SIDHへの鍵復元攻撃について

九州大学 IMI 共同利用・短期共同研究 プログラム
セキュアな量子情報活用に向けた次世代暗号の数理

小貫 啓史

東京大学

2022/8/4

概要

Wouter Castryck and Thomas Decru,
"An efficient key recovery attack on SIDH (preliminary version)"
https://eprint.iacr.org/2022/975

SIDH への古典**確率的多項式時間** (under heuristics) の鍵復元攻撃.
SIKE (SIDH ベースの KEM) は NIST 提案パラメータのすべてが破られた.

Magma 実装による解読時間:

- $IKEp217 ($50,000 USD): 6m,
- SIKEp434 (level 1): 62m,
- SIKEp503 (level 2): 2h19m,
- SIKEp610 (level 3): 8h15m,
- SIKEp751 (level 5): 20h37.

SIDH の公開情報である**補助点**を利用した攻撃.

同種写像問題

問題 1 (同種写像問題)

Given E_0, E: 超特異楕円曲線 $/\mathbb{F}_{p^2}$, find φ s.t. $\varphi : E_0 \to E$.

↑攻撃されていない

↓攻撃された

問題 2 (補助点付き同種写像問題)

E_0, E: 超特異楕円曲線 $/\mathbb{F}_{p^2}$, M, N: coprime smooth integers,
$\varphi : E_0 \to E$ s.t. $\deg \varphi = M$, P_0, Q_0: basis of $E_0[N]$.

Given $E_0, E, M, N, P_0, Q_0, \varphi(P_0), \varphi(Q_0)$, ($\mathrm{End}(E_0)$ の部分情報 *), find φ.

$*$ 定義は後述.

攻撃には以下の情報が用いられる:
1. 補助点 $\varphi(P_0), \varphi(Q_0)$, **2**. 同種写像の次数 M, **3**. ($\mathrm{End}(E_0)$ の部分情報)

影響範囲

同種写像暗号の**全てが破られたわけではない**.

補助点を使う方式は (おそらく) 全部ダメ

破られた	安全性低下？	攻撃されていない
SIDH, SIKE	Séta	CSIDH
B-SIDH		SQISign

Séta は End の部分情報がないので完全には破られていない... かも

攻撃方法

補助点チェックを構成し, SIDH を break (PPT under heuristics) した.

補助点チェック $\mathcal{A}$:

入力: E_0, E, P_0, Q_0: basis of $E[2^a]$, P, Q: basis of $E[2^a]$, 3^b.
(assume $2^a > 3^b$.)

出力: exists? $\varphi : E_0 \to E$ s.t. $\deg \varphi = 3^b, P = \varphi(P_0), Q = \varphi(Q_0)$.

Attack on SIDH:

$\varphi : E_0 \to E$, $\deg \varphi = 3^b$: 秘密の同種写像, P_0, Q_0: basis of $E[2^a]$

1. 最初の 3^β-同種写像の候補 $\varphi_1 : E_0 \to E_1$ を計算.
2. 補助点チェック: $\mathcal{A}(E_1, E, \varphi_1(P_0), \varphi_1(Q_0), \varphi(P_0), \varphi(Q_0), 3^{b-\beta})$
   - 真なら $E_0 \leftarrow E_1$, $b \leftarrow b - \beta$ としてステップ 1 へ.
   - 偽なら φ_1 を取り直してステップ 2 へ.

この繰り返しで 3^β 次毎に秘密の同種写像が復元できる.
(補助点チェックがうまく動くように β は各計算で異なる可能性がある.)

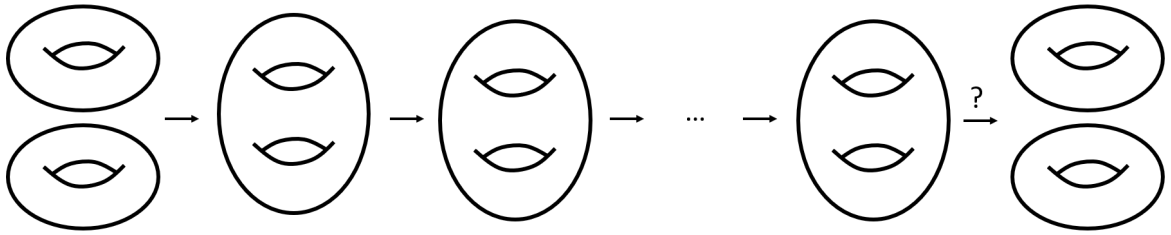
補助点チェック

入力: E_0, E, P_0, Q_0: basis of $E[2^a]$, P, Q: basis of $E[2^a]$, $3^{b-\beta}$.
出力: exists? $\varphi : E_0 \to E$ s.t. $\deg \varphi = 3^{b-\beta}, P = \varphi(P_0), Q = \varphi(Q_0)$.

1. $c := 2^a - 3^{b-\beta}$.
2. c が条件を満たさない場合, β を取り直す (後述).
3. Let $\gamma : E_0 \to C$ s.t. $\deg \gamma = c$.
   (ここで γ は計算できないが, C と $\gamma|_{E_0[2^a]}$ は計算可能.)
4. $P_c := \gamma(P_0)$, $Q_c := \gamma(Q_0)$.
5. $(2^a, 2^a)$-同種写像 with kernel $\langle (P_c, P), (Q_c, Q) \rangle$ の像を計算.
6. Return (像が楕円曲線の積かどうか?).

$(2^a, 2^a)$-同種写像のイメージ

論文より図を転載



適当な $(2,2)$-同種写像の像が分離できる確率は約 $1/p$.
$\Rightarrow$ 最終的な像が分離できるのは正しい補助点のときのみ!

γ の計算

再掲: $c := 2^a - 3^{b-\beta}$, $\gamma : E_0 \to C$ s.t. $\deg \gamma = c$.
C と $\gamma|_{E_0[2^a]}$ を計算するため, c に条件あり.
(条件を満たすように a を a より小さな整数に変えても ok.)

$\mathrm{End}(E_0)$ の部分情報あり

部分情報とは, 小さな非整数自己準同型を持つ E_{start} から E_0 への 2 と互いに素な次数の同種写像のこと.
E.g., $E_{\mathrm{start}} : y^2 = x^3 + x$ or $y^2 = x^2 + 6x^2 + x$ $(2\sqrt{-1} \in \mathrm{End}(E_{\mathrm{start}}))$.
$\Rightarrow$ c の条件: c の因子がすべて $\equiv 1 \pmod 4$.

$\mathrm{End}(E_0)$ の部分情報なし

c の条件: 以下の形で smooth なものが 1 つ見つかれば ok:

$$c = d2^{a-\alpha} - e3^{b-\beta} \ (\alpha < a,\ \beta < b,\ d \text{ と } e \text{ は小}).$$

(安全性パラメータより小さな) 指数時間攻撃は可能かもしれない.

SIDH-SIKE は修正できるか?

以下のどれかを秘密にする必要がある:
1. 補助点 $\varphi(P_0), \varphi(Q_0)$, **2**. 同種写像の次数, **3**. ($\mathrm{End}(E_0)$ の部分情報)

- **1** を無くしたらもはや別の方式? (CSIDH, OSIDH)
- 効率性を損なわずに **2** をなくすのは難しそう.
- SIKE では, **3** を秘密にできるが, 前述の通り攻撃を完全には防げない.