B-SIDH に対する Castryck-Decru 攻撃の構成と実装

九州大学 マス・フォア・イノベーション連係学府
吉住崚 (Ryo YOSHIZUMI) *

概要

楕円曲線の同種写像を用いた鍵共有プロトコルとして SIDH とその variant である B-SIDH がある．2022 年に SIDH への多項式時間攻撃が与えられ, それは理論上 B-SIDH にも適用できる．しかし, 攻撃に用いるアーベル曲面間の素数次数が SIDH と比べ大きく, 単一の写像の実装はなされていたが, それらの合成の効率的な実装は与えられていなかった．本研究では, B-SIDH への攻撃のアルゴリズムを構成し, そのアルゴリズムに基づく B-SIDH に対する攻撃を計算機代数システム Magma 上で実装した．本研究は小貫啓史氏 (東京大学), 大橋亮氏 (東京大学), 工藤桃成氏 (福岡工業大学), 縫田光司氏 (九州大学/産業技術総合研究所) との共同研究に基づく．

1 導入: 同種写像暗号

この節では同種写像暗号に関して述べる．同種写像暗号とは楕円曲線とその間の同種写像を用いて構成される暗号のことである．具体例として, 鍵共有を目的としたプロトコルである SIDH[FJP14] とその variant である B-SIDH[Cos20] がある． しかし, 2022 年に Castryck, Decru [CD23] と Maino, Martindale [MMP+23] らがこれらに対する多項式時間攻撃を与えた．この節ではその中でも B-SIDH の説明とそれに対する攻撃について解説する．

1.1 鍵共有プロトコル B-SIDH

この小節では鍵共有プロトコル B-SIDH について説明する．

最初に B-SIDH の構成に必要な楕円曲線に関する事実を述べる．参考文献として [Sil86] を挙げる．$E/\mathbb{F}_{p^n}$ を有限体 $\mathbb{F}_{p^n}$ 上の楕円曲線とする．p^n 乗フロベニウス写像 $\mathrm{Frob}_{p^n} : E \to E$ のトレース $t_n \in \mathbb{Z}$ が p の倍数のとき, E を超特異楕円曲線という．超特異楕円曲線の同値な定義として, 任意の整数 $r \geq 1$ に対し $E[p^r] = 0$ が成り立つことが挙げられる．よって, 超特異性は代数閉体上の性質である．ここで, 楕円曲線の $\mathbb{F}_{p^n}$-有理点のなす群の位数 $\#E(\mathbb{F}_{p^n})$ は $\#E(\mathbb{F}_{p^n}) = p^n + 1 - t_n$ を満たす．今 $|t_n| \leq 2\sqrt{p^n}$ が成り立つことから, $n = 1$ のとき, E が超特異であることは $\#E(\mathbb{F}_p) = p + 1$ に同値になる．また $n = 2$ のときは超特異であることは t_2 が $\pm 2p, \pm p, 0$ のいずれかであることに同値となる．いま超特異楕円曲線 $E/\mathbb{F}_p$ に対し, $\#E(\mathbb{F}_p) \mid \#E(\mathbb{F}_{p^2})$ であるから, $t_2 = 2p$ で

* E-mail:yoshizumi.ryo.483@s.kyushu-u.ac.jp

$\#E(\mathbb{F}_{p^2}) = (p+1)^2$ となる．$E/\mathbb{F}_{p^2}$ の (自明でない)2 次ツイストを $E^t/\mathbb{F}_{p^2}$ と表す．E^t は E と $\mathbb{F}_{p^2}$ 上同型ではないが $\mathbb{F}_{p^4}$ 上同型である．また $\#E^t(\mathbb{F}_{p^2}) = (p-1)^2$ である．

はじめに, 鍵共有について説明する．十分大きな素数 $p(\approx 2^{256})$ を固定する．今, Alice と Bob の 2 人が秘密の鍵を共有したいと考えている．より具体的にはある元 $j \in \mathbb{F}_{p^2}$ を 2 人だけが知っている状況にしたい．しかし, 2 人は事前に何の情報も共有していなく, また 2 人の会話は全ての人に公開されているとする．2 人以外のある人 (攻撃者と呼ぶ) が公開されている情報から j を求めること (攻撃という) に十分時間が必要ならば, この鍵共有は安全であると言う．より正確には多項式時間で計算可能な攻撃が見つかっていなければその時点で安全であるとみなされる．B-SIDH はそのような具体的な方法の一つとして提案された．しかし, 後述するように多項式時間で計算可能な攻撃が現在見つかっている．

B-SIDH のプロトコルを説明する．$N_A > N_B$ を互いに素で $N_A|(p+1), N_B|(p-1)$ または $N_A|(p-1), N_B|(p+1)$ を満たす smooth な整数とする．ここで, 整数が smooth であるとは任意の素因数が十分小さいという意味である．話を簡単にするため, 以下では

$$N_A|(p+1),\ N_B|(p-1)$$

と仮定して議論を進める．$E_0/\mathbb{F}_p$ を超特異楕円曲線とする．いま $\#E_0(\mathbb{F}_{p^2}) = (p+1)^2$ と $E_0[N_A] \cong (\mathbb{Z}/N_A\mathbb{Z})^2$ から, $E_0[N_A] \subseteq E_0(\mathbb{F}_{p^2})$ が従う．$E_0[N_A]$ の基底 $\{P_A, Q_A\}$ を一組とる．また $E_0^t/\mathbb{F}_{p^2}$ を E_0 の $\mathbb{F}_{p^2}$ 上の非自明な 2 次ツイストとすれば, $\#E_0^t(\mathbb{F}_{p^2}) = (p-1)^2$ より $E_0^t[N_B] \subseteq E_0^t(\mathbb{F}_{p^2})$ となる．同様に $E_0^t[N_B]$ の基底 $\{P_B, Q_B\}$ を一組とる．また, $\mathbb{F}_{p^4}$ 上同型写像 $\sigma : E_0 \to E_0^t$ を一つとる．今, 上記で選んだ情報

$$p, N_A, N_B, E_0, P_A, Q_A, E_0^t, P_B, Q_B, \sigma$$

を公開する．したがって, これらの情報は Alice, Bob, 攻撃者含めた全員が知っている．以上の準備のもと, B-SIDH のアルゴリズムは以下の通りである．

(A1) Alice は $R_A = P_A + n_A Q_A \in E_0[N_A]$ を秘密に選び, $\langle R_A \rangle$ を核とする同種写像 $\phi_A : E_0 \to E_A$ を構成する．

(A2) Alice は $\phi_A(\sigma^{-1}(P_B)), \phi_A(\sigma^{-1}(Q_B)) \in E_A$ を計算し, $E_A, \phi_A(\sigma^{-1}(P_B)), \phi_A(\sigma^{-1}(Q_B))$ を公開する．

(B1) Bob は $R_B = P_B + n_B Q_B \in E_0^t[N_B]$ を秘密に選び, $\langle R_B \rangle$ を核とする同種写像 $\phi_B : E_0^t \to E_B$ を構成する．

(B2) Bob は $\phi_B(\sigma(P_A)), \phi_B(\sigma(Q_A)) \in E_B$ を計算し, $E_B, \phi_B(\sigma(P_A)), \phi_B(\sigma(Q_A))$ を公開する．

(A3) Alice は E_B を $\langle \phi_B(\sigma(P_A)) + n_A \phi_B(\sigma(Q_A)) \rangle$ を核とする同種写像 $E_B \to E_{BA}$ を構成し, E_{BA} を共有鍵とする．

(B3) Bob は E_A を $\langle \phi_A(\sigma^{-1}(P_B)) + n_B \phi_A(\sigma^{-1}(Q_B)) \rangle$ を核とする同種写像 $E_A \to E_{AB}$ を構成し, E_{AB} を共有鍵とする．

このとき, E_{AB} と E_{BA} は $\mathbb{F}_{p^4}$ 上同型で, 特に同じ j 不変量を持つ．以上から, Alice と Bob は同じ情報を共有することができた．

$$\begin{array}{ccc} E_0 \overset{\sigma}{\cong} E_0^t & \xrightarrow{\phi_B} & E_B \\ {\scriptstyle \phi_A}\downarrow & & \downarrow \\ E_A & \longrightarrow & E_{AB} \cong E_{BA} \end{array}$$

ここで σ や $E_A \to E_{AB}, E_B \to E_{BA}$ は $\mathbb{F}_{p^4}$ 上で定義される同種写像だが, Kummer line 上では $\mathbb{F}_{p^2}$ 上定義出来る [Cos20, §3]. これにより扱う点や同種写像の計算は $\mathbb{F}_{p^2}$ 上で行うことが出来る.

1.2 Castryck-Decru 攻撃

前小節では SIDH の variant である B-SIDH に関して説明した. しかし, 2022 年に Castryck, Decru [CD23] と Maino, Martindale [MMP+23] らが SIDH に対する多項式時間攻撃を与え, この攻撃方法は B-SIDH に対しても適用可能である. この小節ではその攻撃方法について説明する.

次の定理がその攻撃の基礎となる. 定理内の用語の定義は 2.1節を参照.

定理 1.1. ([Kan97]) g 次元の主偏極付きアーベル多様体 A, B, C, D が下の可換図式を満たすものとする:

$$\begin{array}{ccc} A & \xrightarrow{f_2} & C \\ {\scriptstyle f_1}\downarrow & & \downarrow{\scriptstyle g_1} \\ B & \xrightarrow[g_2]{} & D \end{array}.$$

ここで互いに素な自然数 d_1, d_2 により, f_1, g_1 は $(d_1)^g$-同種写像, f_2, g_2 は $(d_2)^g$-同種写像であるとする. このとき, 行列 $\begin{pmatrix} \hat{f}_1 & \hat{f}_2 \\ -g_2 & g_1 \end{pmatrix}$ で定まる $(d_1+d_2)^{2g}$-同種写像 $F : B \times C \to A \times D$ の核は次式で与えられる：

$$\operatorname{Ker} F = \{(f_1(P), f_2(P)) \in B \times C \mid P \in A[d_1+d_2]\}.$$

この定理を用いた攻撃 (Castryck-Decru 攻撃) を紹介する. 記号は前節と同じものとする. 簡単のため $N_A > N_B$ とし, $a := N_A - N_B > 0$ とおく. 標数 $p \equiv 3 \pmod 4$ とし, $E_0/\mathbb{F}_p$ を $y^2 = x^3 + x$ で定義される超特異楕円曲線とする. このとき, 詳細は省略するが a 次同種写像 $\alpha : E_0 \to E'$ で, $\alpha(P_A)$ と $\alpha(Q_A)$ が計算できるものが取れる. このとき, ϕ_B と α の push-forward からなる可換図式

$$\begin{array}{ccc} E_0 & \xrightarrow{\phi_B} & E_B \\ {\scriptstyle \alpha}\downarrow & & \downarrow{\scriptstyle \alpha'} \\ E' & \xrightarrow[\phi'_B]{} & E'_B \end{array}$$

に対し上記の定理を適用する. すなわち, (N_A, N_A)-同種写像 $F : E' \times E_B \to E_0 \times E'_B$ を行列 $\begin{pmatrix} \hat{\alpha} & \hat{\phi_B} \\ -\phi'_B & \alpha' \end{pmatrix}$ で定まるものとすれば,

$$\operatorname{Ker} F = \{(\alpha(P), \phi_B(P)) \in E' \times E_B \mid P \in E_0[N_A]\}$$

となる. よって, 具体的に分かっている 2 点

$$(\alpha(P_A), \phi_B(P_A)), (\alpha(Q_A), \phi_B(Q_A))$$

は $\mathrm{Ker}\, F$ を生成するため, F は計算可能である. いま $\mathrm{Ker}\, \phi_B = \hat{\phi_B}(E_B[N_B])$ に注意する. $E_B[N_B]$ の基底 $\{S_1, S_2\}$ を一組取り, $F((0, S_i)) = (\hat{\phi_B}(S_i), \alpha'(S_i))$ を計算することで, $\mathrm{Ker}\, \phi_B$ の生成系を得ることが出来る. 以上が Castryck-Decru 攻撃である.

2 アーベル多様体の計算

前節で攻撃者はアーベル曲面間の (N_A, N_A)-同種写像 F を計算する必要がある. 一般に同種写像を計算する場合, 素数次数の同種写像の合成に分解して計算する方法が最も効率的である. ここで, その素数次数が 2 の場合はいくつかの特別な方法が知られており, SIDH に対する攻撃ではこの場合で十分である. しかし, B-SIDH に対する攻撃を行う場合はそうとは限らない. しかし, 一般の素数次数の同種写像の計算もこの節で紹介する theta 関数を用いることで計算可能である. 紙面の都合上, 本節ではその計算方法のための導入部分のみ紹介する.

2.1 アーベル多様体の射影空間への埋め込み

計算機で計算を行うためには, アーベル多様体に座標を与えることが必要である. そのためにこの小節では, アーベル多様体を射影空間に埋め込むことについて考える.

以下, k は代数閉体とし, その上の代数多様体を考えるとする. 代数多様体に関する参考文献として [Har77] を挙げる.

アーベル多様体とは完備な代数多様体とその上の群構造の組のことである. このとき, 群演算が可換な非特異射影代数多様体になることが知られている. また次元を g で表すとする. アーベル多様体に関する参考文献として [Mum70] を挙げる.

アーベル多様体 A 上の主偏極とは, 次数が 1 の ample line bundle$\mathscr{L}$ の代数的同値類のことである. またこのとき, 組 $(A, \mathscr{L})$ を主偏極付きアーベル多様体 (以下 PPAV) という. 特にこのとき同種写像 $\varphi_{\mathscr{L}} : A \to \hat{A}$ を $\varphi(x) = T_x^* \mathscr{L} \otimes \mathscr{L}^{-1}$ と定義すれば, $\varphi_{\mathscr{L}}$ は同型となる.

Lefschetz の定理から, $n \geq 3$ のとき $\mathscr{L}^n$ は very ample である. また大域切断のなす k-ベクトル空間 $\Gamma(A, \mathscr{L}^n)$ は n^g 次元であるため, 基底を一組とれば, $n^g - 1$ 次元射影空間への閉埋め込み $\iota : A \to \mathbb{P}^{n^g - 1}$ を得る.

今, $\mathrm{PPAV}(A, \mathscr{L})$ に対し, $\Gamma(A, \mathscr{L}^n)$ の基底でその埋め込み ι が次のような条件を満たすものを構成したい.

(i) $x, y \in A$ に対し, その射影座標 $\iota(x), \iota(y) \in \mathbb{P}^{n^g - 1}$ が与えられたとき, 和 $x + y \in A$ の射影座標 $\iota(x + y) \in \mathbb{P}^{n^g - 1}$ が計算できる.

(ii) 被約な有限部分群 $K \subseteq A$ が与えられたとき, 同種写像 $A \to A/K$ が計算できる.

ただし, 「与えられる」,「計算できる」という言葉の詳細はここでは避ける. 今, theta 関数は上記の要求に対し, 完全ではないが部分的に応える. 以下, 簡単のため $\mathbb{C}$ 上の解析的 theta 関数について述

べるが, それらの結果は正標数の場合も適用可能である．また, 正標数における theta 関数の理論は [Mum66] による代数的 theta 関数を挙げる．

2.2 theta 関数

以下, 複素アーベル多様体と theta 関数に関して紹介する．複素アーベル多様体の参考文献として [BL04] を挙げる．

以下, 自然数 $g \geq 1$ を固定する．Siegel 上半平面を

$$\mathbb{H}_g := \{\Omega \in M(g, \mathbb{C}) \mid \Omega = {}^t\Omega,\ \mathrm{Im}(\Omega) > 0\}$$

と定義する．このとき, 各 $\Omega \in \mathbb{H}_g$ に対し, 格子 $\Omega\mathbb{Z}^g \oplus \mathbb{Z}^g \subseteq \mathbb{C}^g$ による商 $A := \mathbb{C}^g/(\Omega\mathbb{Z}^g \oplus \mathbb{Z}^g)$ は $\mathbb{C}$ 上 g 次元アーベル多様体になる．また, Ω の逆行列の虚部 $\mathrm{Im}(\Omega^{-1})$ は $\mathbb{C}^g$ 上の Hermite 形式を与え, Appell-Humbert の定理からこれは A 上の主偏極に対応する．すわわち, $\Omega \in \mathbb{H}_g$ は PPAV を与える．

次に $\mathbb{C}^g$ 上の theta 関数を定義する．theta 関数とは,

$$\theta(z, \Omega) := \sum_{n \in \mathbb{Z}^g} \exp(\pi i\, {}^t n \Omega n + 2\pi i\, {}^t n z)$$

のことである．さらに, 指標付き theta 関数を $a, b \in \mathbb{Q}^g$ に対し,

$$\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z, \Omega) := \theta(z + \Omega a + b, \Omega) \cdot \exp(\pi i\, {}^t a \Omega a + 2\pi i\, {}^t a(z + b))$$

と定義する．今, 自然数 n に対し, level$n$ の theta 関数とは n^g 個の関数

$$\{\theta\left[\begin{smallmatrix} 0 \\ \frac{b}{n} \end{smallmatrix}\right](z, \frac{\Omega}{n})\}_{b \in (\mathbb{Z}/n\mathbb{Z})^g}$$

のことである．これを単に $\theta_b(z)$ と書くとする．

以下, n を偶数とする．このとき nH に対応する symmetric line bundle$\mathscr{L}$ が一意的に存在する．上記の level n の theta 関数は n^g 次元 $\mathbb{C}$ ベクトル空間 $\Gamma(A, \mathscr{L})$ の基底を与える．

特に $n = 4$ のとき, $z \mapsto (\theta_i(z))_i$ で定まる $A = \mathbb{C}^g/(\Omega\mathbb{Z}^g \oplus \mathbb{Z}^g) \to \mathbb{P}^{(\mathbb{Z}/4\mathbb{Z})^g}$ は $(4^g - 1)$ 次元射影空間へのアーベル多様体の閉埋め込みを与える．特にこれによる射影座標を theta 座標という．以下, この $\{\theta_b(z)\}_b$ が上記の (i),(ii) の条件を部分的に満たすことを見る．

そのためにいくつか準備をする．$z \in A$ の theta 座標が与えたれたとき, 各 $i \in (\mathbb{Z}/4\mathbb{Z})^g$ に対する第 i 座標は (射影座標なので,) 単独では扱えない．そのため, theta 座標を affine 座標を持ち上げることで第 i 座標を単独で扱うことが出来る．すなわち, 閉埋め込み $A \to \mathbb{P}^{(\mathbb{Z}/4\mathbb{Z})^g}$ を自然な全射 $\mathbb{A}^{(\mathbb{Z}/4\mathbb{Z})^g} \setminus \{0\} \to \mathbb{P}^{(\mathbb{Z}/4\mathbb{Z})^g}$ によって以下のように持ち上げる．

$$\begin{array}{ccc} \tilde{A} & \longrightarrow & \mathbb{A}^{(\mathbb{Z}/4\mathbb{Z})^g} \setminus \{0\} \\ \downarrow & & \downarrow \\ A & \longrightarrow & \mathbb{P}^{(\mathbb{Z}/4\mathbb{Z})^g} \end{array}$$

そのために, いくつか準備をする．アーベル群 H を $H = \widehat{(\mathbb{Z}/2\mathbb{Z})^g} \oplus (\mathbb{Z}/4\mathbb{Z})^g$ とする．各 $\zeta = (\chi, i) \in H$ に対し u_ζ を, $P = (P_j)_{j \in (\mathbb{Z}/4\mathbb{Z})^g} \in \mathbb{A}^{4^g}$ を

$$u_\zeta(P) = u_{\chi,i}(P) := \sum_{t\in(\mathbb{Z}/2\mathbb{Z})^g} \chi(t)P_{i+t} \in \mathbb{C}$$

に送る写像として定義する. 逆に $\{u_\zeta(P)\}_{\zeta\in H}$ が与えられれば,

$$P_i = \frac{1}{2^g} \sum_{\chi\in\widehat{(\mathbb{Z}/2\mathbb{Z})^g}} u_{\chi,i}(P)$$

を計算することにより, $P = (P_i)_{i\in(\mathbb{Z}/4\mathbb{Z})^g}$ を復元できる.

また H の順序付けられた元 $\zeta_1, \zeta_2, \zeta_3, \zeta_4, \varepsilon$ が Riemann position にあるとは, $\zeta_1+\zeta_2+\zeta_3+\zeta_4 = 2\varepsilon$ が成り立つこととする. このとき, $\zeta_i' := \varepsilon - \zeta_i$ とする $(1 \le i \le 4)$. 今, 加法を計算するために重要な次の定理がある.

定理 2.1. ([LR12, Theorem 3.2]) 2 元 $x, y \in \mathbb{C}^g$ に対し, $(\theta_i(x))_i, (\theta_i(y))_i, (\theta_i(x-y))_i \in \mathbb{P}^{(\mathbb{Z}/4\mathbb{Z})^g}$ が与えられているとする. ここで, それぞれ任意に代表元をとり, それらを $\tilde{x}, \tilde{y}, \widetilde{x-y} \in \mathbb{A}^{(\mathbb{Z}/4\mathbb{Z})^g} \setminus \{0\}$ と書くとする. このとき, $x+y$ の affine theta 座標 $\widetilde{x+y} \in \mathbb{A}^{(\mathbb{Z}/4\mathbb{Z})^g} \setminus \{0\}$ で, 次を満たすものが存在する: アーベル群 H 上の任意の Riemann position $(\zeta_1, \zeta_2, \zeta_3, \zeta_4; \varepsilon = (\phi, m))$ に対し,

$$\begin{aligned} &u_{\zeta_1}(\widetilde{x+y})u_{\zeta_2}(\widetilde{x-y})u_{\zeta_3}(\tilde{0})u_{\zeta_4}(\tilde{0}) \\ =&\frac{1}{4^g} \sum_{\eta=(\omega,h)\in H} \{(\phi+\omega)(2h)(u_{-\zeta_1'+\eta}(\tilde{y})u_{\zeta_2'+\eta}(\tilde{y})u_{\zeta_3'+\eta}(\tilde{x})u_{\zeta_4'+\eta}(\tilde{x}))\} \end{aligned}$$

が成り立つ.

この定理を用いることにより, $x, y \in A$ に対し, $x, y, x-y$ の theta 座標が与えられたとき, $x+y$ の theta 座標が計算できる.

また, この加法を用いることにより, 核の theta 座標が与えられたとき, 同種写像の計算も可能である ([CR15]). 紙面の都合上, その詳細や具体的な計算に関しては省略し, 結果のみ述べる.

定理 2.2. ([CR15, Theorem1.1]) $\ell(\neq 2)$ を標数と異なる素数とし, $K \subseteq A[\ell]$ を Weil paring e_ℓ に関する極大等方部分群とする. このとき, $x \in A$ の theta 座標に対し, その $A \to A/K$ による像の theta 座標が $\tilde{O}(\ell^{\frac{rg}{2}})$ 回の演算で計算可能である. ここで, $\ell \equiv 1 \pmod 4$ のとき $r = 2$, $\ell \equiv 3 \pmod 4$ のとき $r = 4$ である.

3 主結果: B-SIDH に対する攻撃の実装

以上の議論を用いることにより, B-SIDH に対する攻撃を実装することが出来る. 定理 2.2の r の定義から, F の次数 N_A の各素因数の 4 による剰余が計算時間に大きく影響する.

実験は表 1の 4 つの p に対して行なった. これらは論文 [CD23, MMP+23] 以前に B-SIDH に対する最良の攻撃の 1 つであった Meet-in-the-Middle 攻撃 [FJP14, §5.1] に対して, それぞれ, 5 ビット, 10 ビット, 20 ビット, 25 ビットの安全性を持つものである. なお, これらは [Cos20, §5.2] の方法で生成した.

各ビット安全性の B-SIDH に対する攻撃に要した時間を表にした (表 1). ここで, $N_A > N_B$ であり, (N_A, N_A)-同種写像を計算することにより, N_B-同種写像の核の生成元を求めている.

表 1　B-SIDH に対する攻撃の所要時間. p は標数, N_A は与えられる点の位数, N_B は復元する同種写像の次数.

安全性	p	bit	N_A	N_B	時間 [秒]
5bit	104959	16	$3^2 \cdot 7^3 \cdot 17$	2560	436
10bit	202546499	27	$7^2 \cdot 11^2 \cdot 19 \cdot 29 \cdot 31$	4309500	6590
20bit	6257503668239	49	$13 \cdot 17^3 \cdot 19^2 \cdot 41 \cdot 43^2$	1154520972000	38873
25bit	6510321409315018751	62	$5^5 \cdot 7^3 \cdot 13 \cdot 19 \cdot 53 \cdot 59 \cdot 71 \cdot 79$	4274669342951424	263533

参考文献

[BL04] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2004.

[CD23] Wouter Castryck and Thomas Decru. An efficient key recovery attack on sidh. In *Advances in Cryptology –EUROCRYPT 2023*, pages 423–447, 2023.

[Cos20] Craig Costello. B-SIDH: Supersingular isogeny Diffie-Hellman using twisted torsion. In *Advances in Cryptology – ASIACRYPT 2020, LNSC 12492*, pages 440–463, Cham, 2020.

[CR15] Romian Cosset and Damian Robert. Computing (ℓ, ℓ)-isogenies in polynomial time on jacobians of genus 2 curves. *Mathematics of Computation*, 84(294):1953–1975, 2015.

[FJP14] Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Journal of Mathematical Cryptology*, 8(3):209–247, 2014.

[Har77] Robin Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer, 1977.

[Kan97] Ernst Kani. The number of curves of genus two with elliptic differentials. *Journal für die reine und angewandte Mathematik, vol. 1997, no. 485*, 148:93–122, 1997.

[LR12] David Lubicz and Damien Robert. Computing isogenies between abelian varieties. *Compositio Mathematica*, 148(5):1483–1515, 2012.

[MMP+23] Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski. A direct key recovery attack on sidh. In *Advances in Cryptology – EUROCRYPT 2023*, pages 448–471. Springer Nature Switzerland, 2023.

[Mum66] D. Mumford. On the equations defining abelian varieties. i. *Inventiones mathematicae*, 1(4):287–354, 1966.

[Mum70] David Mumford. Abelian varieties tata institute of fundamental research. 1970.

[Sil86] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate*

Texts in Mathematics. Springer-Verlag, New York, 1986.