、計算量理論、組み合わせ論、暗号理論等の応用上で有用な エクスパンダーグラフ になっている.



- グラフ $\mathcal{G}=(\mathcal{V},\mathcal{E})$ は、$\#\,\mathcal{U} \le \#\,\mathcal{V}/2$ である
  任意の頂点集合 $\mathcal{U}$ に対して、$\mathcal{U}$ の境界
  $\Gamma(\mathcal{U}) = \{v \in \mathcal{V} \mid \exists u \in \mathcal{U}, \{u,v\} \in \mathcal{E}\} - \mathcal{U}$ のｻｲｽﾞが
  $\#\,\Gamma(\mathcal{U}) \ge c \cdot \#\,\mathcal{U}$ である時、拡張率 $c > 0$ の ｴｸｽﾊﾟﾝﾀﾞｰｸﾞﾗﾌ という.
- エクスパンダーグラフ上のランダムウォークは、急速に一様分布に収束する.
  $O(\log(\#\mathcal{V}))$ ステップのランダムウォークをさせると、その終点の分布はグラフ上の一様分布を良い精度で近似する（急撹拌性定理）.
- 急撹拌性定理により、多くの頂点集合からの（ほぼ）一様なサンプリングが、少ないランダムネスで可能になる.
- Ramanujanグラフとは、拡張率が“最適に”良い k-正則 エクスパンダーグラフ（の族）である.

3種の同種写像ベース鍵共有

	CRS 鍵共有 (2006)	SIDH 鍵共有 (2011)	CSIDH 鍵共有 (2018)
曲線の種類	通常曲線	超特異曲線	$\mathbb{F}_p$上定義された超特異曲線
グラフの種類	(火山型)	Ramanujan グラフ $\mathcal{G}_1(\overline{\mathbb{F}_p}, 2) \cup \mathcal{G}_1(\overline{\mathbb{F}_p}, 3)$	巡回グラフの重合せ $\bigcup_{i=1,\ldots,n} \mathcal{G}_1(\mathbb{F}_p, \ell_i)$
耐量子安全性	△ 準指数時間解法	○ 指数時間解法のみ	△ 準指数時間解法
実用性	△	◎	○
特長	—	同種写像に基づきNIST標準化に提案された鍵共有はSIDHベースのみ (SIKE暗号化)	DH鍵共有と強く類似しており、リング署名などといった暗号応用技術に展開可能

CSIDH鍵共有用グラフ
$\mathcal{G}_1(\mathbb{F}_p, \ell_1) \cup \cdots \cup \mathcal{G}_1(\mathbb{F}_p, \ell_n)$

- 奇素数 p（ s.t. $p+1 = 4 \cdot \ell_1 \cdots \ell_n$), ℓ_i: 小奇素数

- 超特異 EC $E/\mathbb{F}_p$: $E(\mathbb{F}_p) \simeq \mathbb{Z}/(p+1)\mathbb{Z} \supseteq \mathbb{Z}/\ell_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/\ell_n\mathbb{Z}$
  例: $y^2 = x^3 + x$ with $p = 4 \cdot \ell_1 \cdots \ell_n - 1$
  $\mathrm{End}_{\mathbb{F}_p} E \equiv \mathcal{O} = \mathbb{Z}[\pi_p] = \mathbb{Z}[\sqrt{-p}]$, $\mathfrak{l}_i \coloneqq (\ell_i, \boldsymbol{\pi_p} - \mathbf{1}) \subset \mathcal{O}$, $\mathfrak{l}_i^{-1} \coloneqq (\ell_i, \boldsymbol{\pi_p} + \mathbf{1})$
  E を始点とする同種写像 $\phi_{\mathfrak{l}}$ s.t. $\mathrm{Ker}(\phi_{\mathfrak{l}}) = \cap_{\alpha \in \mathfrak{l}} \mathrm{Ker}(\alpha)$

- $\mathcal{G}_1(\mathbb{F}_p, \ell) \coloneqq$ $\mathbb{F}_p$上の超特異楕円曲線（の $\mathbb{F}_p$−同型類）間の $\mathbb{F}_p$上定義された ℓ−同種写像のなすグラフ.

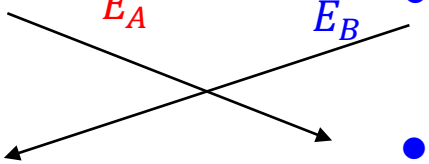
CSIDH 鍵共有

- Montgomery モデル: $E\colon y^2 = x^3 + ax^2 + x\ (a \neq \pm 2)$ に関して
  Montgomery 係数 $M(E) \coloneqq a$ とすると、$E_1/\mathbb{F}_p \cong E_2/\mathbb{F}_p \Leftrightarrow M(E_1) = M(E_2)$
- 公開パラメータ: 奇素数 p（ s.t. $p+1 = 4 \cdot \ell_1 \cdots \ell_n$), ℓ_i: 小奇素数

  超特異 EC $E/\mathbb{F}_p$: $E(\mathbb{F}_p) \simeq \mathbb{Z}/(p+1)\mathbb{Z} \supseteq \mathbb{Z}/\ell_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/\ell_n\mathbb{Z}$

  $\mathrm{End}_{\mathbb{F}_p}E \equiv \mathcal{O} = \mathbb{Z}[\pi_p] = \mathbb{Z}[\sqrt{-p}]$, $\mathfrak{l}_i \coloneqq (\ell_i, \boldsymbol{\pi_p} - \mathbf{1}) \subset \mathcal{O}$, $\mathfrak{l}_i^{-1} \coloneqq (\ell_i, \boldsymbol{\pi_p} + \mathbf{1})$

Alice	Bob
• $\mathbf{e}_A \coloneqq (e_{A1}, \ldots, e_{An}) \leftarrow [-\mu, \mu]^n$, $[\mathfrak{a}] \coloneqq [\mathfrak{l}_1^{e_{A1}} \cdots \mathfrak{l}_n^{e_{An}}] \in \mathrm{Cl}(\mathcal{O})$,	• $\mathbf{e}_B \coloneqq (e_{B1}, \ldots, e_{Bn}) \leftarrow [-\mu, \mu]^n$, $[\mathfrak{b}] \coloneqq [\mathfrak{l}_1^{e_{B1}} \cdots \mathfrak{l}_n^{e_{Bn}}]$,
• $\phi_A\colon E \to E_A \coloneqq [\mathfrak{a}]E$	• $\phi_B\colon E \to E_B \coloneqq [\mathfrak{b}]E$
• $K_{\mathrm{Alice}} \coloneqq M([\mathfrak{a}]E_B)$	• $K_{\mathrm{Bob}} \coloneqq M([\mathfrak{b}]E_A)$



- 共有鍵: $K_{\mathrm{Alice}} = M([\mathfrak{a}]E_B) = M([\mathfrak{a}][\mathfrak{b}]E) = M([\mathfrak{b}]E_A) = K_{\mathrm{Bob}}$
- 安全性: $E, E_A \coloneqq [\mathfrak{a}]E$ から $[\mathfrak{a}]$ を計算することの困難性に基づく

3種の同種写像ベース鍵共有

	CRS 鍵共有 (2006)	SIDH 鍵共有 (2011)	CSIDH 鍵共有 (2018)
曲線の種類	通常曲線	超特異曲線	$\mathbb{F}_p$上定義された超特異曲線
グラフの種類	(火山型)	Ramanujan グラフ $\mathcal{G}_1(\overline{\mathbb{F}_p}, 2) \cup \mathcal{G}_1(\overline{\mathbb{F}_p}, 3)$	巡回グラフの重合せ $\bigcup_{i=1,\ldots,n} \mathcal{G}_1(\mathbb{F}_p, \ell_i)$
耐量子安全性	△ 準指数時間解法	○ 指数時間解法のみ	△ 準指数時間解法
実用性	△	◎	○
特長	—	同種写像に基づきNIST標準化に提案された鍵共有はSIDHベースのみ (SIKE暗号化)	DH鍵共有と強く類似しており、リング署名などといった暗号応用技術に展開可能

同種写像グラフ
と
格子暗号の安全性

3種の同種写像ベース鍵共有

	CRS 鍵共有（2006）	SIDH 鍵共有（2011）	CSIDH 鍵共有（2018）
曲線の種類	通常曲線	超特異曲線	$\mathbb{F}_p$上定義された超特異曲線
グラフの種類	（火山型）	Ramanujan グラフ $\mathcal{G}_1(\overline{\mathbb{F}_p}, 2) \cup \mathcal{G}_1(\overline{\mathbb{F}_p}, 3)$	巡回グラフの重合せ $\bigcup_{i=1,\ldots,n} \mathcal{G}_1(\mathbb{F}_p, \ell_i)$
耐量子安全性	△ 準指数時間解法	○ 指数時間解法のみ	△ 準指数時間解法
実用性	△	◎	○
特長	—	同種写像に基づきNIST標準化に提案された鍵共有はSIDHベースのみ（SIKE暗号化）	DH鍵共有と強く類似しており、リング署名などといった暗号応用技術に展開可能

通常楕円曲線同種写像グラフの暗号応用 [JMV09]

$\mathrm{Cl}(\mathcal{O}_\Delta)$: 判別式 $\Delta(<0)$ の虚 2 次 整環 (オーダー) $\mathcal{O}_\Delta$ のｲﾃﾞｱﾙ類群

$\mathrm{Ell}_p(\mathcal{O}_\Delta)$: $\mathcal{O}_\Delta$ を自己準同型環にもつ $\overline{\mathbb{F}_p}$ 上の楕円曲線 の $\overline{\mathbb{F}_p}$-同型類全体

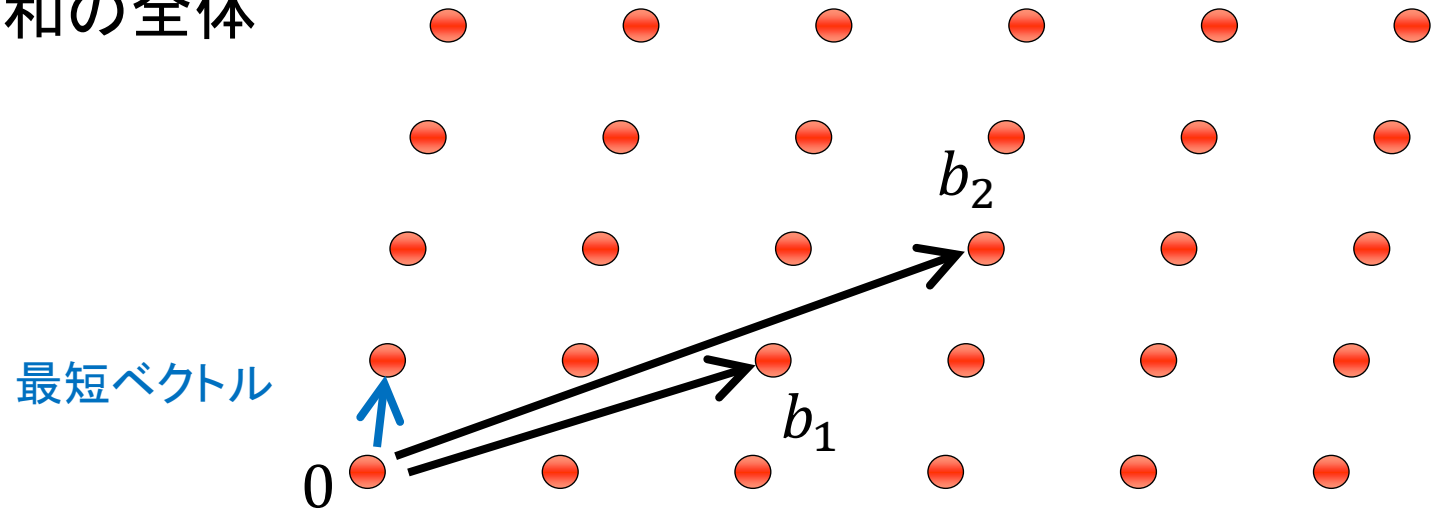
- 楕円曲線集合へのｲﾃﾞｱﾙ類群作用（CM作用）:
  $[a] * E_0 :=$ [$\mathrm{Ker}(\phi_a) = \bigcap_{z\in a} \mathrm{Ker}(z)$ となる同種写像 ϕ_a の値域曲線 E_1]

$$
\begin{array}{rccc}
* : & \mathrm{Cl}(\mathcal{O}_\Delta) \times \mathrm{Ell}_p(\mathcal{O}_\Delta) & \longrightarrow & \mathrm{Ell}_p(\mathcal{O}_\Delta) \\
 & (\ [a], \quad E_0 \ ) & \mapsto & E_1 = [a] * E_0
\end{array}
$$

- E_0 を含む通常楕円曲線同種写像グラフとして、小ノルム素イデアル $\{\mathfrak{p} \in \mathrm{Cl}(\mathcal{O}) : N\mathfrak{p} \le x\}$ とその逆数イデアルを辺とする ケーリーグラフ で与えられるものを考えると、2次指標に関する GRH の下で、それが 急攪拌性定理 を満たすことが示される.
- E_0 から少ないステップ数のランダムウォークによって、このグラフ内の“ランダムな” 楕円曲線への同種写像が得られる.
- E_0 上の楕円曲線離散対数問題 を“ランダム” E 上の問題へ効率的に帰着することで E_0 上の計算問題の安全性保証を与える（ランダム自己帰着性）

格子問題 SVP と 格子暗号

- 格子 = 線形独立なベクトル $b_1, \cdots, b_n \in \mathbb{Q}^n$ の整数係数の線形和の全体



- 最短ベクトル探索問題 SVP (Shortest Vector Problem)
  = 原点以外で一番短い格子点を探す問題
  - 暗号で使用する場合 $n > 400$ 程度
  - 量子コンピュータで効率的に解くアルゴリズムが知られていない
- 格子暗号 = SVP などの格子問題困難性に基づく暗号
- イデアル格子暗号 = 代数体整環のイデアル格子による格子暗号

格子問題のランダム自己帰着性

楕円曲線集合へのｲﾃﾞｱﾙ類群作用 の類似で、イデアル格子集合へのアラケロフ類群作用を考えることで、ヘッケ L-関数 ERHの下で、Ideal-SVP問題のランダム自己帰着性が示された（K.de Boer et al. CRYPTO 2020）.

2つのランダム自己帰着 ケーリーグラフ

	ECDLP	Ideal-SVP
頂点集合	{楕円曲線群}	{イデアル格子（群）}
作用する群	虚2次整環のイデアル類群	アラケロフ類群
辺集合	{小ノルム 同種写像}	{小ノルム “近似等長”写像}

- 計算量理論では、専ら (Ideal-SVP問題の) worst-case 計算量 を論じるが、暗号理論では、通常 average-case が安全性に関係する. であるので、それら 2つの計算量間にタイトな帰着関係があることが望ましい.

Ideal-SVP 問題のランダム自己帰着性を利用して、かなり精度よい Ideal-SVP問題の worst-case / average-case 帰着を示せる.

⇒ ｲﾃﾞｱﾙ格子暗号の安全性解析に寄与

種数2 CGL ハッシュ関数
と
超特殊 (superspecial) 同種写像グラフ
[T18, FT19, CDS20, CS20, KT20, FS21a, FS21b, …]

“Efficient Algorithms for Isogeny Sequences and Their Cryptographic Applications” [T18]

CREST Crypto-Math Project 報告集, 2018

- (改善された) CGL-型 同種写像列計算アルゴリズム
  - 楕円曲線間の 2-同種写像列計算 [YT13]
  - 楕円曲線間の 3-同種写像列計算 [TTT17]
  - 種数 2 超楕円ヤコビアン J_C 間の (2,2)-同種写像列計算
    (= Richelot アルゴリズム) [S05, TY09, FT19, CDS19]
  - 種数 2 超楕円ヤコビアン J_C 間の (3,3)-同種写像列計算

＊種数 2 曲線 C: $y^2 = f(x)$: $f(x)$は有限体 $\mathbb{F}_q$ 係数 5次または 6次多項式

- 種数 2 同種写像暗号, e.g., CGL ハッシュ関数
  - [T18]の出版後、[FT19] で、種数 2 CGL ハッシュ関数 in [T18] に衝突が見つかることが指摘されたが、Castryck ら [CDS20] によって、超特殊(超特別)同種写像グラフを用いる回避法が提案された
  - 更に、Costelloら [CS20] は、種数2同種写像グラフの構造を利用した(指数時間)攻撃法を提案した

超特殊 (superspecial) 種数 2 曲線 と そのヤコビ多様体

- 種数 2 曲線 $C: Y^2 = \prod_{m=0}^{5}(X - a_m)$ 上の Richelot 同種写像 は、分岐点 $(a_m, 0)$ を用いて計算でき、楕円曲線上の 2-同種写像の自然な拡張である.

- 超特殊アーベル曲面間 同種写像グラフを用いた CGLハッシュ関数

  - C が超特異曲線 ⇔ そのヤコビ多様体 J_C が、超特異楕円曲線の直積と 同種 である

  - C が超特殊曲線 ⇔ そのヤコビ多様体 J_C が、超特異楕円曲線の直積と 同型 である

- 任意の超特異楕円曲線 E_i $(i = 1,2,3,4)$ に対して、$E_1 \times E_2 \cong E_3 \times E_4$ が成り立つ. つまり、J_C の同型類だけでなく、その主偏極も込めた (J_C, C) の同型類を頂点とするグラフを考えないといけない.

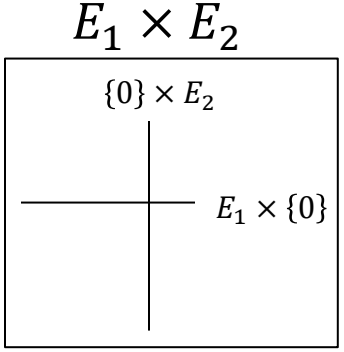
$$J_C = \{\Sigma\, n_i P_i \mid P_i \in C, n_i \in \mathbb{Z}, \Sigma\, n_i = 0\}/\sim \text{ (線形同値)}$$

$\cup$ アーベル曲面

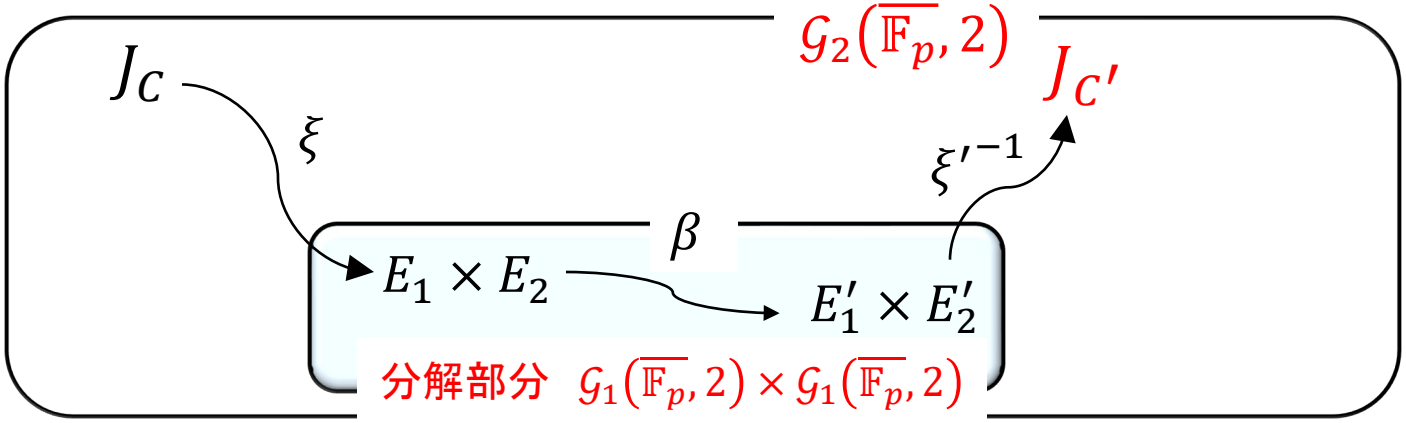
$C = \{P - P_0\}$, P_0 : 基点 ($C^2 = 2$)

Costello-Smith 種数 2 同種写像探索ｱﾙｺﾞﾘｽﾞﾑ [CS20]

- 分解部分ｸﾞﾗﾌ を利用して、同種写像探索を効率化
  - 分解部分ｸﾞﾗﾌ頂点集合
    $= \{(E_1 \times E_2) : E_1, E_2 :$ 超特異楕円曲線$\}$
  - 入力：“p.p.超特殊” 種数2 ヤコビアン $J_C, J_{C'}$ (非分解)
    出力：$\rho : J_C \to J_{C'}$ となる道（Richelot 同種写像列）



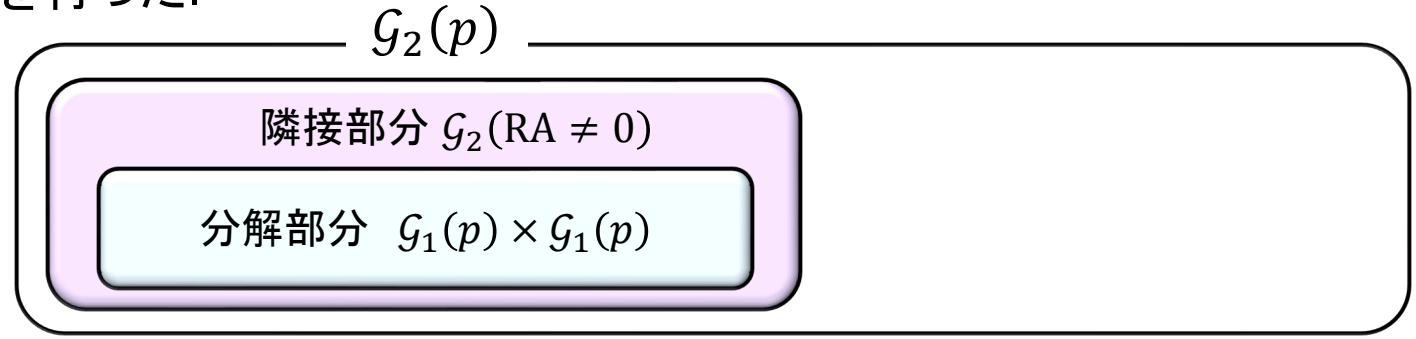
1. J_C と $E_1 \times E_2$ を結ぶ道 ξ を探索する
2. $J_{C'}$ と $E_1' \times E_2'$ を結ぶ道 ξ' を探索する
3. $\beta_1 : E_1 \to E_1'$, $\beta_2 : E_2 \to E_2'$ を探索して、$\beta = \beta_1 \times \beta_2$ とする
4. $\rho = {\xi'}^{-1} \circ \beta \circ \xi : J_C \to J_{C'}$ を出力する



- 古典計算量：$O(p^{1.5}) \to O(p^1)$, 量子計算量：$O(p^{0.75}) \to O(p^{0.5})$ に改良.

我々の論文 [KT20] の成果概要

- 超特殊 Richelot 同種写像グラフ $\mathcal{G}_2(p)(=\mathcal{G}_2(\overline{\mathbb{F}_p}, 2))$ 構造解析
  - Costello らが着目した $\mathcal{G}_1(p)\times\mathcal{G}_1(p)$ の周辺に，$\mathrm{RA}\neq 0$ で特徴づけられる部分グラフ $\mathcal{G}_2(\mathrm{RA}\neq 0)$ が存在して、$\mathcal{G}_1(p)\times\mathcal{G}_1(p)$ と $\mathcal{G}_2(\mathrm{RA}\neq 0)$ との隣接状況を明らかにした.
  - 被約自己同型群 $\mathrm{RA}=\mathrm{RA}(C)=\mathrm{Aut}(C)/\langle\iota\rangle$ (ι: 超楕円対合). [IKO86]で、$\mathrm{RA}(C)$ の分類を用いて、種数2 超特殊曲線の数え上げが行われた. [KT20]では、それに基づき、超特殊 Richelot 同種写像の分類と数え上げを行った.

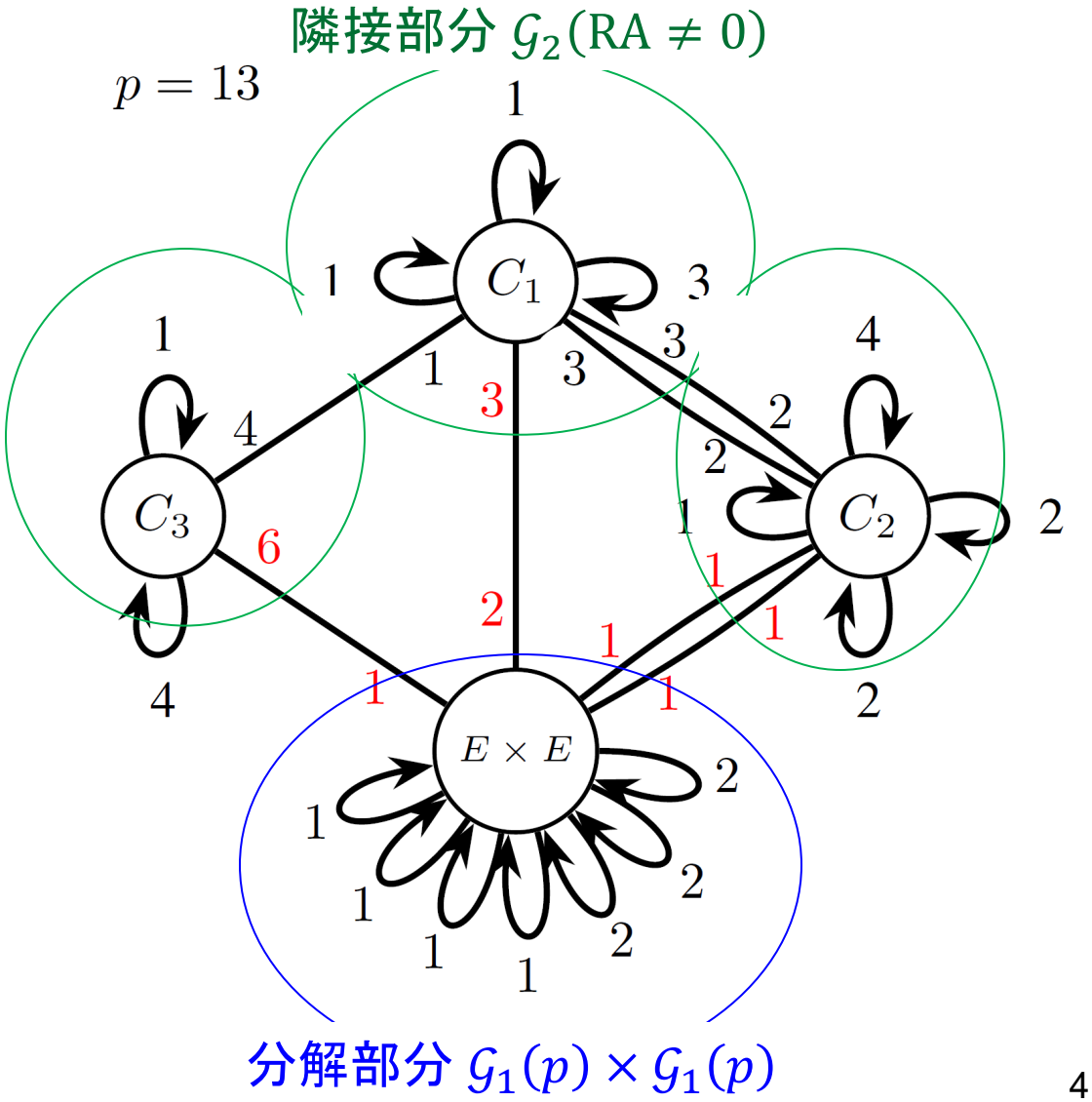


[IKO86] T. Ibukiyama, T. Katsura, F. Oort, “Supersingular curves of genus two and class numbers”, Compositio Math., 1986.

[KT20] T. Katsura, K. Takashima, “Counting Richelot isogenies between superspecial abelian surfaces”, ANTS XIV, 2020.

論文 [KT20] の成果概要

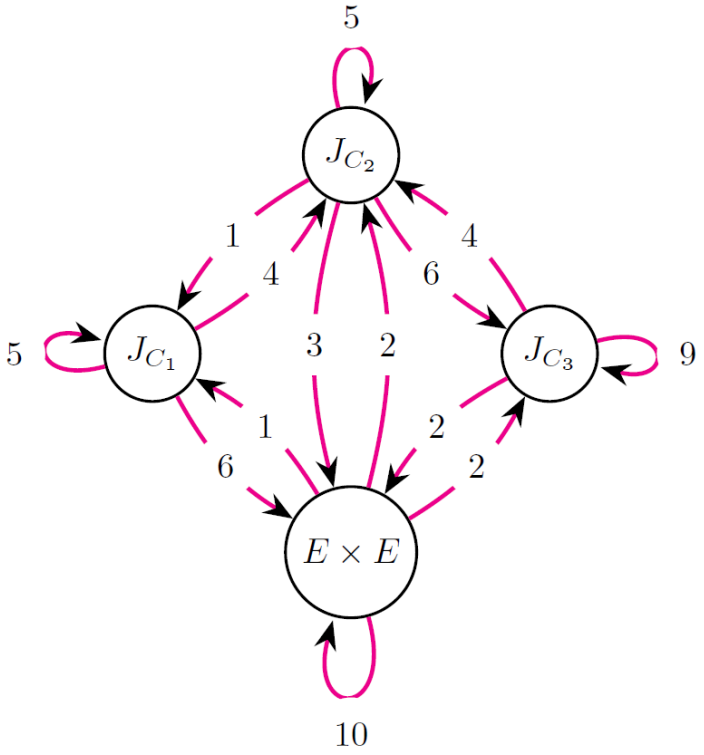
- Castryckらは、[CDS20] 定理2で、隣接部分の頂点から分解部分へ出る辺の個数が 6 以下であることを示した. しかし、以下の意味で不十分な結果であった.
  - 正確な個数を求めていない.
  - 証明が計算機によっていて、根拠が不明瞭.
- 我々は、代数幾何的な[IKO86]の結果に基づいて、正確 かつ 概念的にクリアな形で、それらの個数勘定に行った(右図参照).



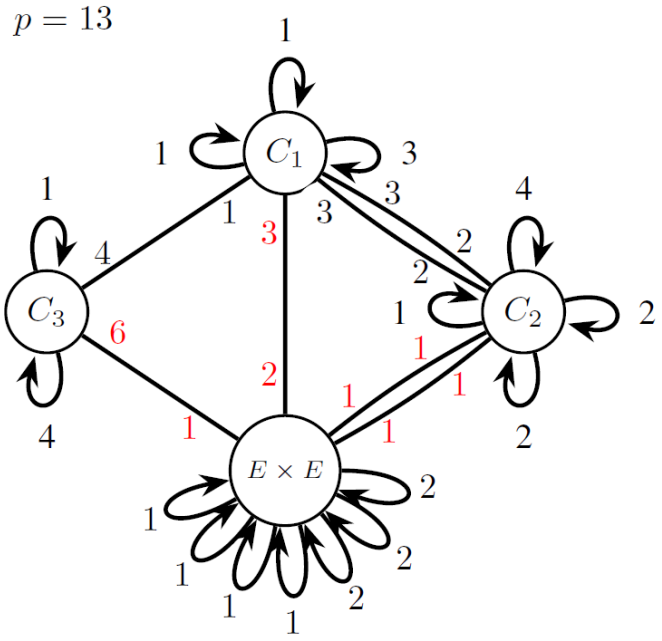
論文 [KT20] の成果概要

- Castryckらの論文[CDS20]でも、同様の図が載っているが、我々の勘定法は、より精密であり（同型性を加味した勘定）、一般の大素数 p に対しても、計算できるが、[CDS20] の方法ではそうでない.

[CDS20] の図1



[KT20] の図



論文 [KT20] の成果概要

- 実際、我々の勘定法により、以下のような具体的な 2次式の等式として、
  $G_2(\mathrm{RA} \neq 0)$ から $G_1(p) \times G_1(p)$ への（同型を除いた）辺の数
  $= G_1(p) \times G_1(p)$ から $G_2(\mathrm{RA} \neq 0)$ への（同型を除いた）辺の数
  を得た.

Theorem (The total number of Richelot isogenies from $J(C)$)

$$
\begin{aligned}
N_{\mathrm{nd}} &= 15n_0 + 11n_1 + 7n_2 + 8n_3 + 5n_4 + 4n_5 + 3n_6 \\
&= \frac{(p-1)(p+2)(p+7)}{192} - 3\{1 - (\frac{-1}{p})\}/32 + \{1 - (\frac{-2}{p})\}/8, \qquad (*)
\end{aligned}
$$

$$
\begin{aligned}
N_{\mathrm{nd}\to\mathrm{d}} &= n_1 + n_2 + 2n_3 + 2n_4 + n_5 \\
&= \frac{(p-1)(p+3)}{48} - \{1 - (\frac{-1}{p})\}/8 + \{1 - (\frac{-3}{p})\}/6.
\end{aligned}
$$

$G_2(\mathrm{RA} \neq 0)$ から $G_1(p) \times G_1(p)$ への（同型を除いた）辺の数

Theorem (The total number of Richelot isogenies from elliptic curve products)

The total number of non-decomposed Richelot isogenies $N_{\mathrm{d}\to\mathrm{nd}}$ (resp. decomposed Richelot isogenies $N_{\mathrm{d}\to\mathrm{d}}$) up to isomorphism outgoing from decomposed principally polorized superspecial abelian surfaces is equal to

$$
N_{\mathrm{d}\to\mathrm{nd}} = \frac{(p-1)(p+3)}{48} - \{1 - (\frac{-1}{p})\}/8 + \{1 - (\frac{-3}{p})\}/6,
$$

$$
N_{\mathrm{d}\to\mathrm{d}} = \frac{(p-1)(3p+17)}{96} + (p+6)\{1 - (\frac{-1}{p})\}/16 + \{1 - (\frac{-3}{p})\}/3.
$$

$G_1(p) \times G_1(p)$ から $G_2(\mathrm{RA} \neq 0)$ への（同型を除いた）辺の数

高種数同種写像グラフ

- [Kat21] では、種数 2 時の [KT20]の方法を種数 3 時に適用・拡張して、種数3 分解 Richelot同種写像の特徴づけを与えた.

  [Kat21] T. Katsura, “ Decomposed Richelot isogenies of Jacobian varieties of curves of genus 3 ”, To appear in Journal of Algebra

- [KT21] では、一般種数の 超楕円曲線 と一般化 Howe 曲線の時に、分解 Richelot同種写像の特徴づけを与えた.

  [KT21] T. Katsura, K. Takashima, “ Decomposed Richelot isogenies of Jacobian varieties of hyperelliptic curves and generalized Howe curves ”, arxiv:2108.06936.

- 高種数同種写像グラフに関する論文
  Florit-Smith [FS21a, FS21b], Jordan-Zaytman [JZ20],
  Aikawa-Tanaka-Yamauchi [ATY22]

まとめ

- 超特異楕円曲線同種写像に基づくCGL ハッシュ関数とSIDH, CSIDH 鍵共有を紹介するとともに、実用的な同種写像ベース SQISign 署名方式も紹介した.

- それらが基づくグラフ $\mathcal{G}_1(\overline{\mathbb{F}_p}, \ell)$, $\mathcal{G}_1\left(\mathbb{F}_p, \ell\right)$ の数理（群作用、急攪拌性、部分グラフ構造）が、暗号解析に重要な役割を果たしていることも紹介した.

- さらに、通常曲線同種写像グラフの数理が、格子暗号の安全性と関係していることも紹介した.

- 種数2同種写像暗号の例として、超特殊 Richelot 同種写像グラフに基づく 種数2 CGL ハッシュ関数と、我々のグラフ解析に関する成果を紹介した.

主な参考文献

[CLG09] D.X. Charles, K.E. Lauter, E.Z. Goren,
"Cryptographic Hash Functions from Expander Graphs ",
J. Crypto., 22(1), 93-113, 2009.

[JMV09] D. Jao, S. D. Miller, and R. Venkatesan.
" Expander graphs based on GRH with an application to elliptic curve cryptography. J. Number Theory, 2009.

[DJP14] L. De Feo, D. Jao, J. Plut,
"Towards quantum-resistant cryptosystems from supersingular elliptic curve Isogenies ", J. Math. Crypt. 2014.

[CJS14] A.M. Childs, D. Jao, and V. Soukharev.
" Constructing elliptic curve isogenies in quantum subexponential time ". J. Math. Crypt. 2014.

主な参考文献

[T18] K. Takashima,
" Efficient Algorithms for Isogeny Sequences and Their Cryptographic Applications ", Mathematical Modelling for Next-Generation Cryptography, MfI, vol.29, 2017.

[CLM+18] W. Castryck, T. Lange, C. Martindale, L. Panny, J. Renes, " CSIDH: an efficient post-quantum commutative group action ", ASIACRYPT 2018.

[FT19] E.V. Flynn, Y.B. Ti,
" Genus Two Isogeny Cyptography ", PQCrypto 2019.

[CDS20] W. Castryck, T. Decru, B. Smith
" Hash functions from superspecial genus-2 curves using Richelot isogenies ", J. Math. Crypt. 2020.

主な参考文献

[KT20] T. Katsura, K. Takashima,
" Counting Richelot isogenies between superspecial abelian surfaces ", ANTS XIV, 2020.

[LB20] J. Love, D. Boneh, " Supersingular Curves With Small Non-integer Endomorphisms ", ANTS XIV, 2020.

[BDPW20] K. de Boer, L. Ducas, A. Pellet-Mary, B. Wesolowski,
" Random Self-reducibility of Ideal-SVP via Arakelov Random Walks ", CRYPTO 2020.

[CS20] C. Costello, B. Smith,
" The supersingular isogeny problem in genus 2 and beyond ", PQCrypto 2020.

[DKL+20] L. De Feo, D. Kohel, A Leroux, C. Petit, B. Wesolowski,
" SQISign: compact post-quantum signatures from quaternions and isogenies ". ASIACRYPT 2020.

ご清聴 ありがとうございました。