耐量子計算機暗号と量子情報の数理

同種写像暗号１：楕円曲線と同種写像グラフ

三菱電機　情報技術総合研究所 / JST ACT-X

相川　勇輔

アナウンス

- 2022/7/30にCastryckとDecruによって同種写像暗号SIDH（cf. 守谷さんのご講演）に対する深刻な鍵復元攻撃が提案された

[CD22]An efficient key recovery attack on SIDH (preliminary version)

https://eprint.iacr.org/2022/975

緊急企画

この論文の内容と影響の範囲について、現段階での認識を共有します：

8/4（木） 12:00-12:30

タイトル：SIDHへの鍵復元攻撃[CD22]について

発表者：小貫啓史

この講演の目的

- 同種写像暗号分野のオーバービューを提供すること
- 同種写像暗号を構築する際の数学的基礎付けや、その実装可能性を実現するアイデアを共有すること
  - 楕円曲線って何？超特異って？同種写像グラフって？
  - 同種写像問題ってどう定式化される？
  - 計算効率性が悪いみたいだけどなんで？
  - ECCが超楕円に発展したような展開は同種ではどうなの？
- 【お詫び】同種写像問題へのDeuring対応によるアプローチについては時間の都合上触れられません・・・！
  （小貫さんのご講演である程度触れられる予定です）

アジェンダ

1. 概略：同種写像暗号
2. 楕円曲線と同種写像
3. 同種写像の計算
4. 超特異同種写像グラフ
5. 高次元への研究の展開：アーベル多様体の同種写像グラフ

1 概略：同種写像暗号

■同種写像の計算困難性に基づく暗号方式の総称

同種写像の像となる曲線が公開情報

同種写像が秘密情報

（一般）超特異同種写像問題

同種な超特異楕円曲線E_1とE_2が与えられたとき、
同種写像$f: E_1 \to E_2$を求めよ

実際はこの問題への帰着を持つ問題の困難性の仮定の下で暗号を構成

特徴を一言で述べると、、、

■暗号として

- 総じてデータサイズが小さい

	sk	pk	ct
SIKE	350	197	236
Kyber	1632	800	768

in bytes

→データサイズが大きくなりがちなPQC他候補の弱点を克服

- 一方でアルゴリズムの計算量が重い
- さらに応用、高機能化に弱い

■分野として

- 数学（主に整数論）とのインタラクションが盛ん
  →ここ１，２年で急激に難しくなった印象
- 新しい分野のため安全性の、特に計算量的観点からの研究が発展途上

研究の方向性

■超特異同種写像グラフを利用する

- CGL-ハッシュ関数
- SIDH鍵共有: NIST標準化Round 4候補
- SQISign署名

など

高次元類似の研究へ発展

■アーベル多様体の同種写像グラフ

- CGL-ハッシュの類似
- グラフの局所的な記述や拡張性の研究　など

■イデアル類群の群作用を利用する

- CRS鍵共有: 通常曲線を利用し、実装性を伴わない
- CSIDH鍵共有: 超特異曲線を利用し、効率的な方式
  - CSI-FiSh: CSIDHベースのデジタル署名
  - SiGamal, SimS: CSIDHベースの暗号化　など

青：相川の講演
緑：守谷さんのご講演
橙：小貫さんのご講演

Development of Isogeny-based Crypto

2006 2009 2011 2018 2020

From Supersingular Isogeny Graphs

From Group Action

Higher Dimensional Analogue

Mathematical Foundation

[CGL09] CGL Hash function

[JD11] SIDH Key exchange

😢Serious Attack [CD22]

Under standardization process since 2016

[DKL+20]SQISign Signature

😢inefficient

[C06],[RS06] C-RS Key exchange

[CLM+18] CSIDH Key exchange

[BKV19]CSI-FiSh Signature

[T18] CGL-like hash from supersingular abelian var's

[CDS20]CGL-like hash from superspecial abe

🐻Attack [FT19]

😢Reduction to 1 dim [CS20]

Complex multiplication on ordinary curves

Complex multiplication on supersingular curves

Deuring Correspondence

[KT20], [FS21a,b], [JZ20], [ATY22] Analysis of isogeny graphs of superspecial abelian var's

[P](1990) SSIG are Ramanujan

[CH17],[MOAT22] etc Isogeny Fomula

and more...

2 楕円曲線と同種写像

約束

- pは素数を表す
  （しばしば大きい、512ビットとか、もちろん2でも3でもない）
  - 例えば次のような規模
    $\mathrm{p} = 5326738796327623094747867617954605554069371494832722337$
    $612446642054009560026576537626892113026381253624626941643949447926628812416213732889428802880650659$ (CSIDH-512)
- ℓはpと異なる素数を表す
  （しばしば小さい、2とか3とか）
- qは素数pのベキp^nを表す（あまり出番はない）

有限体

- 有限体とは元の個数が有限個の体
- pを素数として$q = p^n$とすると元の個数がqの有限体が（同型を除き）一意に存在し、それを$\mathbb{F}_q$とかく
  このとき、体の標数はp（1をp個足すと0になる）である、という
- $\mathbb{F}_p \subset \mathbb{F}_q$であり、 $\mathbb{F}_q$は$\mathbb{F}_p$のn次の拡大である、という
  また$\mathbb{F}_p$を素体という
- $\mathbb{F}_q$の代数閉包を$\overline{\mathbb{F}}_q$と書く
- この講演では素体の**二次拡大$\mathbb{F}_{p^2}$が大事**

楕円曲線

定義（<u>有限体上</u>の楕円曲線）：
pを（５以上の）素数とし$\mathbb{F}_q$を有限体とする。$\mathbb{F}_q$上の**楕円曲線E**とは、$\mathbb{F}_q$上の種数１の非特異射影代数曲線のこと。以下のモデルを持つ：

$$Y^2 = X^3 + aX + b \left(a, b \in \mathbb{F}_q, 4a^3 + 27b^2 \neq 0\right).$$

- $E(\mathbb{F}_q)$でEの$\mathbb{F}_q$上の解に無限遠点∞を付け加えた集合を表す

$$E\left(\mathbb{F}_q\right) = \left\{(x, y) \in \mathbb{F}_q^2 \,\middle|\, y^2 = x^3 + ax + b\right\} \cup \{\infty\}$$

⇒ **アーベル群の構造が定まる**（∞を単位元とする）

- この発表では、**有限体上の楕円曲線のみ**を考える

モンゴメリー曲線

■実際には暗号ではモンゴメリー曲線をしばしば使う

楕円曲線のモンゴメリーモデルとは

$$y^2 = x^3 + Ax^2 + x \qquad A \in \mathbb{F}_q$$

のことであり、このモデルで表示された楕円曲線を**モンゴメリー曲線**という[M87]。
また、係数Aを**モンゴメリー係数**とよぶ。

■単一座標系を持つ： $\mathrm{x} : E_A \to \mathbb{P}^1; (x, y) \mapsto x.$

この時、$\mathrm{x}(P) = \mathrm{x}(Q)$
$\Leftrightarrow P = Q$ or $P = -Q$

効率的なスカラー倍演算が可能に

同種写像

定義（同種写像）：
E_1, E_2を楕円曲線とする。有理多項式で表せる群準同型写像$f: E_1 \to E_2$を**同種写像**とよぶ。またこのとき、E_1とE_2は**同種である**という。

- 同種写像には次数が定義され、n次の同種写像のことを
  n-同種写像という（しばしば**素数ℓ次の同種写像**を考える）

- $n-$同種写像$f: E_1 \to E_2$があるとき$\hat{f}: E_2 \to E_1$であって$\hat{f} \circ f = [n]$
  なるものが唯一存在し、これをfの双対同種写像という

定理（Tate）：
楕円曲線E_1とE_2が$\mathbb{F}_q$上同種であることと、$\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$は同値

同種写像の例

- 楕円曲線E上のスカラー倍算はn^2 −同種写像（$p \nmid n$）：

$$[n]: E \to E; P \mapsto nP$$

- スカラー倍算の核を$E[n]$と書く

$$E[n] = \{P \in E(\overline{\mathbb{F}}_q) \mid nP = \infty\}$$

  - $E[n]$をねじれ部分群といい、その元を**ねじれ点**という
  - $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ $(p \nmid n)$

例えば$E: Y^2 = X^3 + X$のとき、2倍算は以下で書ける：

$$[2](x, y) = \left(\frac{(x^2-1)^2}{4(x^3+x)}, \frac{y(x^6+5x^4-5x^2-1)}{8(x^3+x)} \right)$$

j –不変量

- Eのj-不変量を以下で定義：

$$j_E = 1728\frac{4a^3}{4a^3 + 27b^2}$$

- E_1とE_2が同型であることと$j_{E_1} = j_{E_2}$は同値
  - より厳密には$\overline{\mathbb{F}}_q$上で同型
  - j-不変量は等しいが素体$\mathbb{F}_p$上では同型でない場合もある

- 通信者間で曲線の情報を共有するときは、しばしばこの値を用いる

通常曲線と超特異曲線

- 有限体上の楕円曲線は**通常曲線**と**超特異曲線**に分類できる
- 標数p上の超特異曲線は約$\frac{p}{12}$個存在する
  - ランダムに曲線を生成したとき超特異である確率はおおよそ$\frac{1}{p}$
- **標数p上の超特異曲線は全て$\mathbb{F}_{p^2}$上で定義される：$j \in \mathbb{F}_{p^2}$**
  - j-不変量を鍵として共有するとき**サイズは$2\log p$くらい**
- 超特異曲線Eは位数で特徴づけられる：

例
- $\#E(\mathbb{F}_p) = p + 1$
- $\#E(\mathbb{F}_{p^2}) = (p+1)^2 \ or \ (p-1)^2$

超特異曲線と同種な曲線は超特異
（Tateの定理）

pで位数が決まるので群論的にも扱いやすい

自己準同型環

■ Eの自己準同型環を以下の記号でかく：

$$\mathrm{End}(E)=\{f: E \to E \mid f\text{は同種写像}\}$$

Eの群構造から定まる和と合成による積で環をなす

■ Eが標数p上の楕円曲線とする

- 通常曲線のとき$\mathrm{End}(E)$は虚2次体のオーダー；例えば$\mathbb{Z}[\sqrt{-D}]$などの形

Dはある正整数

- 超特異曲線のとき$\mathrm{End}(E)$はpと∞で分岐する四元代数$B_{p,\infty}$の極大オーダー

例　$p \equiv 3 \bmod 4$の時、$E_0: Y^2 = X^3 + X$は超特異曲線であり、

$$\mathrm{End}(E_0) \simeq \left\langle 1, i, \frac{1+k}{2}, \frac{i+j}{2} \right\rangle_{\mathbb{Z}}$$

このとき$B_{p,\infty} \simeq \mathbb{Q}\langle i, j\rangle$
$(i^2 = -1, j^2 = -p,$
$k = ij = -ji)$

3 同種写像の計算

同種写像計算の基本命題

命題：

Eを体$\mathbb{F}_q$上の楕円曲線とし、**Gを$E(\overline{\mathbb{F}}_q)$の有限部分群**とする。このとき、楕円曲線$E'$と次数$\#G$の分離的同種写像$\phi_G: E \to E'$で核が$G$のものが存在する。$E'$は同型を除いて$G$から一意に定まるので**$E/G$**と書く。

- 同種写像の情報を**部分群（つまり点の集合）の情報**として持てる
- 素数次数の場合核は巡回群なので**生成元（点）が同種写像の情報**

Eが始点の
ℓ-同種写像

$\longleftrightarrow$

$E[\ell] \simeq \mathbb{F}_\ell \times \mathbb{F}_\ell$の
1次元部分空間$\langle P \rangle$

$\ell + 1$個

Véluの公式（参考です、読まなくてOK）

定理(Véluの公式[V71]):

$E: Y^2 = X^3 + aX + b$とし、GをEの有限部分群とする。

分割$G = \{\infty\} \cup G^+ \cup G^-$を$P \in G^+ \Leftrightarrow -P \in G^-$で定める。

また$P = (x_P, y_P) \in G^+$に対して,

$$g_P^x = 3x_P^2 + a,\ g_P^y = -2y_P, v_P = 2g_P^x,\ u_P = (g_P^y)^2,\ v = \sum_{P \in G^+} v_P, w = \sum_{P \in G^+} u_P + x_P v_P.$$

このときE/Gと、f_Gは次のように書き下せる

$$E/_G : Y^2 = X^3 + (a - 5v)X + (b - 7w)$$

Gの元$P = (x_P, y_P)$たちの値から代数的に計算できる

$$f_G(x, y) = \left(x + \sum_{P \in G^+} \frac{v_P}{x - x_P} - \frac{u_P}{(x - x_P)^2}, y - \sum_{P \in G^+} \frac{2u_P y}{(x - x_P)^3} - v_P \frac{y - y_P - g_P^x g_P^y}{(x - x_P)^2} \right)$$

Costello-Hisilの公式：Montgomery-to-Montgomery

定理 [CH17]:

$E_A: y^2 = x^3 + Ax^2 + x$　　$P = (x_P, y_P)$: 位数$\ell = 2d + 1$　　に対し、

$\phi_P: E_A \to E/\langle P \rangle$は$E/\langle P \rangle$の係数を$A'$とし、$Q \in E_A$としたとき次のように計算できる:

$$A' = \left(6 \sum_{i=1}^{d} \frac{1}{\mathrm{x}(iP)} - 6 \sum_{i=1}^{d} \mathrm{x}(iP) + A \right) \cdot \prod_{i=1}^{d} \mathrm{x}(iP)$$

$$\mathrm{x}\left(\phi_P(Q)\right) = \mathrm{x}(Q) \prod_{i=1}^{d} \left(\frac{\mathrm{x}(Q) \cdot \mathrm{x}(iP) - 1}{\mathrm{x}(Q) - \mathrm{x}(iP)} \right)^2 .$$

- 同種写像暗号では単一座標による公式の利用が標準的で色々計算手法が提案されている
- SIKEでは[CH17]を利用し、CSIDHでは[MR18]の手法を用いる

超特異性とℓ-同種写像

- $P \in E[\ell]$をとれば、 巡回群$\langle P \rangle$を核とする同種写像を計算できる
  - Eが$\mathbb{F}_q$上定義されていても一般には$E[\ell] \not\subset E(\mathbb{F}_q)$

    ➡ ねじれ点はしばしば拡大体上に座標を持ち、非効率な計算を招く

例：$p = 17795587, E: Y^2 = X^3 + X$に対し、$E[101]$は$\mathbb{F}_p$の200次拡大に入る

- $\mathbb{F}_p$上の超特異曲線Eを使う
  - このとき$\#E(\mathbb{F}_{p^2}) = (p+1)^2$
  - 標数を$p = \ell_1 \cdot \ell_2 \cdots \ell_n - 1$と設定すると$\#E(\mathbb{F}_{p^2}) = \ell_1^2 \cdots \ell_n^2$

    ➡ $E[\ell_i] \subset E(\mathbb{F}_{p^2})$

ℓ_i−同種写像を考える限りは
二次拡大上で完結！

超特異曲線(Winner) vs 通常曲線(Loser) in Isogeny-based Crypto

MITSUBISHI ELECTRIC
Changes for the Better

- ねじれ点のとりやすさから**同種写像暗号では超特異曲線**を利用する
  - SIDH (Supersingular Isogeny Diffie-Hellman)

    素数　$p = \ell_A^{e_A} \ell_B^{e_B} - 1$ ⇒ $E[\ell_A^{e_A}] \subset E(\mathbb{F}_{p^2})$
  - CSIDH (Commutative Supersingular Isogeny Diffie-Hellman)

    素数　$p = \ell_1 \ell_2 \cdots \ell_n - 1$ ⇒ $E[\ell_i] \subset E(\mathbb{F}_{p^2})$
- 通常曲線を使った方式もあるがどれも非効率 [C06],[RS06], [DKS18]
  - [DKS18]ではモジュラー多項式とVeluの公式を使い分ける手法を提案している
  - Veluの公式を効果的に使うために小さな素因数をたくさん持つ曲線を生成する必要があるが、[DKS18]ではその生成に17,000 CPU 時間かかってる

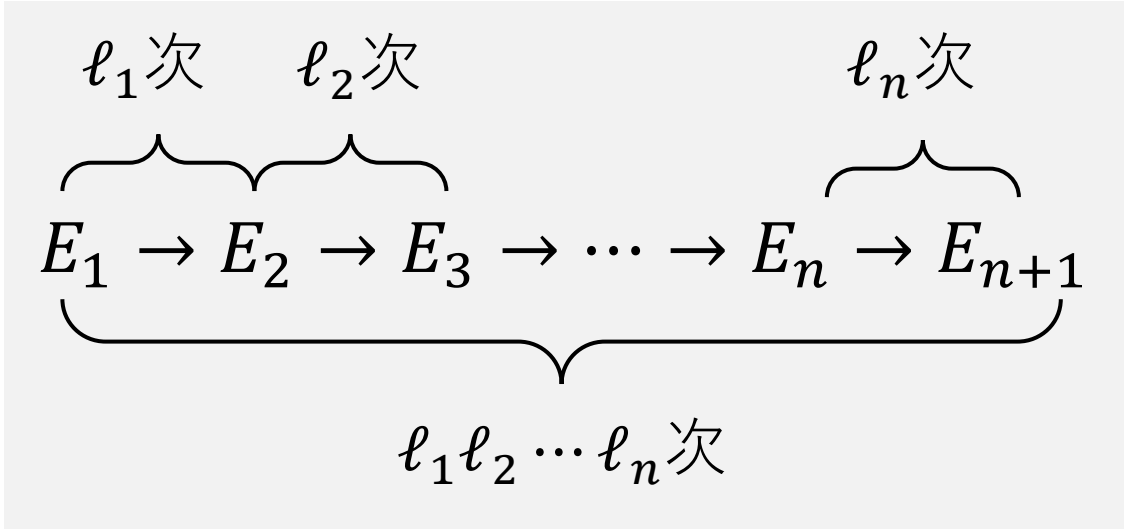
同種写像計算の計算量とフィージビリティ

- 次数nの同種写像の計算量は$O(n)$（指数時間！）

  $\sqrt{élu}$の公式[BDLS20]は$\tilde{O}(\sqrt{n})$は計算でき、高次の場合に効く

  - しばしば次数2^{256}程度の同種写像計算を行う

⇒ 小素数次数同種写像を繰り返し計算することで計算量の爆発を回避



同種写像計算の基本アイデア

■始点をE_1（位数をnとする）とする小素数の積$n = \ell_1 \ell_2 \cdots \ell_n$
（例えば2^{256}）次数の同種写像計算構成のスタンダードな手順

1．位数ℓ_1の点$P_1 \in E_1$を生成

1－1．ランダムな点$P \in E_1$をとって

1－2．スカラー倍で位数を調節$P_1 = \frac{n}{\ell_1} P$

このスカラーは$O(p)$くらい

これを繰り返す

2．点P_1の生成する巡回群を核とする同種写像を
Costello-Hisilの公式などで計算

$$f_1 : E_1 \to E_2$$

■同種写像暗号のアルゴリズムはスカラー倍演算と同種写像計算を多用するため計算量が比較的重くなってしまう

色々なモデルに対する単一座標と公式

モデル	式	座標	スカラー倍演算	同種写像計算
モンゴメリー	$y^2 = x^3 + Ax^2 + x$	x	[M87]	[Ren18] [CH17]
モンゴメリー　－	$y^2 = x^3 + Ax^2 - x$	x	[CD20]	[CD20]
エドワード	$x^2 + y^2 = 1 + dx^2y^2$	$w = dx^2y^2$	[FH17]	[KYPH19]
ハフ	$cx(y^2 - 1) = y(x^2 - 1)$	$w = \frac{1}{xy}$	[HZHL20] [DKW20]	[HZHL20] [DKW20]
ヤコビ交差	$\begin{cases} ax^2 + y^2 = 1 \\ bx^2 + z^2 = 1 \end{cases}$	$\omega = \sqrt{ab}x^2$	[HWZ21]	[HWZ21]

■ これまでの知見：どのモデルを使っても効率性に差はない

⇒ これら演算公式の記述は本質的に同じことやってるのでは？

Generalized Montgomery Coordinate[MOAT22] 1/3

定義：

qを素数べきとし、Eを$\overline{\mathbb{F}_q}$上の楕円曲線とする。CをEの有限部分群とし、$R_0 \in E \setminus C$を$2R_0 \in C$なる点とする。さらに$\mathcal{R}_0 := R_0 + C$とおく。
Cと$\mathcal{R}_0$に付随する**一般化モンゴメリー座標（GMC）**とは以下を満たす関数$h_{C,\mathcal{R}_0} \in \overline{\mathbb{F}_q}(E)$のこと：

$$div\, h_{C,\mathcal{R}_0} = 2\sum_{P \in C}(P + R_0) - 2\sum_{P \in C}(P).$$

- 単一座標を利用したスカラー倍や同種写像計算の公式をGMCで一般化

Theorem 23 (odd degree isogeny). *Let G be a finite subgroup of E satisfying*

$$G \cap (\mathcal{G} \cup \mathcal{R}_0) = \{O_E\}.$$

Let ϕ be a separable isogeny $\phi\colon E \to E/G$ with $\ker\phi = G$. Then, there is a normalized generalized Montgomery coordinate of E/G with respect to $\phi(\mathcal{G})$ and $\phi(\mathcal{R}_0)$ satisfying

$$h_{\phi(\mathcal{G}),\phi(\mathcal{R}_0)}(\phi(P)) = h_{\mathcal{G},\mathcal{R}_0}(P) \prod_{Q \in G\setminus\{O_E\}} \frac{(h_{\mathcal{G},\mathcal{R}_0}(P)h_{\mathcal{G},\mathcal{R}_0}(Q) - 1)}{(h_{\mathcal{G},\mathcal{R}_0}(P) - h_{\mathcal{G},\mathcal{R}_0}(Q))}.$$

GMCに対する同種写像計算公式

Theorem 25 (odd degree isogeny). *Let $\mathcal{R}_1$ be a subset of E defined in Lemma 4, let R_1 be a point in $\mathcal{R}_1$, and let G be a subgroup of E satisfying*

$$G \cap (\mathcal{G} \cup \mathcal{R}_0 \cup \mathcal{R}_1) = \{O_E\}.$$

Let ϕ be a separable isogeny $\phi\colon E \to E/G$ with $\ker\phi = G$, and let $h_{\phi(\mathcal{G}),\phi(\mathcal{R}_0)}$ be a normalized generalized Montgomery coordinate of E/G which is defined in Theorem 23. Then, the generalized Montgomery coefficient of $h_{\phi(\mathcal{G}),\phi(\mathcal{R}_0)}$ is

$$\alpha_{h_{\phi(\mathcal{G}),\phi(\mathcal{R}_0)}} = -h_{\mathcal{G},\mathcal{R}_0}(R_1) \prod_{Q \in G\setminus\{O_E\}} \frac{(h_{\mathcal{G},\mathcal{R}_0}(R_1)h_{\mathcal{G},\mathcal{R}_0}(Q) - 1)}{(h_{\mathcal{G},\mathcal{R}_0}(R_1) - h_{\mathcal{G},\mathcal{R}_0}(Q))} - \frac{1}{h_{\mathcal{G},\mathcal{R}_0}(R_1)} \prod_{Q \in G\setminus\{O_E\}} \frac{(h_{\mathcal{G},\mathcal{R}_0}(R_1) - h_{\mathcal{G},\mathcal{R}_0}(Q))}{(h_{\mathcal{G},\mathcal{R}_0}(R_1)h_{\mathcal{G},\mathcal{R}_0}(Q) - 1)}.$$

GMCに対する像の計算公式

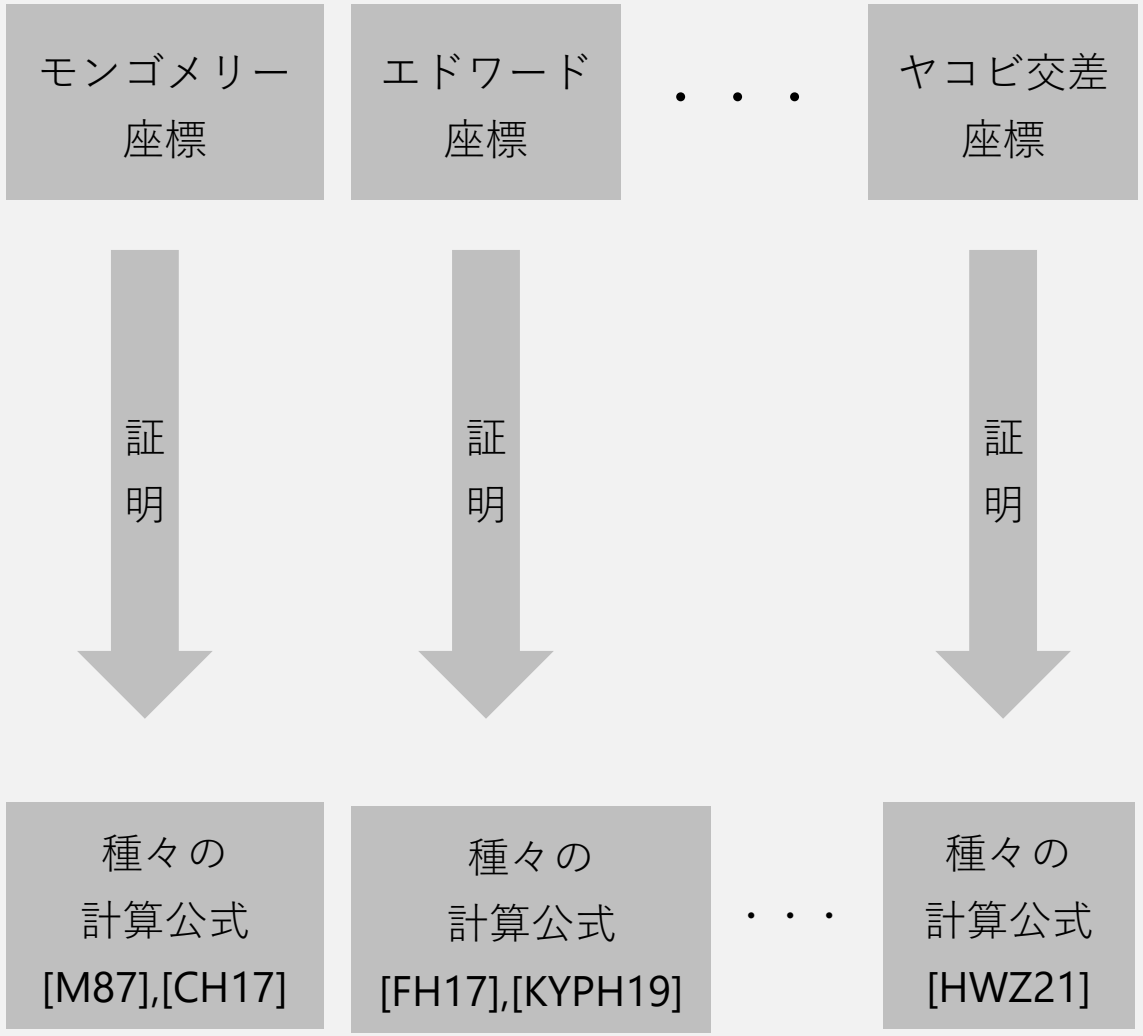
Generalized Montgomery Coordinate[MOAT22] 2/3

■具体的な単一座標の多くはGMCの一例となっている

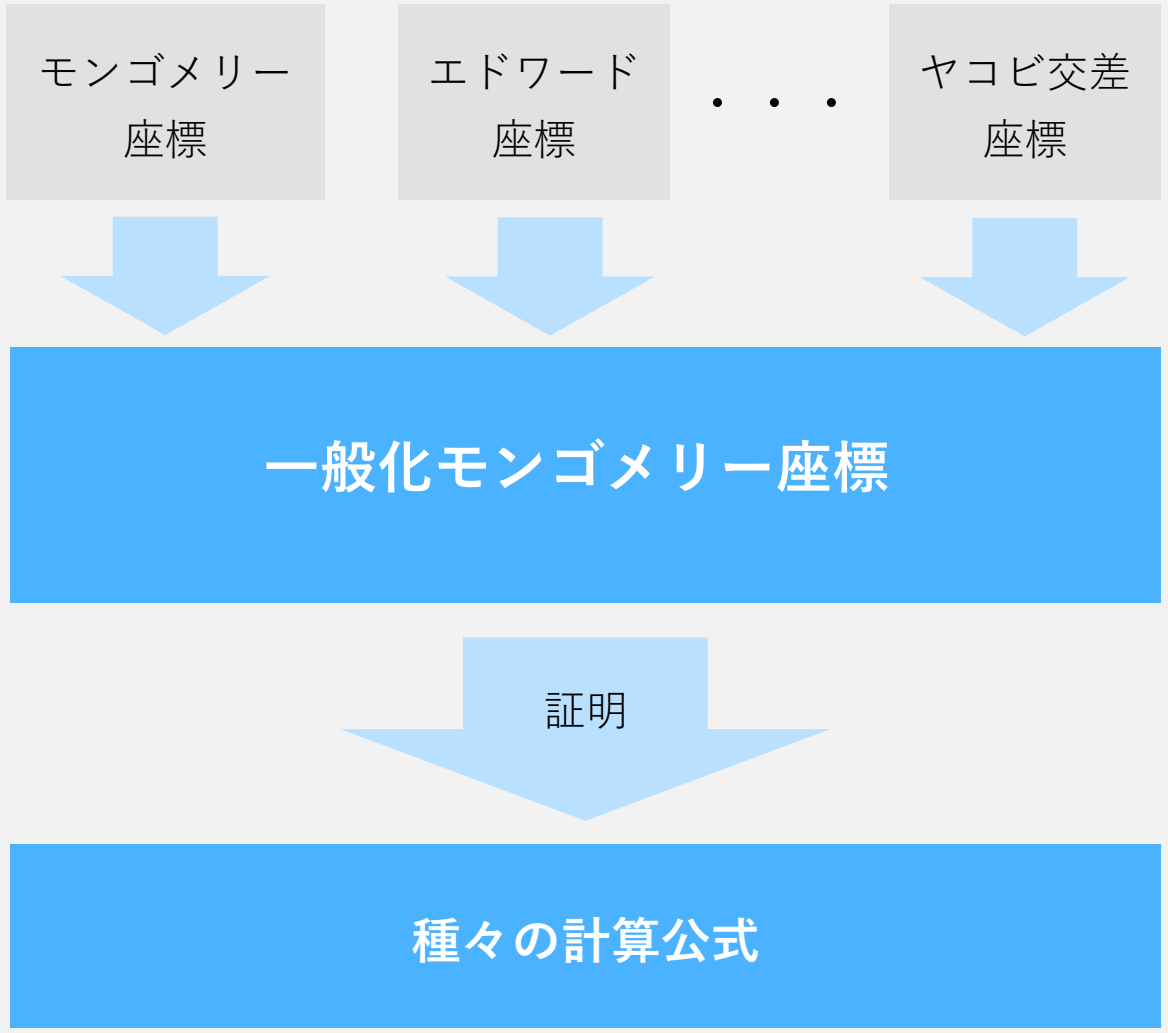
モデル	式	既存座標	GMC $h_{C,\mathcal{R}_0}$	C	$\mathcal{R}_0$
モンゴメリー	$y^2 = x^3 + Ax^2 + x$	x	x	$\{O_E\}$	$\{(0,0)\}$
モンゴメリー　－	$y^2 = x^3 + Ax^2 - x$	x	$\sqrt{-1}x$	$\{O_E\}$	$\{(0,0)\}$
エドワード	$x^2 + y^2 = 1 + dx^2y^2$	$w = dx^2y^2$	w^{-1}	C_4	$\infty_1 + C_4$
ハフ	$cx(y^2 - 1)$ $= y(x^2 - 1)$	$w = \frac{1}{xy}$	w	$\{O_E\}$	$\{\infty_3\}$
ヤコビ交差	$\begin{cases} ax^2 + y^2 = 1 \\ bx^2 + z^2 = 1 \end{cases}$	$\omega = \sqrt{ab}x^2$	ω^{-1}	$E[2]$	{points at infinity}

Generalized Montgomery Coordinate[MOAT22] 3/3

これまでの研究手法



我々の研究手法[MOAT22]



4 超特異同種写像グラフ

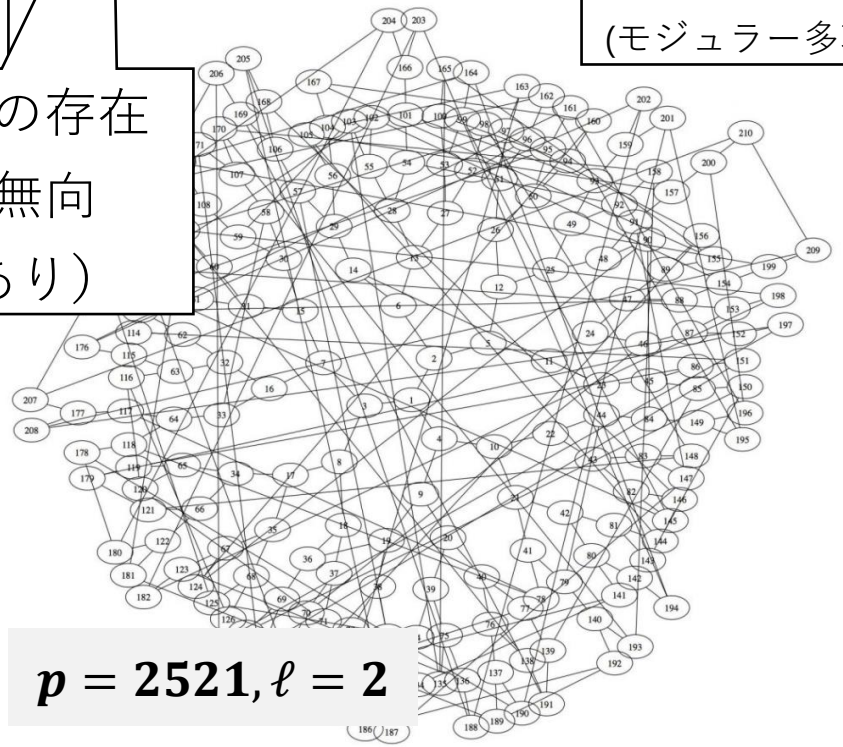
超特異同種写像グラフ

- 標数p上の超特異楕円曲線の**同型類を頂点**とし,**辺をℓ次の同種写像**とするグラフを**ℓ-超特異同種写像グラフ**$\mathcal{G}_1^{SS}(\ell,p)$（SSIG）という
  - **素数pに関する無限グラフ族**
  - 頂点の個数はおおよそ$\frac{p}{12}$個
    つまり、$p \to \infty$で**頂点は発散**
  - $(\ell+1)$-正則グラフ

頂点はj-不変量：
$j \in \mathbb{F}_{p^2}$

双対同種の存在より、無向（例外あり）

(j_1, j_2)が辺⇔
$\Phi_\ell(j_1, j_2) = 0$
(モジュラー多項式)



$p = 2521, \ell = 2$

- CGLハッシュ関数やSIDHはこのグラフ上のランダムウォークで構成される

[出典] Where cryptography and quantum computing intersect - Microsoft Research
https://www.microsoft.com/en-us/research/blog/cryptography-quantum-computing-intersect/

暗号学的ハッシュ関数

- ハッシュ関数Hとは任意のビット長のビット列を固定長ビットへ圧縮する効率的に計算可能な関数

$$H:\{0,1\}^* = \cup_{n=1}^{\infty} \{0,1\}^n \rightarrow \{0,1\}^s$$

  - セキュリティパラメータλに応じた関数の族$\{H_\lambda:\{0,1\}^* \rightarrow \{0,1\}^{s(\lambda)}\}$だと嬉しい

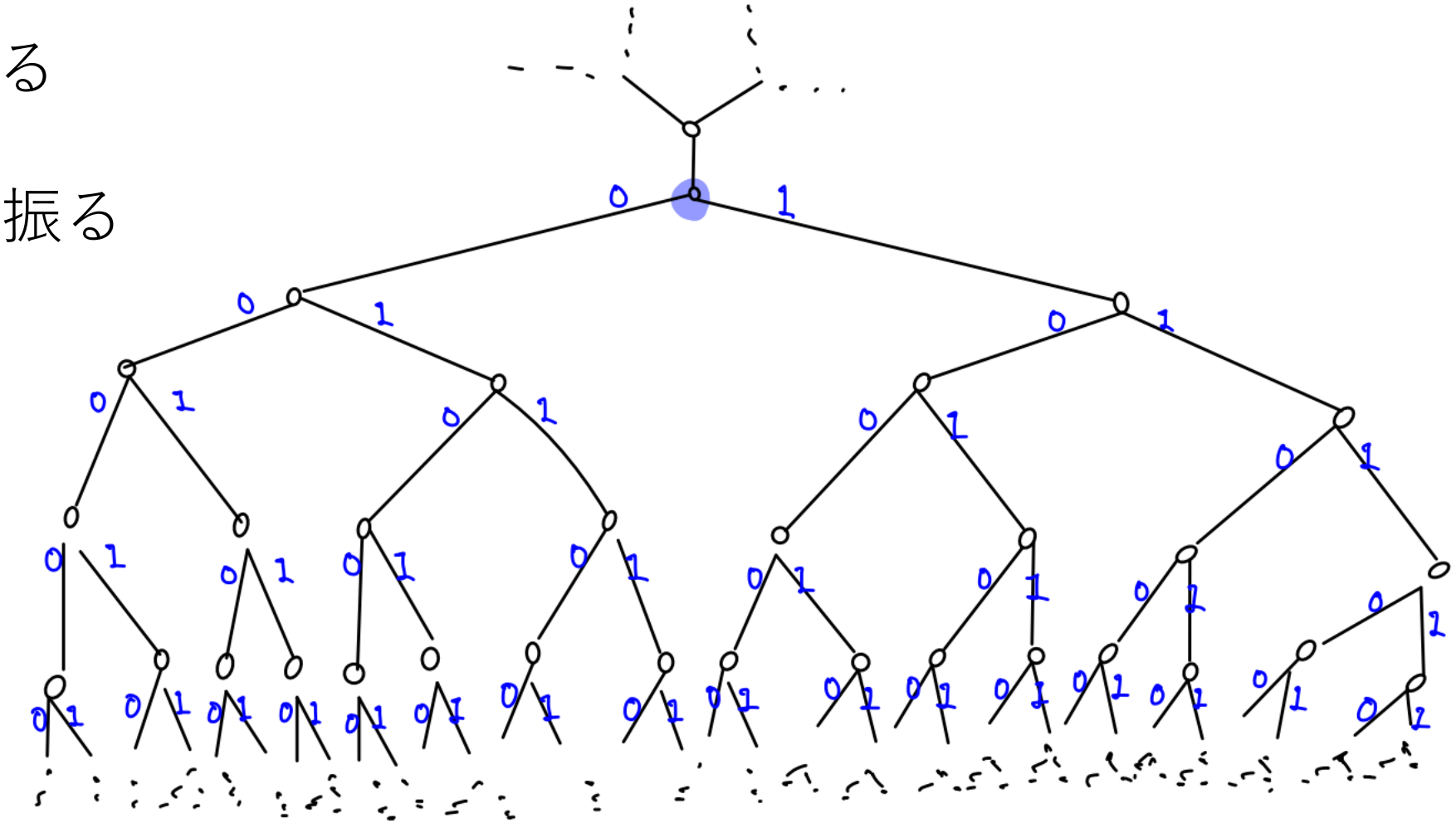
- ハッシュ関数は暗号の構成において安全性を高める目的でしばしば用いられる　→　いくつかの安全性要件が存在する：

代表的要件（衝突困難性）
$H(x_1) = H(x_2)$なる入力対(x_1, x_2)を発見することが計算量的に困難であること

CGLハッシュ関数のアイデア[CLG09]

- $\ell = 2$の同種写像グラフを考え
  頂点を一つ固定する

- 各辺に0と1を割り振る

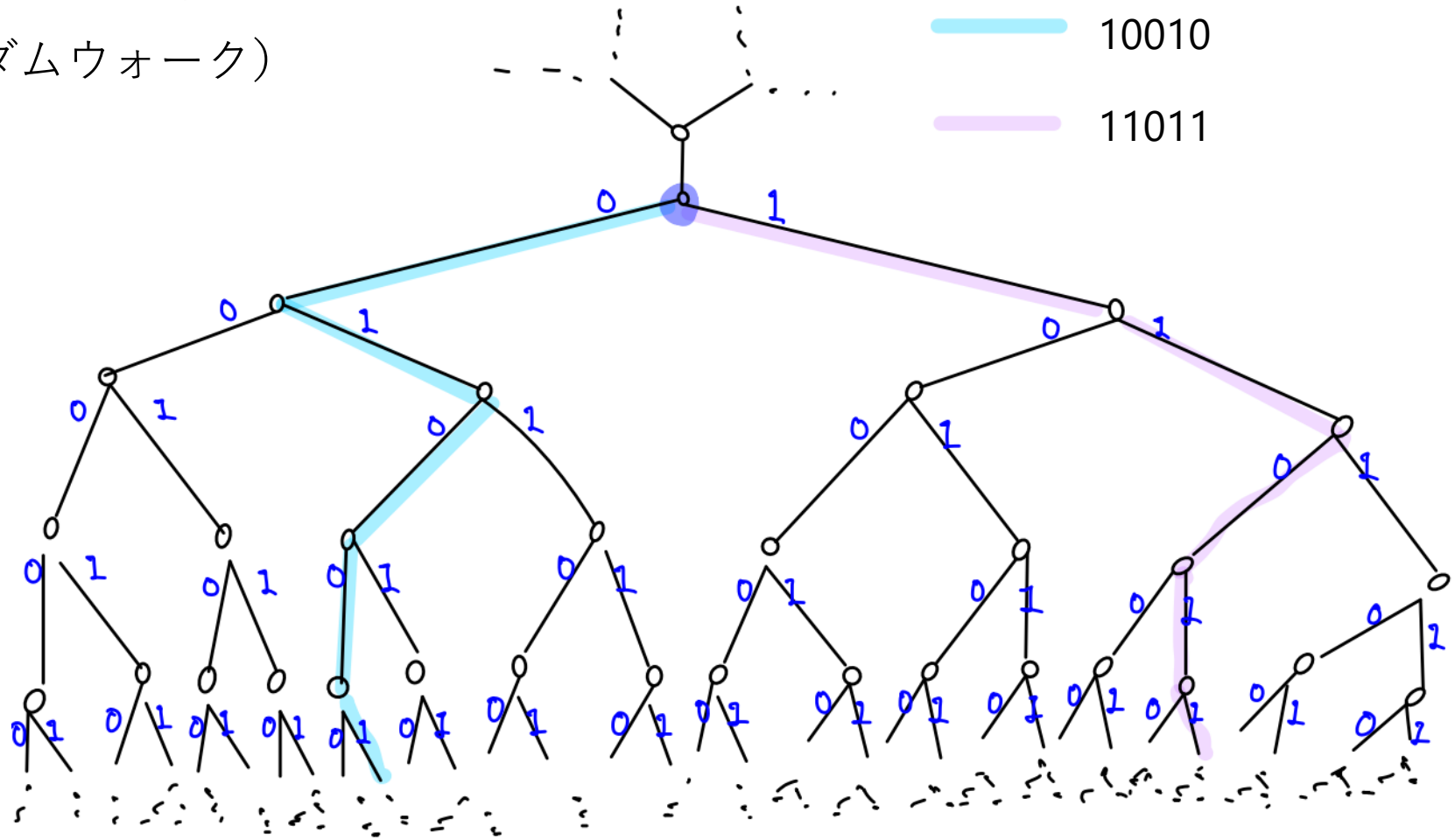


CGLハッシュ関数のアイデア[CLG09]

- 固定された頂点から入力されたビット列に対応するパスを進む
  （バックトラックのないランダムウォーク）

- 終点の超特異曲線のj-不変量$\in \mathbb{F}_{p^2}$を出力

Q 出力の分布は？



エクスパンダー族

定義（エクスパンダー族）
$\{G_n\}_{n\geq 1}$を$n \in \mathbb{N}$で添え字付けられた有限および連結なd-正則無向グラフ$G_n = (V_n, E_n)$の族とする。
族$\{G_n\}_{n\geq 1}$がエクスパンダー族とは以下が成り立つとき：

1．$|V_n| \to +\infty \ (n \to +\infty)$

2．正の定数εが存在し，任意の$n \geq 1$に対して$\mathbf{1 - \mu_1(G_n) \geq \varepsilon.}$

spectral gapとよぶ

隣接行列$\frac{1}{d}A(G_n)$の固有値を
$1 = \mu_0 \geq \mu_1 \geq \cdots \geq \mu_{\#V_n - 1}$
とおいた（正規化してる）

- エクスパンダー族のグラフはランダムウォークが$O(\log \#V)$ステップで一様分布に収束し、$1 - \mu_1$が大きいほど効率が良い
- バックトラック無しの場合のmixing timeは[ABLS07]

SSIGs are Ramanujan

定理（Alon-Boppana）
$\{G_n\}_{n\geq 1}$を有限、連結なd-正則無向グラフ$G_n = (V_n, E_n)$の族で、$\#V_n \to \infty (as\ n \to \infty)$とする。このとき、

$$\liminf_{n\to\infty} \mu_1(G_n) \geq \frac{2\sqrt{d-1}}{d}$$

- 有限、連結なd-正則無向グラフGがラマヌジャングラフとは± 1でない

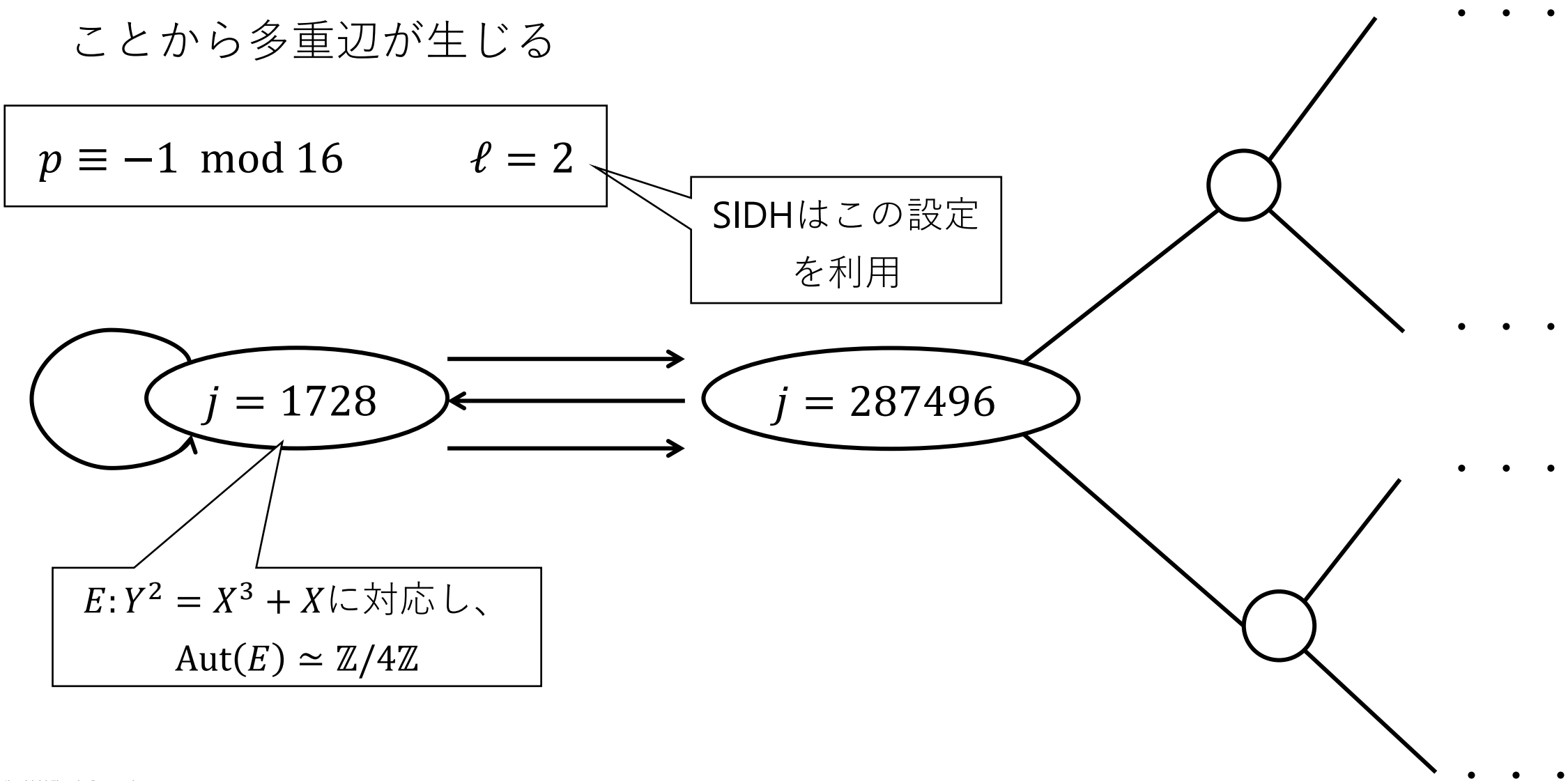
  任意の固有値μが$|\mu| \leq \frac{2\sqrt{d-1}}{d}$を満たすとき

定理[P98]
$p \equiv 1 \bmod 12$のとき$\mathcal{G}_1^{SS}(\ell, p)$はラマヌジャングラフである

そうでないとき有向辺が生じるが、
同種写像暗号ではそのような場合も扱う

Remark: 有向辺の存在

- $j = 0, 1728$の曲線は非自明な自己準同型群（$\neq \mathbb{Z}/2\mathbb{Z}$）を持つことから多重辺が生じる



5 高次元への研究の展開：アーベル多様体の同種写像グラフ

（主編極付）アーベル多様体

■ 楕円曲線は群構造を持つ1次元の代数的な図形のこと

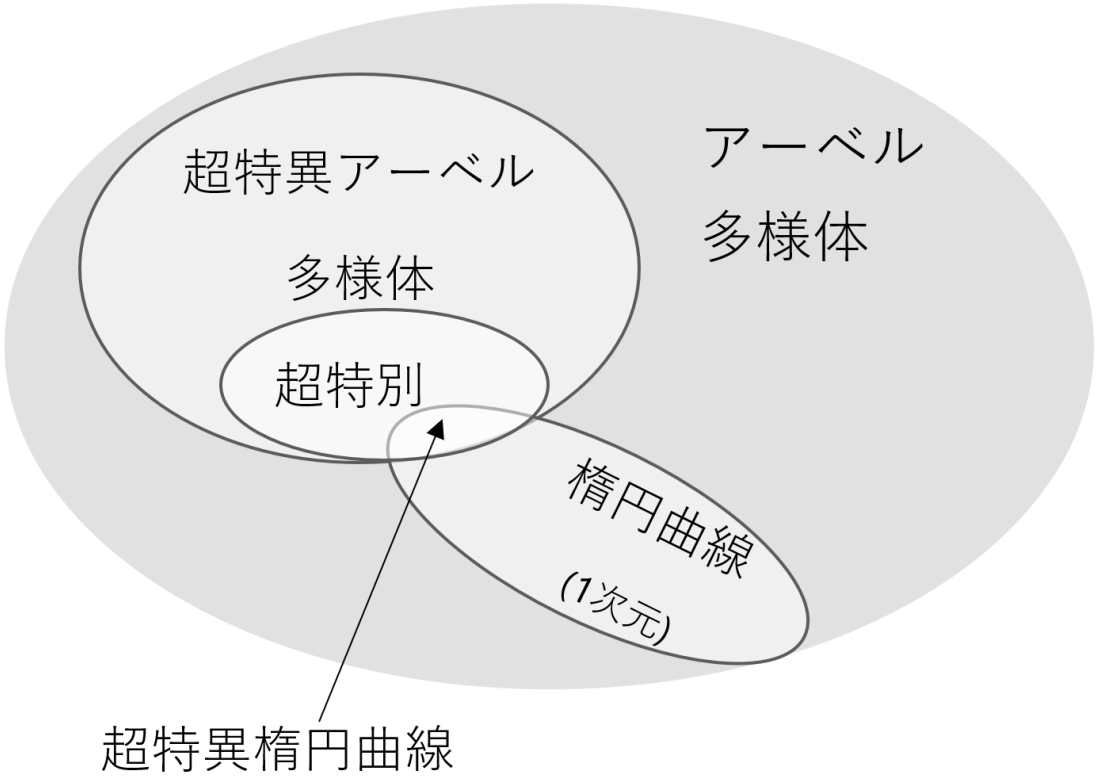
群構造を持つ代数的な図形という性質を保ったまま次元を一般のものにしたものが**アーベル多様体**（インフォーマル）（cf.[M70],[M86]）

例
- 楕円曲線の直積
- 超楕円曲線のヤコビアン

■ 有限体上のアーベル多様体には

- 超特異アーベル多様体
- 超特別アーベル多様体

という種類が存在する



CGLハッシュ関数のアーベル多様体への拡張

- 超特異アーベル多様体を用いたCGLハッシュの類似の構成[T18]
  - 超特異アーベル多様体の同種写像グラフのサイクルを利用した攻撃[FT19]
- 超特別アーベル多様体を用いたCGLハッシュの類似の構成[CDS20]
  - 2次元以上となるとグラフの構造が大きく変わりテクニカルな構成
  - 2次元以上の同種写像問題の1次元の場合への帰着[CS20]

数学的関心として超特別アーベル多様体の同種写像グラフの構造が問題に

超特別同種写像グラフ

- SSIG $\mathcal{G}_1^{SS}(\ell, p)$の一般化として$\mathcal{G}_g^{SS}(\ell, p)$を定める

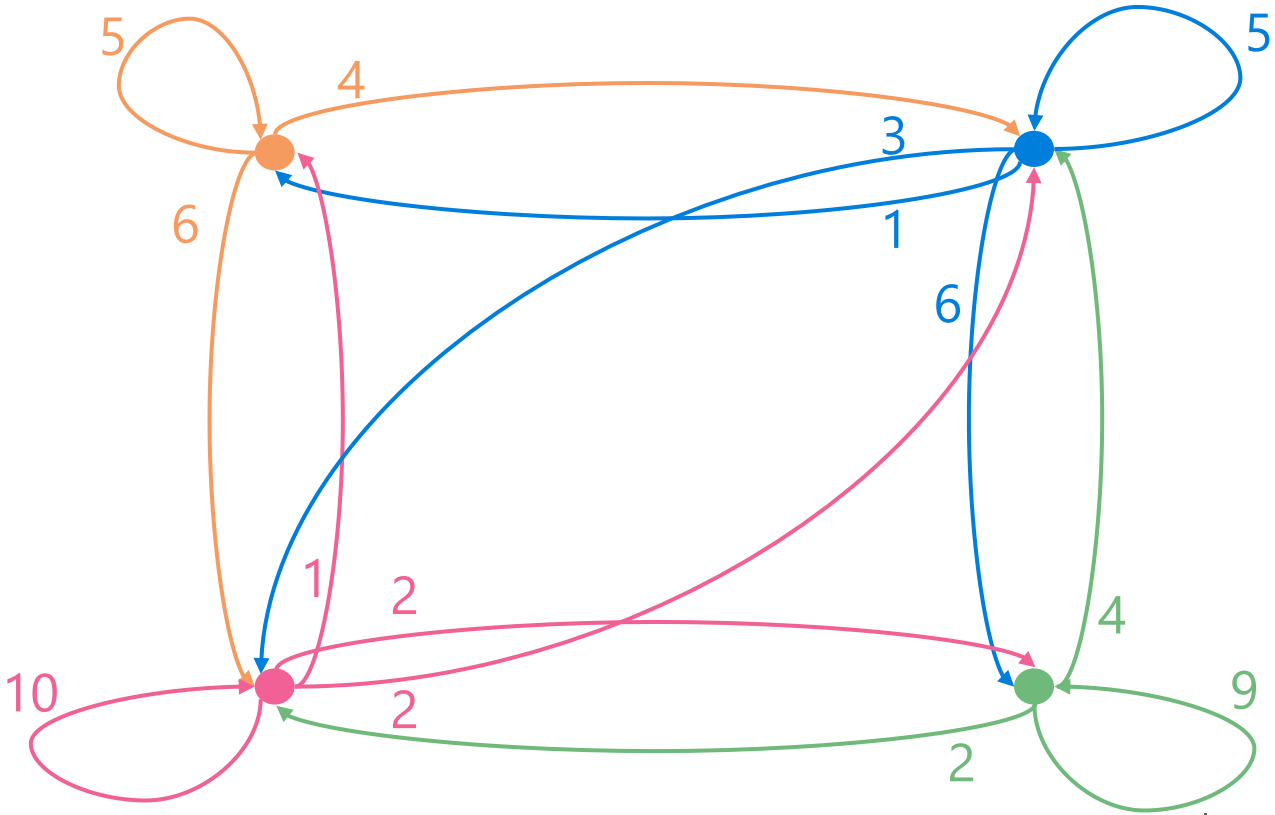
  頂点がg次元超特別アーベル多様体
  辺は$(\ell)^g$ – 同種写像

  - 一般にd –正則**有向多重**グラフ

    ただし$d = \prod_{k=1}^{g}(\ell^k + 1)$

  - 頂点の個数は$O(p^{\frac{g(g+1)}{2}})$くらい

$p = 13, g = 2, \ell = 2 \rightarrow d = 15$



- 頂点はその自己同型群によっていくつかのタイプに分類でき、それぞれの近傍の詳細な研究が[KT20], [FS21a]でなされている

超特別同種写像グラフの固有値に関する研究

探索範囲は
$(g, \ell, p) = (2, < 5, <$ およそ$300)$,
$(3, < 3, <$ およそ$40)$

- [JZ20]は$\mathcal{G}_g^{SS}(\ell, p)$が連結であることを証明
  さらに数値計算によりいくつかの例のラマヌジャン性を示した：

$$(g, \ell, p) = (2,2,5), (2,2,7), (2,3,7), (3,2,3)$$

  - 逆に言えば、ほとんどがラマヌジャンでない

- [FS21b]では$\mathcal{G}_2^{SS}(2, p)$のランダムウォークの統計的性質や固有値の数値的研究が行われた
  - 固有値が一様なバウンドを持つことを予想（観察）

An explicit lower bound for the spectral gap of $\mathcal{G}_g^{SS}(\ell, p)$

■ $g \geq 2$とℓに関する条件なしに、spectral gapの下界を明示的に与えた

定理 ([ATY22])

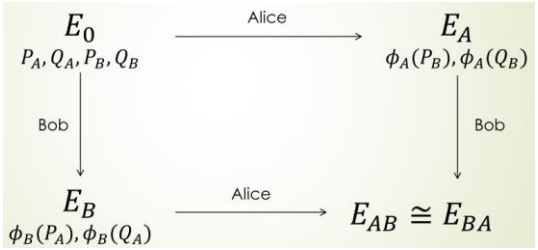
pを素数とし、整数$g \geq 2$と素数$\ell \neq p$を固定する。標数p上のg次元超特別アーベル多様体を頂点集合とする$(\ell)^g$ – 同種写像グラフの族$\{\mathcal{G}_g^{SS}(\ell, p)\}_p$の固有値は以下を満たす：

$$1 - \mu_1\left(\mathcal{G}_g^{SS}(\ell, p)\right) \geq \frac{1}{4(g+2)}\left(\frac{\ell - 1}{2(\ell - 1) + 3\sqrt{2\ell(\ell+1)}}\right)^2.$$

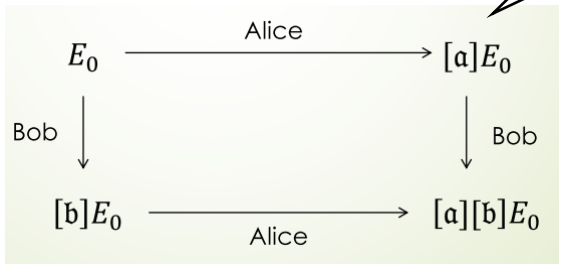
まとめ

- 同種写像暗号を支える数学的基礎について、またそれを実装可能にするアイデアについて紹介した
  - 楕円曲線や同種写像とは何か
  - なぜ超特異曲線を利用するか
  - 同種写像はどのように計算されるか
  - CGLハッシュやSIDHの舞台となる超特異同種写像グラフはしかるべき性質（エクスパンダー族）を持っているか
  - また高次元への拡張の研究はどのように進んでいるか

SIDH, CSIDHへ



守谷さんのスライドより



References

- [ATY22] Y.Aikawa, R.Tanaka, T.Yamauchi, Isogeny graphs on superspecial abelian varieties: Eigenvalues and Connection to Bruhat-Tits buildings, arXiv: 2201.04293.
- [ABLS07] N.Alon, I.Benjamini, E.Lubetzky, S.Sodin, Non-backtracking random walks mix faster, Communications in Contemporary Mathematics, 9:585–603, 2007.
- [BDLS20] Bernstein, D.J., De Feo, L., Leroux, A., Smith, B.: Faster computation of isogenies of large prime degree. ANTS XIV (2020)
- [BKV19] Beullens, W., Kleinjung, T., Vercauteren, F. (2019). CSI-FiSh: Efficient Isogeny Based Signatures Through Class Group Computations. In: Galbraith, S., Moriai, S. (eds) Advances in Cryptology – ASIACRYPT 2019. ASIACRYPT 2019. Lecture Notes in Computer Science(), vol 11921.
- [C06] Jean-Marc Couveignes. Hard Homogeneous Spaces, 2006. IACR Cryptology ePrint Archive 2006/291.
- [CD20] Castryck, W., Decru, T. (2020). CSIDH on the Surface. In: Ding, J., Tillich, JP. (eds) Post-Quantum Cryptography. PQCrypto 2020. Lecture Notes in Computer Science(), vol 12100. Springer, Cham.
- [CDS20]W. Castryck, T. Decru, and B. Smith, Hash functions from superspecial genus-2 curves using Richelot isogenies. J. Math. Cryptol. 14 (2020), no. 1, 268292.
- [CH17] Costello, C., Hisil, H. (2017). A Simple and Compact Algorithm for SIDH with Arbitrary Degree Isogenies. In: Takagi, T., Peyrin, T. (eds) Advances in Cryptology – ASIACRYPT 2017. ASIACRYPT 2017. Lecture Notes in Computer Science(), vol 10625. Springer, Cham.
- [CLG09] D-X. Charles, K. lauter, E-Z. Goren, Cryptographic hash functions from expander graphs. J. Cryptology, 2009.

References

- [CLM+18] Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J. (2018). CSIDH: An Efficient Post-Quantum Commutative Group Action. In: Peyrin, T., Galbraith, S. (eds) Advances in Cryptology – ASIACRYPT 2018. ASIACRYPT 2018. Lecture Notes in Computer Science(), vol 11274. Springer, Cham.
- [CS20] Costello, C., Smith, B. (2020). The Supersingular Isogeny Problem in Genus 2 and Beyond. In: Ding, J., Tillich, JP. (eds) Post-Quantum Cryptography. PQCrypto 2020. Lecture Notes in Computer Science(), vol 12100. Springer, Cham.
- [DKL+20]De Feo, L., Kohel, D., Leroux, A., Petit, C., Wesolowski, B. (2020). SQISign: Compact Post-quantum Signatures from Quaternions and Isogenies. In: Moriai, S., Wang, H. (eds) Advances in Cryptology – ASIACRYPT 2020. ASIACRYPT 2020. Lecture Notes in Computer Science(), vol 12491. Springer, Cham.
- [DKS18] De Feo, L., Kieffer, J., Smith, B. (2018). Towards Practical Key Exchange from Ordinary Isogeny Graphs. In: Peyrin, T., Galbraith, S. (eds) Advances in Cryptology – ASIACRYPT 2018. ASIACRYPT 2018. Lecture Notes in Computer Science(), vol 11274. Springer, Cham.
- [DKW20]R. Dorylo et al., Efficient Montgomery-like formulas for general Huff's and Huff's elliptic curves and their applications to the isogeny-based cryptography, IACR ePrint Archive: 2020/526.
- [FH17] Farashahi, R.R., Hosseini, S.G. (2017). Differential Addition on Twisted Edwards Curves. In: Pieprzyk, J., Suriadi, S. (eds) Information Security and Privacy. ACISP 2017. Lecture Notes in Computer Science(), vol 10343. Springer, Cham.
- [FS21a]E. Florit and B.Smith, An atlas of the supespecial Richelot isogeny graph, To appear in the RIMS Kôkyûro Bessatsu volume on supersingular curves and abelian varieties.

References

- [FS21b]E. Florit and B. Smith, Automorphisms and isogeny graphs of abelian varieties, with applications to the superspecial Richelot isogeny graph, In Arithmetic, Geometry, Cryptography, and Coding Theory 2021, 779:103-32. Contemp. Math. Amer. Math. Soc., 2022.
- [FT19] Flynn, E.V., Ti, Y.B. (2019). Genus Two Isogeny Cryptography. In: Ding, J., Steinwandt, R. (eds) Post-Quantum Cryptography. PQCrypto 2019. Lecture Notes in Computer Science(), vol 11505. Springer, Cham.
- [HWZ21] Hu, Z., Wang, L., Zhou, Z. (2021). Isogeny Computation on Twisted Jacobi Intersections. In: , *et al*. Information Security Practice and Experience. ISPEC 2021. Lecture Notes in Computer Science(), vol 13107. Springer, Cham.
- [HZHL20] Huang, Y., Zhang, F., Hu, Z., Liu, Z. (2020). Optimized Arithmetic Operations for Isogeny-Based Cryptography on Huff Curves. In: Liu, J., Cui, H. (eds) Information Security and Privacy. ACISP 2020. Lecture Notes in Computer Science(), vol 12248. Springer, Cham.
- [JD11] Jao, D., De Feo, L. (2011). Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies. In: Yang, BY. (eds) Post-Quantum Cryptography. PQCrypto 2011. Lecture Notes in Computer Science, vol 7071. Springer, Berlin, Heidelberg.
- [JZ20]B-W. Jordan and Y. Zaytman, Isogeny graphs of superspecial abelian varieties and Brandt matrices, arXiv:2005.09031.
- [KT20] Toshiyuki Katsura and Katsuyuki Takashima. Counting richelot isogenies between superspecial abelian surfaces. In Steven D. Galbraith, editor, Proceedings of the Fourteenth Algorithmic Number Theory Symposium, volume 4 of The Open Book Series, pages 283–300. Mathematical Sciences Publishers, 2020.

References

- [KYPH19] Kim, S., Yoon, K., Park, YH., Hong, S. (2019). Optimized Method for Computing Odd-Degree Isogenies on Edwards Curves. In: Galbraith, S., Moriai, S. (eds) Advances in Cryptology – ASIACRYPT 2019. ASIACRYPT 2019. Lecture Notes in Computer Science(), vol 11922. Springer, Cham.
- [M87] Peter L Montgomery. Speeding the Pollard and elliptic curve methods of factorization. Mathematics of computation, 48(177):243–264, 1987.
- [MOAT22] T.Moriya, H.Onuki, Y.Aikawa, T.Takagi, The Generalized Montgomery Coordinate: A New Computational Tool for Isogeny-based Cryptography, to appear in: MathCrypt2022.
- [MR18] Meyer, M., Reith, S. (2018). A Faster Way to the CSIDH. In: Chakraborty, D., Iwata, T. (eds) Progress in Cryptology – INDOCRYPT 2018. INDOCRYPT 2018. Lecture Notes in Computer Science(), vol 11356. Springer, Cham.
- [P98]A-K. Pizer, Ramanujan graphs. Computational perspectives on number theory (Chicago, IL, 1995), 159-178, AMS/IP Stud. Adv. Math., 7, Amer. Math. Soc., Providence, RI, 1998.
- [R17] Renes, J. (2018). Computing Isogenies Between Montgomery Curves Using the Action of (0, 0). In: Lange, T., Steinwandt, R. (eds) Post-Quantum Cryptography. PQCrypto 2018. Lecture Notes in Computer Science(), vol 10786. Springer, Cham.
- [RS06] Alexander Rostovtsev and Anton Stolbunov. Public-key cryptosystem based on isogenies, 2006. IACR Cryptology ePrint Archive 2006/145.

References

- [T18]K. Takashima, Efficient algorithms for isogeny sequences and their cryptographic applications. Mathematical modelling for next-generation cryptography, 97114, Math. Ind. (Tokyo), 29, Springer, Singapore, 2018.
- [V71] Jacques Vélu, Isogénies entre courbes elliptiques, Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences, Série A 273 (1971), 238–241.